

ISBN 978-1-902983-17-2



**£70.00**

**Technical Support Helpline:**  
+44 (0)845 6023075

## 8 Solutions

Head Office  
The Business Park  
Woodhouse Lane  
Bolsover, Chesterfield  
Derbyshire S44 6BD

[www.8solutions.com](http://www.8solutions.com)



Data centre contamination control handbook | First edition | [www.8solutions.com](http://www.8solutions.com)

# Data centre contamination control handbook

A definitive guide to understanding  
and controlling data centre contamination

**Kaushal Doshi, Amit Mehta**

First edition



---

---

---

---

---

---

---

---

---

---

# The Data Centre Contamination Control Handbook

The definitive guide to data centre contamination management

Prevent ICT equipment failures

Maximise data centre uptime

Improve energy efficiency

---

---

---

---

---

---

---

---

# Contents

|  |           |
|--|-----------|
| <b>1 What is a data centre?</b>  | <b>7</b>  |
| Introduction   | 7         |
| Data centre history  | 7         |
| Today's demands on data centres  | 8         |
| Data centre classification   | 9         |
| Industry views on data centre contamination, availability and energy costs | 10        |
| Summary  | 11        |
| <b>2 Contaminants and their effects on data centres</b>                    | <b>12</b> |
| Types of contamination   | 12        |
| Particulate matter   | 12        |
| Gaseous contamination  | 14        |
| How contamination makes critical contact with ICT equipment                | 15        |
| How contamination damages ICT equipment.                                   | 16        |
| Contaminant properties   | 16        |
| Equipment susceptibility to PM   | 16        |
| Equipment susceptibility to gaseous contamination                          | 18        |
| Why ICT equipment is increasingly susceptible to contamination damage      | 18        |
| Contamination and OEM warranties   | 19        |
| Summary  | 19        |

|   |           |
|---|-----------|
| <b>3 Contamination control classification standards and information resources</b> | <b>20</b> |
| The origins of contamination control  | 20        |
| International standards and contamination classification                          | 20        |
| Particle sizing   | 21        |
| Federal Standard 209  | 22        |
| ISO Standard 14644-1  | 22        |
| Guidelines for assessing gaseous contamination                                    | 24        |
| Information sources   | 25        |
| Summary   | 27        |
| <b>4 A 'whole life' strategy for contamination management</b>                     | <b>28</b> |
| <b>5 Data centre location, design and construction</b>                            | <b>29</b> |
| Geographical location of facility   | 29        |
| Locating the computer room within the building                                    | 30        |
| Attached or adjacent staging areas  | 30        |
| Attached or adjacent storage areas  | 31        |
| Movement of people, equipment and materials                                       | 31        |
| Office and operations areas   | 31        |
| Considerations for computer room materials  | 31        |
| Computer room materials – wall, ceiling, underfloor and surfaces                  | 32        |

---

---

# Contents

## **6 HVAC Systems 36**

|   |    |
|---|----|
| Makeup air                                      | 36 |
| Positive pressurisation                         | 36 |
| Humidification systems                          | 36 |
| Air filtration                                  | 38 |
| High Efficiency Air Filtration and HEPA filters | 41 |
| HEPA Specifications                             | 42 |
| HEPA Filter Testing                             | 42 |
| Filter housing for high efficiency filters      | 43 |
| Fire suppression systems                        | 44 |
| Mechanical malfunction                          | 44 |
| Ceiling returns                                 | 45 |
| Computational Fluid Dynamics (CFD)              | 46 |

## **7 Data Centre Operations and Security Procedures 47**

|  |    |
|--|----|
| Record keeping                                   | 47 |
| Monitoring                                       | 47 |
| Severe equipment failure monitoring              | 48 |
| Non-severe equipment failure monitoring          | 48 |
| Access control                                   | 48 |
| Contamination control mats                       | 49 |
| Data centre change control                       | 51 |
| Managing non routine events                      | 51 |
| Maintenance, repair and re-organisation activity | 52 |

---

---

## **8 Data centre decontamination 54**

|  |    |
|--|----|
| Elements of cleaning programme design                  | 55 |
| Specialist decontamination contractors and their staff | 55 |
| Do they have a Security Check (SC)?                    | 56 |
| Ceiling void and infill bags                           | 64 |
| Walls, doors and ledges                                | 65 |

## **9 Testing and assessing contamination levels 69**

---

---

# Foreword:

## 8 Solutions Perspective

8 Solutions has been an expanding business since 1991 for one simple reason: Data centre decontamination makes sound commercial sense to owners and operators. For a modest investment in a suitable decontamination service, they can enjoy benefits ranging from an improvement in energy efficiency through to protection from a catastrophic systems failure.

But what exactly is data centre decontamination, why is it so important, and why is this importance to data centres growing continuously? This handbook answers these questions and provides a practical reference guide to inform your own data centre decontamination strategy.

Data centres have evolved into facilities which are frequently essential to their owners' continued business viability. We look at the level of service they are expected to provide, and how such service levels have now been classified into tiers. We see how a data centre's role within most organisations means that its uptime and energy efficiency have both become business critical issues. With this in mind we review the contaminants which would, if allowed uninhibited access into the data centre, pose a threat to the ICT equipment, its uptime and energy efficiency. We also show why advances in ICT technology are increasing the hardware's susceptibility to such contamination.

Knowing what the contaminants are is important, but for this knowledge to be useful we must understand how these contaminants translate from a threat to a problem. This happens in a number of ways, which we explain.

Having established which contaminants are threats, and how they can damage ICT equipment, we describe how to avoid these harmful effects. We see how it's possible to develop a strategy that begins before the data centre has even been built. The outdoor environment, as well as the data centre's design, layout and use of materials are all contributing factors. Once the data centre becomes operational, a strict policy for security, and for controlling access of people and equipment into sensitive areas, is also essential. However the reality is that no matter how much effort is put into designing contamination out, it will inevitably find its way into areas where it isn't wanted.

Therefore, setting up an ongoing decontamination schedule is an essential part of any contamination control strategy. However we shall see that this type of decontamination is not something that general purpose office cleaners can be expected to do. Such cleaners won't actually be effective and are more likely to cause serious problems

---

---

instead. To achieve reliable, safe and measurable protection from contamination takes specialist skills, equipment and decontamination products.

This Handbook describes how to plan and implement a professional cleanliness strategy appropriate to the needs of a data centre. It covers how to qualify the staff or contractor you use, how to plan the depth and frequency of any decontamination operations, and how to design your strategy according to the conditions within your data centre – the type and density of equipment, cabling, floor and ceiling voids, air conditioning, surface finishes and materials used. It also reviews how testing can ensure that cleanliness to ISO 14644 and other relevant standards has been achieved. Such certification of cleanliness not only gives confidence that the contaminant threat has been removed, but may become vital evidence in warranty replacement claims.

In short, this Handbook explains the threat of contamination to information processing and communications equipment housed within data centre environments. It's also a practical guide, with information you can use directly to safeguard your equipment from such contamination throughout the lifetime of your data centre.

LoRes, rights managed image



# What is a data centre?

## Introduction

Generally, a 'Data Centre' is a space dedicated to housing, supporting and protecting information and communications technology (ICT) equipment. However, today this could mean a server and modem for a High Street travel agent, or it could refer to Next Generation Data's 750,000 sq ft facility in South Wales, with capacity for up to 19,000 server racks. The consequences of failure vary hugely in scale, yet they are always serious to those affected by the loss of service. Data centres in one form or another are everywhere, and their security and availability is essential for all of us.

Therefore, operators and owners of all sized data centres are consistently concerned with improving availability and security. And in today's climate of ever increasing energy costs and environmental sensitivity, the need to cut energy demand is also a pressing issue. We shall see how an effective cleanliness policy can help to address both these concerns. Because data centres have become so central to their owners' operational viability, we also show how they are now being classified according to their reliability. The chapter finishes with a review of different industries' perspective on data centres, and on how decontamination is increasingly contributing to ICT equipment reliability and energy management.

## Data centre history

Early commercial computers were large, complex and difficult to operate and maintain. They also required large amounts of cabling, and generated heat which had to be removed. Security also became an issue as computers accumulated information vital to their operators' records and activities. It was therefore a natural response to build large computer rooms to house these early systems, which were clearly unsuitable for location within an office environment. A computer room could provide the necessary cooling, adequate space to site the equipment racks, and arrangements such as under floor voids or cable trays to handle the cabling generated by these systems. Containing all the computing equipment within one area also made security easier to manage.

The advent of the microprocessor and the PC in the Eighties brought a change to this scenario. The promise of personal computing was too compelling to ignore, so the focus of computing power moved from the computer room out to the desktop. Little attention was paid to the computers' environment, but then the loss of a single machine was not so catastrophic for the organisation as a whole.

However during the Nineties IT discipline began to reassert itself, especially with the rise of network popularity and client/server architectures. IT departments were moving servers back into central locations where they could better control the hardware and access to it. This trend was accelerated in the later Nineties and the Dotcom bubble. Companies of all sizes had to establish an Internet presence very quickly – something beyond the resources of many of them. To meet this new opportunity, third party Internet data centres, as they were then called, sprang up to offer rentable online computing and communications capacity. New technologies and practices were developed to manage these large scale centres, then taken up more widely as user organisations deployed them internally. Although developments in both ICT technology and environmental management have continued apace, the data centre as we now know it had arrived.

## Today's demands on data centres

Although today's data centre provides the same centralised processing role as its earlier computer room equivalent, there are important differences in its relationship with its operator as well as in the equipment it contains. Originally, computers were something of a luxury as they automated tasks that had previously been performed manually – and could be performed manually again if the computer failed. Today, many organisations are entirely dependent on their ICT equipment's uninterrupted availability to stay in business. Typically, they have 24/7 operations involving online transaction processing at a national or international level. Reverting to manual operation in the event of an extended ICT failure is no longer an option. The stakes are much higher,

with more profound implications for the operating companies. Protection and security of data is equally as important. At the same time, data centres tend to generate high energy demands which must be addressed. Failure to do so will not only incur financial costs but also reputational damage with the advent of environmental sensitivity and CRC legislation.

Operators everywhere are endeavouring to meet today's demands for uninterrupted availability and energy efficiency. UPS systems protect the quality and availability of the electrical supply to the processing hardware, and typically feature built-in redundancy. Increasingly, back-up generators are made available to complement the UPS batteries' finite autonomy. Redundancy in both power and data cabling is used to increase availability, and more recently, concepts such as cloud servers or clustered servers are being implemented. Here, virtual servers (The servers that users see) can run on any one of a cluster of 'real' hardware servers, freeing them from the problem of a single server failure. Server virtualisation can also improve energy efficiency by making better use of hardware server capacity. Care in the choice of UPS system can also contribute significantly to energy saving.

Data centre cleanliness is now recognised as a key factor in these efforts to maximise availability and minimise energy costs. And with the advent of cleanliness standards such as ISO 14644, and energy surveys conducted by major data centre users, this contribution can now be measured and quantified.

## Data centre classification

Because data centre availability is of such vital importance, an organisation called the Uptime Institute has established a definitive classification system to describe data centre availability and the topologies used to achieve it. Based on earlier work by the Telecommunications Industry Association, the classification comprises four tiers, of which Tier 4 is the most stringent. Table 1.1 (opposite) shows the tier definitions.

This 4-Tier classification is one result of the Institute's research, which in its own words "focuses on data center facilities, the IT and facilities interface, and how both functions affect the cost, reliability and energy consumption of computing".

The next section of this chapter reveals different industry views on these interrelated topics of cleanliness, reliability, energy and costs.

Table 1.1: Uptime Institute 4-Tier Data Centre Classification

| Tier Level | Requirements   |
|------------|--|
| 1          | <ul style="list-style-type: none"> <li>• Single non-redundant distribution path serving the IT equipments</li> <li>• Non-redundant capacity components</li> <li>• Basic site infrastructure guaranteeing 99.671% availability</li> </ul>   |
| 2          | <ul style="list-style-type: none"> <li>• Fulfils all Tier 1 requirements</li> <li>• Redundant site infrastructure capacity components guaranteeing 99.741% availability</li> </ul>   |
| 3          | <ul style="list-style-type: none"> <li>• Fulfils all Tier 1 and Tier 2 requirements</li> <li>• Multiple independent distribution paths serving the IT equipments</li> <li>• All IT equipments must be dual-powered and fully compatible with the topology of a site's architecture</li> <li>• Concurrently maintainable site infrastructure guaranteeing 99.982% availability</li> </ul>         |
| 4          | <ul style="list-style-type: none"> <li>• Fulfils all Tier 1, Tier 2 and Tier 3 requirements</li> <li>• All cooling equipment is independently dual-powered, including chillers and Heating, Ventilating and Air Conditioning (HVAC) systems</li> <li>• Fault tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability</li> </ul> |

## Industry views on data centre contamination, availability and energy costs

Our feedback from different areas of the IT industry reveals operators' views and depth of concern on controlling contamination to mitigate both reliability and energy efficiency issues.

The Telecom industry leads the field in terms of concern. This is partly due to how critical data centres are to their business, but also because increased contamination will increase power costs across their estate by an estimated 2–5%, which represents a huge amount of money. Also, telecom companies own much high-value Cisco hardware such as Catalyst switches, LAN switches and associated media cards. This hardware is at increased risk of contamination due to the high volume of human traffic in telecom data centres. As we shall see, allowing this hardware to become contaminated could compromise its warranty cover; a loss which is unacceptably expensive to its owners. BT, Orange, C&W, Vodafone and other telecom companies have been early adopters of specialist decontamination services, typically scheduling a deep clean every quarter.

---

Second in terms of expressed concern are the IT Services and Managed Data Centre Services companies such as EDS and CSC. As the data centre is actually the core product and USP of such companies, its wellbeing is vital to their continued business existence. Their security levels are reflected by their use of retinal scanning and finger print entry systems to control access, and they clean quarterly or 6-monthly, with a surface clean every month. Because of the sales role of the data centres within these organisations, the aesthetic and visual benefits of scheduled decontamination are important as well.

Banks and building societies, and Government agencies are joint third in expressed concern. Merrill Lynch, CSFB and RBS clean their High Availability data centres at least six monthly, sometimes via their M&E FM partner. DrKW/Commerzbank decontaminates their main UK data centre every month. The Inland Revenue and Land Registry implement similar decontamination schedules. As with the other industry sectors, these organisations are running expensive hardware and critical systems that cannot be allowed to fail due to the financial consequences of doing so. Citigroup recently suffered an outage in Paris on a settlements system which was traced to a cabinet completely enveloped in contamination. Energy efficiency is also an important factor here; Lloyds Banking Group has estimated that higher contamination levels will increase power consumption by approximately 1.93%. Security is a major issue, with security clearance and police vetting imperative for most people entering any Government site and data centre. Only specialists with an intimate understanding of these environments are given access, with generalist decontamination companies very rarely used.

## Summary

This chapter has shown how data centres have grown to fill the role once performed by computer rooms. We have also seen how, far more than the original computer rooms, data centre availability is of vital importance to business survival. The Uptime Institute's work on classifying data centre reliability reveals energy efficiency as an important and related issue. This is borne out by feedback from different ICT users revealing how they regard contamination control as an essential part of both their data centre availability and energy efficiency strategies. The next chapter looks more closely at what contamination is, and how it damages ICT equipment.

---

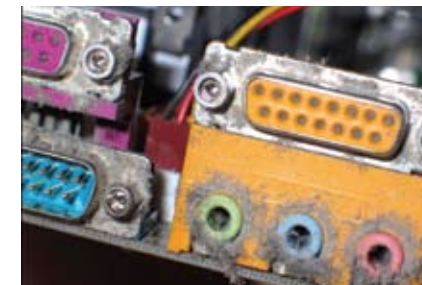
# Contaminants and their effects on data centres

HP's BladeSystem Site Planning Guide describes contamination in its various forms as an environmental element that can affect a HP BladeSystem installation. It cites mechanical failure of disk and tape drives, electrical failures of power supplies and densely packed circuit boards, corrosion damage, and overheating as examples of equipment damage and malfunctions due to contamination.

HP's advice reflects a growing awareness and concern among equipment vendors as well as data centre operators on the subject of contamination and its control. In particular, warranty claims can increasingly be an issue: For some vendors, data centres who cannot prove that they have maintained decontamination to an agreed standard such as ISO 14644-1 will find their ICT equipment warranty claim invalid. A bank in New York lost a warranty claim for \$50k for this reason, and equipment OEMs are increasingly using loss adjusters to review equipment failure causes.

Protection from such problems starts with a clear understanding of what contamination is, how it is created, how it enters data centres, penetrates and settles on ICT equipment, and how it disrupts when it does so. This chapter covers these issues, providing a background from which to develop an effective contamination control strategy.

## Types of contamination



Contamination is airborne, and exists in two forms: particulate matter (PM) and gaseous. Both forms in turn break down into different types, which can cause problems in different ways. Also particulate and gaseous contamination can interact, and particulate contamination effects can be modified by ambient humidity levels.

### Particulate matter

Particulate matter contamination can be solid or liquid. It can originate either from within the data room, elsewhere within the building housing the data centre, or outside the building in the open air environment. If it is generated outside, it can enter the data centre through open doors, through the air handling system, on people's clothes, on equipment brought into the room, or on packaging for the equipment.

---

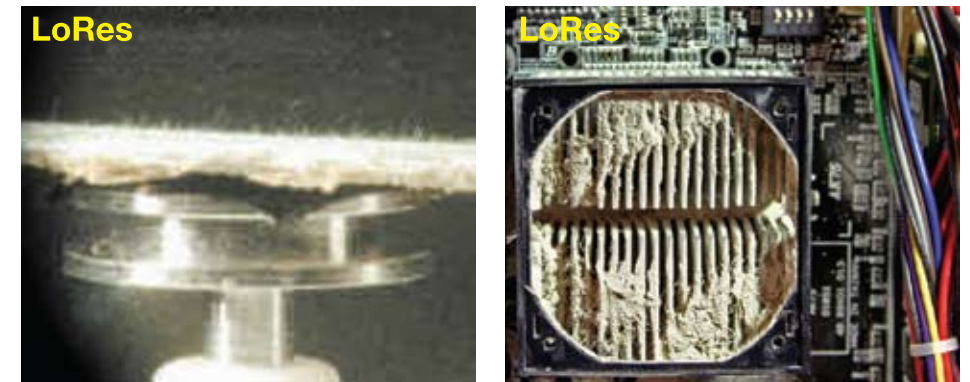
---

Contamination originating from outside the building comes from many potential sources. The exact mix of these depends very much on the geographical location of the data centre building, and possibly on the time of year. For example a data centre near a farm could be subjected to high levels of dust, and these levels could be exacerbated during times of ploughing. Alternatively a nearby fire could raise the airborne particle count as well as creating gaseous contamination. Winds carrying salt from the sea, nearby processing plant, generating stations, plant pollens and traffic can all also contribute. Contamination generating activities and equipment within the data centre's building include toner dust from copiers and printers and the paper used for them, occupant hair and clothing, smoking, (a cigarette smoke particle is eight times larger than the gap between a hard disk drive read/write head and the platter surface). Activities such as unpacking equipment, construction, decorating and refurbishment create cement wall dust, drywall dust, insulation, paper and cardboard fibre. Fan belt wear in air handling units (AHUs) and vacuum cleaners also creates PM, as can materials used in the construction of the building's ceilings, walls and floors.

People entering a data centre can be a source of contamination for many reasons. Hair, clothes fibres and mud on shoes all contribute directly. This is increased by any activities they may engage in, such as eating, drinking, bringing equipment into the room and unpacking it. Contamination can also enter through the air handling system and doors as mentioned.

The data centre itself often contains contamination sources as well. Metal, glass and some plastic materials can look good in a data centre, and they are beneficial from a contamination control perspective as well, because they produce little or no PM. However, for cost or other limitations, they are typically not used on walls, ceilings or floor coverings. Instead, the rooms often comprise concrete floors, drywall walls and cellulose suspended ceiling tiles. Each of these materials generates significant PM, particularly during construction when vibration or abrasion can exacerbate PM release.

Concrete materials, found in almost all data rooms, can be particularly problematic. Exposed concrete surfaces continuously oxidise and break down. This releases loose sand and lime PM. Lime dust is particularly corrosive when combined with water or humidified. Wall coverings create PM if they are of poor quality or badly maintained. Sub-standard paint can become chalky and rub off and unused holes can admit contaminants if they are not painted and sealed without delay. Porous surfaces such as fabric can capture and release PM, as well as being difficult to clean. Most commercial ceiling tiles are unsuitable for data centres as they are manufactured from compressed cellulose, which can easily be broken into small fragments. Either vibration or movement for maintenance access can cause small fragments to chip or break off. Above these panels, exposed concrete in the ceiling space can release the same PM as that in floors and other surfaces. Sprayed-on fire insulation used to protect structural steel can also be a source of PM.



Raised access floors can be a source of zinc whiskers, which are a particularly hazardous form of PM. They most frequently originate from the zinc-plated underside of raised-access floor tiles and raised-access support structures such as pedestals and stringers. These metal surfaces are coated with zinc in a galvanisation process to help protect them from corrosion. While several techniques such as hot-dip or spraying are used, whisker growth appears to be limited to electroplated samples. The whiskers are zinc crystals formed by the degradation (corrosion) of the galvanised metal surface. Whisker growth on access floor tiles is of particular concern as these have a large surface area and are often disturbed during normal activity on a computer room. Growth is most likely to occur on wood-core access panels and flat-bottomed concrete core panels. Although access floor tiles have been used in high-technology facilities since the 1960's, it is apparent that some, if not all of their manufacturers did not give adequate forethought to the electro-chemical instabilities of the metal stock used in their products.

These whiskers are typically 2 microns in diameter and over many years can grow up to 10 mm in length, although typically less than 1 mm. Under proper lighting, they can be visible to the naked eye on surfaces. The whisker formation process consists of an unpredictable incubation period, typically lasting months or even years without any growth at all, followed by a period of growth at rates as high as 1mm per year. Some zinc coated surfaces may never grow whiskers. Unfortunately, accelerated techniques do not currently exist to predict if, when, and to what extent a zinc-coated surface will produce whiskers. Not all electroplated surfaces exhibit whisker growth and not all develop the problem at the same rate. There is no clear evidence that environmental factors will exacerbate whisker growth.

Other metals besides zinc are known to produce whiskers. These include tin, indium, gold, cadmium and antimony.

Poor maintenance and badly fitted interiors can contribute to PM levels as well as inappropriate materials. The volume of air entering through building cracks can be significant, and this can bring in PM either from contaminated areas within the building,

or from outdoors. Positive pressurisation, which can help to keep contamination out, can be hard to maintain if air leakage is excessive. These leaks can be caused by broken or chipped ceiling tiles, insufficient caulking of drywalls, and building movement or expansion. Openings left in the base of columns after cable installations can also create significant airflow, and transport of contaminants, due to the chimney effect.

PM can arise from the ICT equipment itself as well as from the environment within and beyond the data room. Equipment cabinet frames and server frames, racks, housings and rails have all been reported as sources of zinc whiskers.

### Gaseous contamination



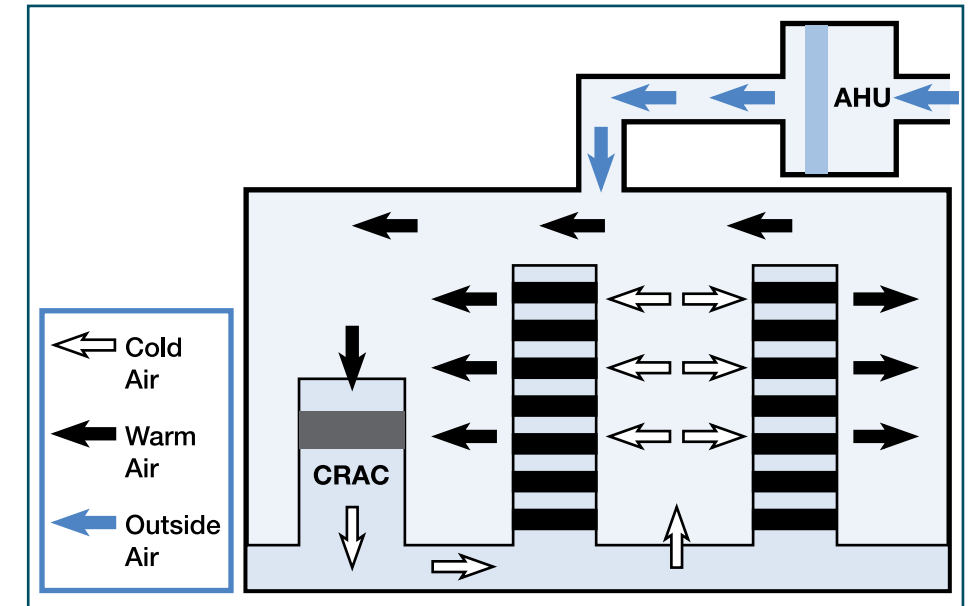
Gaseous contamination can be a threat to electronics equipment, mainly through causing corrosion. Gases can occur naturally or as a by-product of industrial or manufacturing processes. Outside pollution such as smog can contain sulphur, bromine and chlorine compounds. The most common gases affecting data centres are Sulphur Dioxide (SO<sub>2</sub>) and Hydrogen Sulphide (H<sub>2</sub>S).

Other gases of less concern but still occurring in data centres include Chlorine (Cl), Hydrogen Chloride, (HCl), Nitrogen Dioxide (NO<sub>2</sub>), Ozone (O<sub>3</sub>) and Ammonia (NH<sub>3</sub>). Gases can act alone, in conjunction with one another or in combination with particulate matter. Depending on the location, external circumstances and events, the presence of contaminating gases is inevitable, although it can be controlled.

## How contamination makes critical contact with ICT equipment

PM enters the data centre, moves around it, and finds its way into ICT equipment, because it is transported by the airflow through the room. Outside air, sometimes referred to as makeup air, is drawn through an air handling unit (AHU), where it is conditioned by being passed through a series of air filters. The conditioned air is then supplied to the servers through the raised access floor. Fans within the servers draw the air through the equipment cabinets. The warmed air is then cycled back and conditioned through computer room air conditioning units (CRACs), computer room air handling units (CRAHs) or through the AHU return. Most data centres only draw in a small volume of outside air, to maintain positive pressurisation for a system which is basically using internal air recirculation. Sometimes, air can only enter the data room through filters from adjacent building areas. However adding outside air economisers

Figure 1.3: Airflow in a raised-access floor data centre



to AHUs is increasingly popular, because operators can save energy by using outside air for cooling.

Contamination becomes a problem when PM is transferred onto vulnerable equipment lying within its air flow path. This can happen through three different reasons:

- Gravitational settling.
- Diffusion movement.
- Electrostatic attraction.

Gravitational settling affects large particles the most, because it is a function of particle mass. It becomes insignificant for particles smaller than approximately 1 µm in diameter, while those greater than 10 µm have a short residence time and are likely to settle out before reaching the ICT equipment. However, strong air currents can prolong airborne residence time, even for larger particles.

The diffusional movement of PM is caused by random collision of air molecules against airborne particles. These collisions allow particle migration from higher to lower concentrations. Diffusion is only significant for very small particles, with minimal effect on particles greater than 0.1 µm in diameter. Larger particles mainly deposit on horizontal surfaces, while smaller particles tend to deposit equally on both horizontal and vertical surfaces.

---

Electrostatic attraction relates to the force that attracts oppositely charged articles, or causes them to settle on surfaces. Clothes clinging together with static electricity demonstrate the same effect.

Particles that settle on a surface tend to remain deposited, irrespective of how they arrived, because of the cohesive forces between the particle and the surface. However, activities such as floor sweeping or movement of tiles for maintenance can cause resuspension.

Gaseous contaminants diffuse in the air to occupy the entire room volume, but differences in air density may cause stratification. The air movement controls the movement of contaminants.

## How contamination damages ICT equipment

### Contaminant properties

PM can affect ICT equipment in different ways, according to its composition and properties. PM can comprise organic, inorganic, synthetic or metallic materials, alone or combined. It can be abrasive, corrosive, electrically or thermally conductive, insulating, or hygroscopic. Its effect on ICT equipment falls into three categories:

- Electrical: Some PM – particularly zinc whiskers – is conductive, and can cause impedance changes or bridge tracks in electronics circuit boards.
- Chemical: Corrosion of surfaces, dendrite growth and material property changes such as embrittlement or clouding of optical surfaces.
- Mechanical: Obstruction of cooling air flow, interference with moving parts, abrasion, optical interference, interconnect interference, deformation of magnetic media and other surfaces, and other similar effects.

These effects can be caused by one form of PM, several forms combined, or by combinations of PM and gaseous contamination. Elevated humidity can also accelerate contaminant damage, particularly corrosion. In addition to these damage modes, the appearance of PM contamination is unsightly. This can encourage lax operational procedures, and is a particular disadvantage where data centre processing capacity is being offered to third party users.

### Equipment susceptibility to PM

PM creates the problems listed above by accumulating. Its rate of accumulation is related to its concentration and the volume of air passing through the susceptible equipment. Therefore, forced-air cooled equipment may be more susceptible to accumulated PM

---

than liquid – or free convection – cooled equipment. Not all particulates will settle within the equipment; some will pass through and exit with the exhaust air. Also, particles that do settle will not be evenly distributed across the equipment; some locations are more likely to be particularly susceptible. These include:

- Small airflow openings such as intake and exhaust openings, as well as unintended air leakage areas including rivet holes and sheet metal seams.
- Fine-pitch heat sink cooling features.
- Areas where flow bypass is impossible; particularly noticeable where flow ducting forces air through a heat sink.
- Areas where airflow is suddenly reduced in speed or is changed in direction.
- Sharp, rough or adhesive surfaces, including surfaces so rendered by airborne contaminants.

PM can cause different problems, depending on where it settles within the ICT equipment, as below:

### Fans, heat sinks and cooling mechanisms



Current CPU heatsink designs typically feature thin, closely spaced metal cooling fins. These are susceptible to PM blockage, especially if the PM has significant fibre content. Fibres lodge across the fins, building a barrier that captures further PM until airflow can become entirely blocked. This reduces the cooling efficiency of the heat sink, possibly leading to

intermittent or permanent equipment failure due to overheating. A fan mounted on the heatsink would also become blocked.

Restriction of intake and outlet vents can alter an equipment enclosure's pressure curve, causing greater fan loading or reduced airflow. Changes in processor temperatures caused by blocked heat sinks can also trigger fan speed increases in systems equipped with fan speed controllers. These contamination issues may be misdiagnosed as fan problems.

### Power efficiency issue

If the equipment fans are driven to work harder to compensate for impaired heat sink efficiency or for their own reduced efficiency, the equipment's energy demands and carbon footprint will be increased.

---

### Magnetic media and optical drive mechanisms

PM can accumulate on grease used in media drive positioning and auto-loading functions, where it can cause abrasion or blockage of the moving parts. Magnetic media can also generate PM in the form of oxide flake-off. Particles can cause deformation of media surfaces, or interfere with head contact or spacing. In extreme cases PM may abrade read/write heads. Fixed-disk hard drives use filters to prevent these vulnerabilities. Optical drives may experience similar problems; PM may also interfere with the optical signal used to read or write data on the media.

### Electronics circuit boards and connectors

PM, especially zinc whiskers, can be electrically conductive. If such PM settles within ICT equipment so as to bridge between signal tracks on an electronics circuit board, it can cause a short circuit resulting in either intermittent or permanent equipment failure. Short circuits can also be caused by less obvious mechanisms such as leakage paths created by moisture-laden hygroscopic particulate accumulation. Water-soluble ionic salts can also produce electrically conductive contaminants if they absorb sufficient moisture from the ambient air. Sulphate, Nitrate and sea salt are the most commonly occurring and represent a significant proportion of urban PM (McMurry et al 2004). Empirical results have shown that exposure to high sulphate concentrations at high humidity can cause electronic equipment failure (Litvak et al 2000). Whereas particle accumulation may take place over a number of years, the change in conductivity can occur suddenly. Sudden spikes in humidity can trigger equipment failure.

## Equipment susceptibility to gaseous contamination

As previously mentioned, sulphur bearing gases such as sulphur dioxide (SO<sub>2</sub>) and Hydrogen Sulphide (H<sub>2</sub>S), are the most common gases in data centres causing corrosion. SO<sub>2</sub> is a product of fossil fuel combustion, organic waste incineration, and is also found in paper, fabrics, food preservatives, fumigants and refining. It reacts with water to form sulphuric acid, which is highly corrosive. Other gases can act similarly. For example Nitrogen Dioxide (NO<sub>2</sub>), produced by traffic and energy production, combines with water to form nitric acid which corrodes electronics materials.

Sulphur bearing gases can also react with silver inside electronic components to form silver sulphide (Ag<sub>2</sub>S) flowers. Such formations have been known to create enough mechanical stress to cause component failure.

---

## Why ICT equipment is increasingly susceptible to contamination damage

Data centre operators and OEMS have been aware of contamination issues for decades, but the problem has been becoming steadily more acute for a number of reasons, mostly associated with hardware density.

At room level, higher packing densities of more powerful equipment demand extremely efficient heatsinks and greater air exchange volume. These heatsinks are more susceptible to loss of efficiency through clogging, while the higher air flow carries more airborne contaminants to the equipment.

The age of existing floor structures is also becoming an issue, as many facilities now have flooring that has been in place for over ten years, allowing whiskers to reach a length sufficient to bridge exposed conductor tracks. This can be exacerbated by increased maintenance and up-grade activity in raised-floor facilities. Any activity that involves moving flooring can dislodge whiskers, and in current high-tech environments, computing facilities frequently undergo regular maintenance activity such as adding and removing hardware or repositioning and reconfiguring equipment.

At equipment level, OEMs constantly strive to deliver more processing power from smaller enclosures. The resulting shrinkage means smaller distances between adjacent circuit board tracks, which can more easily be bridged by smaller conductive particles. Processor chips and other ICs are also tending to be driven by lower voltages, so there is less energy available to melt conductive bridges as they appear across tracks. In addition, the Restriction of Hazardous Substances (RoHS) Directive, which came into force in July 2006, required the elimination of lead from electronic equipment, forcing manufacturers to find alternative processes. Some of these replacement processes may be more susceptible to gaseous contamination. For example, creep corrosion has occurred in environments where lead based products performed satisfactorily. OEMs are now pursuing methods to eliminate this aspect of susceptibility. (Schueller 2007).

## Contamination and OEM warranties

OEMs have increasingly been recognising the threat that contamination poses to ICT equipment that they are supplying into data centres. In the US, they have started sending out loss adjusters to audit their clients' data centres before fulfilling claims for warranty equipment failures. If the data centre operator cannot demonstrate that his ICT equipment environment has consistently been kept contamination free to a measured and certified level, his warranty is void and replacement equipment claim denied.

---

## Summary

Contamination can cause a range of ICT equipment problems, including intermittent and permanent failures, overheating and loss of energy efficiency. Problems can be caused by the contaminants' electrical, mechanical and chemical properties. These in turn are controlled by the type of contaminants present, the mixture of airborne PM and gaseous compounds, and the levels of ambient humidity. The type and concentration of contaminants depends on the data centre building's geographical location, external activities, the configuration of the data centre within the building housing it, its construction method and materials, control of human and equipment traffic, and the air handling system.

Some level of contamination is inevitable within a data centre. However it can be measured and reduced with a suitable contamination management strategy to a level safe for the ICT equipment running within. Apart from preventing intermittent faults, more catastrophic failures, overheating and energy losses, a professionally managed and documented contamination control strategy protects data centre operators from warranty voiding problems if equipment does fail.

The next sections in this Handbook discuss applicable standards for classifying contamination, and then methods for its control, measurement and elimination.

---

# Contamination control classification standards and information resources

## The origins of contamination control

The origins of contamination control go back hundreds of years to Swiss watchmakers who, to prevent dust from falling on their sensitive timepieces when they were not being worked on, covered them with a small bell jar.

The American Civil War of 1860 to 1865, with its immense loss of life from bullet wounds, led surgeons to realise the need for preventing post traumatic infection. Work by Lister and other established sterility in operating theatres. In 1945 the need to test gas mask filters against particulate and biological materials led to the development of the aerosol particle counter.

The final step, the High Efficiency Particulate Air (HEPA) filter was developed at Sandia Labs for the Atomic Energy Commission after World War II.

Through the 60s documents such as FED STD 209a, NASA SP-5076, "Contamination Control Handbook", NASA SP-4074, "Clean Room Technology", NASA SP-5045, "Contamination Control Principles", and AF-TO-00-25-203, "Contamination Control of Aerospace Facilities, US Air Force" were written. These documents stated principles which are still relevant today.

## International standards and contamination classification

The above thumbnail history shows how decontamination procedures were developed to overcome specific problems that contamination caused. However, as demands for decontamination became more sophisticated, the establishment of cleanliness measurements and standards became essential. This was so users could be sure that their facilities were decontaminated to a known level sufficient for their operational needs. Accordingly, clean rooms are classified by the cleanliness of their air. Different clean room types must be decontaminated to different classification stringency levels, depending on the nature of their application. Against this background, a data centre can be considered as a clean room requiring a relatively low level of stringency. This

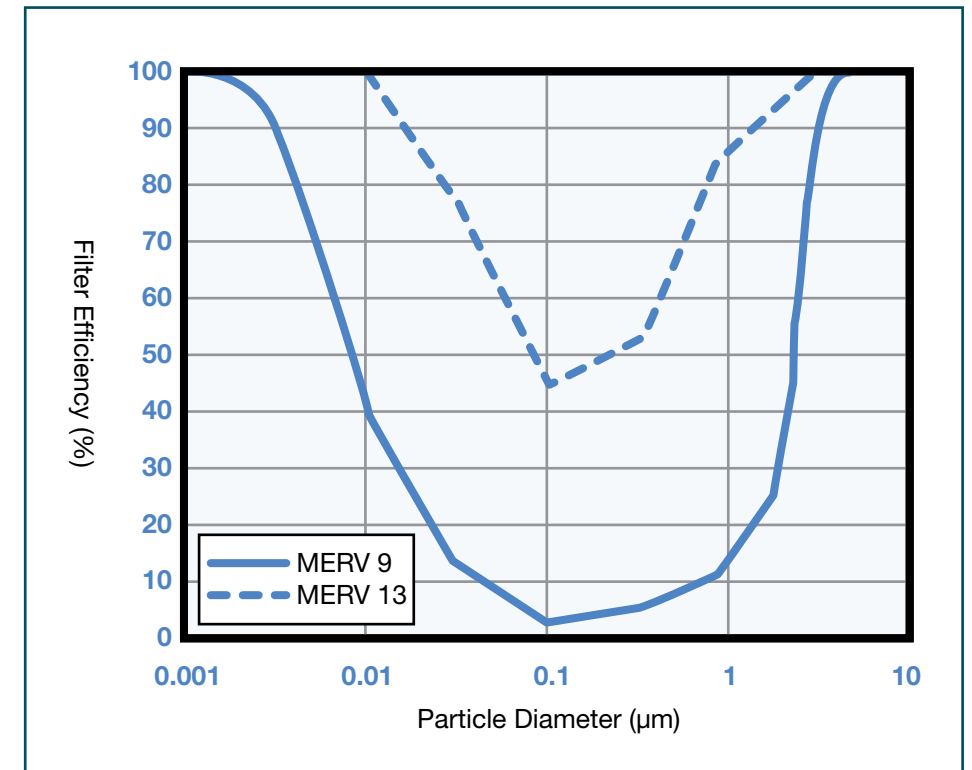
level, although low by clean room standards, must be consistently met to ensure an acceptable decontamination level for the ICT equipment protected by the data centre.



The IT industry now uses ISO 14644-1, Cleanrooms and Associated Controlled Environments – Part 1: Classification of Air Cleanliness (ISO 1999). This international standard was adopted by the European Union in 1999 and the USA in 2001. However, the most easily understood classification of cleanrooms is the obsolete Federal Standard 209 of the USA; it is still widely used. The two standards have much in common. In particular, they are both based on defining air cleanliness in terms of the numbers of particles of different sizes found in a standard volume of air. While a particle's composition determines the nature of its damage potential, its size determines its ability to pass through filters intended to capture it.

### Particle sizing

Particle sizing is significant firstly because it can provide clues for the particles' source, but also because it affects filtration efficiency. Overall, contaminating particles can range in size from 0.001 to more than 100 micrometers ( $\mu\text{m}$  or  $10^{-6}$  m). This range is commonly categorized into three modes; fine mode (0.001 to 0.1  $\mu\text{m}$ ), accumulation mode (0.1 to 2.5  $\mu\text{m}$ ) and coarse mode (2.5–10  $\mu\text{m}$ ). Coarse mode is sometimes extended to include fibres and particles as large as 100  $\mu\text{m}$  and accounts for about 95% of the PM in ambient air. PM in each of these size categories may comprise different materials, come from different sources and vary in airborne suspension lifetime. Combustion generated contamination from sources such as traffic and electricity generation is typically fine and accumulation mode, whereas pollen, human hair and windblown dust are typically coarse mode. Other coarse mode examples include sea salt, natural and artificial fibres. Tobacco smoke is accumulation mode.



Previous measurements have shown outdoor air to be the main source of data centre PM contaminants (Shehabi et al. 2008), but it is possible that events within the data centre's building can potentially contribute to PM concentrations. These mainly comprise coarse mode types such as AHU fan belt wear, toner dust from copiers and printers, occupant hair and clothing, and activities such as unpacking equipment or construction. Zinc whiskers, particularly from floor tiles, are potentially another significant internal source of PM.

The relative proportions of these PM size modes as constituents of an environment's PM matter because their susceptibility to filtration capture varies significantly. Conventional filters can remove coarse mode particles greater than 2.5  $\mu\text{m}$  very efficiently. In fact particles with diameters greater than about 1.0  $\mu\text{m}$  can be filtered effectively because they are too massive to follow the rapidly changing patterns of the airflow through the filter. This allows their capture by the filter fibres. Particles smaller than about 0.1  $\mu\text{m}$  can also be effectively filtered because their small size causes them to drift away from the air stream passing through the filter, and into the filter fibres. However particles in the in-between accumulation mode present a problem because they easily follow the air flow straight through the filters.

Both Federal Standard 209 and ISO 14644-1 recognise these issues. ISO 14644-1 is now the international standard, but its forerunner DEF 209 was popular and is

still widely used today. Therefore a brief coverage of Federal Standard 209 is given before moving on to ISO 14644-1.

### Federal Standard 209

The first Federal Standard 209 was published in 1963 in the USA, and titled Cleanroom and Work Station Requirements, Controlled Environments. It was revised in 1966 (209A), 1973 (B), 1987 (C), 1988 (D) and 1992 (E), and withdrawn in 2001. The cleanroom class limits, given in the earlier 209 A to D versions, are shown in Table 4.1. The class of a cleanroom is found by measuring the number of particles of various sizes in one cubic foot of room air, and determining which class limit is not exceeded; this is the cleanroom classification.

Table 4.1 Federal Standard 209 class limits

| Class   | Particles / ft <sup>3</sup> |           |           |           |           |
|---------|-----------------------------|-----------|-----------|-----------|-----------|
|         | >= 0.1 µm                   | >= 0.2 µm | >= 0.3 µm | >= 0.5 µm | >= 5.0 µm |
| 1       | 35                          | 7.5       | 3         | 1         | N/A       |
| 10      | 350                         | 75        | 30        | 10        | N/A       |
| 100     | N/A                         | 750       | 300       | 100       | N/A       |
| 1,000   | N/A                         | N/A       | N/A       | 1,000     | 7         |
| 10,000  | N/A                         | N/A       | N/A       | 10,000    | 70        |
| 100,000 | N/A                         | N/A       | N/A       | 100,000   | 700       |

In the last edition of Federal Standard 209 (E) the airborne concentrations in the room was also given in metric units, i.e. per m<sup>3</sup>. This nomenclature never became established, and was only used in the occasional published article. The earlier version's nomenclature shown in table 4.1 continues to be used and is likely to be used by some operators for many years. Data centres typically aim to comply with Class 100,000.

### ISO Standard 14644-1

Compared with Federal Standard 209, ISO 14644-1 uses new class designations, uses a metric measure of air volume, and adds three new classes. Other ISO 14644 standards (-02 to -08) concern other aspects of air cleanliness, including an introduction to cleanroom design, construction and start-up considerations and operations. ISO 14644-2 is concerned with requirements for monitoring a clean room or clean zone, and for verifying its continued compliance with ISO 14644-1.

Update: ISO 14644 now includes nine standards, as this update advises.

### ISO 14644-9 Final Draft International Standard Released

The updated document has been refined and reorganized for greater efficiency and ease of use. This new Standard describes the classification of particle

contamination levels on solid surfaces in cleanrooms and associated controlled environment applications.

Table 4.2 below shows the ISO 14644 Air Cleanliness Classifications in terms of maximum particle concentrations allowed for different particle sizes.

Against the ISO 14644-1 Classes, data centres are required to reach Classes 7–9, most usually Class 8.

Table 4.2: ISO Air Cleanliness Classifications

| ISO Class | Max. no. of particles in each cubic metre of air equal to or greater than the specified size |          |          |           |           |         |
|-----------|--|----------|----------|-----------|-----------|---------|
|           | Particle size  |          |          |           |           |         |
|           | > 0.1 µm   | > 0.2 µm | > 0.3 µm | > 0.5 µm  | > 1 µm    | > 5 µm  |
| Class 1   | 10   | 2        |          |           |           |         |
| Class 2   | 100  | 24       | 10       | 4         |           |         |
| Class 3   | 1000   | 237      | 102      | 35        | 8         |         |
| Class 4   | 10,000   | 2370     | 1020     | 352       | 83        |         |
| Class 5   | 100,000  | 23,700   | 10,200   | 3520      | 832       | 29      |
| Class 6   | 1,000,000  | 237,000  | 102,000  | 35,200    | 8320      | 293     |
| Class 7   |  |          |          | 352,000   | 83,200    | 2930    |
| Class 8   |  |          |          | 3,520,000 | 832,000   | 29,300  |
| Class 9   |  |          |          |           | 8,320,000 | 293,000 |

Table 4.3: Comparison between selected equivalent classes of Federal Standard 209 and ISO 14644-1

| ISO 14644-1 Classes | Class 3 | Class 4 | Class 5 | Class 6 | Class 7 | Class 8 |
|---------------------|---------|---------|---------|---------|---------|---------|
| FS 209 Classes      | 1       | 10      | 100     | 1000    | 10,000  | 100,000 |

## Guidelines for assessing gaseous contamination

Standards such as IEC 60271-3-3 (IEC 2002), which include gaseous composition environmental limits, were developed primarily for telephone switching centres. The standard most relevant to data centres is the International Society of Automation's ANSI/ISA S71.04-1985, Environmental Conditions for Process Measurements and Control Systems: Airborne Contaminants (ISA 1985). This classifies the level of airborne contaminants that are safe for electronic equipment, including gaseous contamination.

The standard establishes environmental corrosion levels by measuring the rate of corrosion buildup in terms of corrosion thickness over time measured in Angstroms (one ten-billionth of a metre) using copper coupon strips and then categorizing the severity into one of four classes: G1, G2, G3 or GX as shown in Table 4.4 and Table 4.5.

Table 4.4: ISA Corrosion Class Levels (ISA 1985)

| ISA Class | Level    | Description  |
|-----------|----------|--|
| G1        | Mild     | Corrosion is not a factor in determining equipment reliability |
| G2        | Moderate | Corrosion is measurable and may be an issue in five years      |
| G3        | Harsh    | Corrosion will probably occur within five years                |
| GX        | Severe   | Only specifically designed and packaged equipment will survive |

Table 4.5: Corrosion buildup in ISA Classes

| ISA Class | Corrosion buildup in 30 days |
|-----------|------------------------------|
| G1        | <300 Å                       |
| G2        | <1000 Å                      |
| G3        | <2000 Å                      |
| GX        | >2000 Å                      |

There are some points to bear in mind when assessing the potential of an atmosphere to inflict corrosive damage:

- Predicting corrosion is complicated by the synergy between gases. While hydrogen sulphide (H<sub>2</sub>S) is relatively non corrosive to silver, H<sub>2</sub>S combined with nitrous oxide (N<sub>2</sub>O) is very corrosive to silver. (Volpe and Peterson 1989). Similarly, while neither sulphur dioxide (SO<sub>2</sub>) nor nitrous oxide (N<sub>2</sub>O) alone are corrosive to copper, together they attack copper at a very rapid rate (Johansson 1985).
- Since the advent of RoHS, electronics manufacturers have been forced to find other manufacturing materials instead of lead. Data centres in urban areas have been reporting failures of the resulting equipment in the presence of small quantities of atmospheric sulphur and chlorine. This has prompted ISA to revise S71.04-1985 to include silver corrosion in its severity levels.

There is still much study and research to be done in understanding how the combined results of composition, concentration and the thermal environment impact ICT equipment as the industry works towards a single set of limits. Until then, limits from ISA and other sources will remain subject to caveats and exceptions.

## Information sources

Operators responsible for data centre decontamination may wish to purchase the full ISO, Federal or ISA standards. There is also an international confederation of societies that promote interest in cleanroom technology. Accordingly, contact details for the relevant organisations appear below:

**ISO 14644** is generated and published by The International Organization for Standardization (ISO) which can be contacted at the address below:

### ISO Central Secretariat

International Organization for Standardization (ISO)  
 1, ch. de la Voie-Creuse,  
 Case postale 56  
 CH-1211 Geneva 20, Switzerland  
 Tel: +41 22 749 01 11  
 Fax: +41 22 733 34 30  
 Email: sales@iso.org  
 Web: www.iso.org

Within the UK, information about ISO standards is available from The British Standards Institution:

### BSI

389 Chiswick High Road  
 London. W4 4AL  
 United Kingdom  
 Tel: +44 (0)20 8996 9001  
 Fax: +44 (0)20 8996 7001  
 Email: cservices@bsigroup.com  
 Web: www.bsigroup.com

Federal Standard 209 has been replaced by ISO 14644, but it is still in use throughout the world. The Standard is available from IEST:

### IEST – Institute of Environmental Sciences and Technology

Arlington Place One  
 2340 South Arlington Heights Road, Suite 100  
 Arlington Heights, IL 60005-4516  
 Tel: +1 (847) 981-0100  
 Fax: +1 (847) 981-4130  
 Email: information@iest.org  
 Web: www.iest.org

---

---

## Information sources

### **ISA – International Society of Automation**

ISA

67 Alexander Drive

PO Box 12277

Research Triangle Park, NC 27709

Tel: +1 (919) 549-8411

Fax: +1 (919) 549-8288

Email: [info@isa.org](mailto:info@isa.org)

Web: [www.isa.org](http://www.isa.org)

To keep up to date with developments in clean room technology you can refer to a member society of the **International Confederation of Contamination Control Societies (ICCCS)**, of which the IEST (above) is one. The UK member societies are:

### **SEE – Society of Environmental Engineers**

The Society of Environmental Engineers

The Manor House,

High Street,

Buntingford,

Herts. SG9 9AB.

UK

Tel: + 44 (0)1763 271209

Fax: + 44 (0)1763 273255

Email: [office@environmental.org.uk](mailto:office@environmental.org.uk)

Web: <http://environmental.org.uk>

### **ICS – Irish Cleanroom Society**

Web: [www.cleanrooms-ireland.ie](http://www.cleanrooms-ireland.ie)

### **S2C2 – The Scottish Society for Contamination Control**

Scottish Society for Contamination Control

272 High Street

Glasgow

G4 0QT

Tel: +44 844 800 7809 or +44 141 552 8180

Email: [admin@s2c2.co.uk](mailto:admin@s2c2.co.uk)

Web: <http://www.s2c2.co.uk>

---

---

## Summary

In this chapter we have seen how international standards have developed for classifying particulate contamination levels in clean rooms. These standards have culminated in ISO 14644-1, although the earlier Federal Standard 209E is still in use. A data centre can be kept sufficiently contamination free for the safety of its ICT equipment by meeting a relatively low stringency ISO 14644 or 209E class. These standards define the maximum allowable concentration of different sized particles within the cleanroom environment.

For gaseous contamination, standards more specific to data centres and ICT equipment have been developed, in particular ISA standard S71.04-1985, which estimates the potential of a given level of gaseous contamination to cause corrosion in electronic equipment. Understanding gaseous contaminants and how they interact with one another, particulate contaminants and related environmental conditions is still subject to ongoing research.

The development of these standards highlights the inevitable existence of particulate and gaseous contaminants within data centre environments. The next chapter looks at the measures that can be taken to minimise their access to vulnerable ICT equipment.

---

# A 'whole life' strategy for contamination management

We have now defined what contamination is, why it's a threat, and how it can be classified. Next, we need to know how to stop this contamination reaching and damaging our ICT equipment.

The best possible contamination strategy has four elements:

- Firstly, minimise contamination access to the data centre through intelligent location, design and construction;
- Secondly, design and install a suitable HVAC and filtration system;
- Thirdly, minimise its ongoing ingress by enforcing rigorous operations and security procedures;
- Fourth, maintain a carefully profiled decontamination and monitoring schedule to remove the contamination that inevitably penetrates into data centres, even with the most strenuous effort to prevent it.

This strategy starts before the data centre is even built, and continues until the end of its operational life.

---

# Data centre location, design and construction

## Geographical location of facility

Selecting the site for a data centre, and considering all the internal and external hazards, is an important exercise. Firstly, consider contamination risks from any activities near the site for the proposed new or relocated data centre. Risks can arise from agricultural, chemical, biological, nuclear and manufacturing processes, storage and waste treatment operations. Other critical factors include susceptibility to floods, tornadoes, volcanoes or other acts of nature. Transportation activity, particularly commercial transportation such as heavy lorries and trains passing close to the facility, present a contamination threat. A similar threat arises from airport operations and overhead aircraft flight paths. The environment we live in makes a completely risk-free location for a data centre facility very difficult to find. In practice, the choice of site is usually a 'best fit' compromise.

Protection from severe weather events is costly, but important. Data centres must allow for these in terms of design as well as location. In flood-prone areas, it may be necessary to locate all of the ICT hardware and its associated vulnerable equipment on an upper floor in case the ground floor of the facility is flooded. In areas prone to tornadoes and hurricanes, it may be important to orientate the building and adjust its design to survive high winds.

Even without storm threats, a building's physical location can significantly affect the contamination levels within the data centre. Particulate matter, airborne or otherwise can and will penetrate buildings through cracks, makeup air, and on people and materials entering the facility.

Urban locations have man-made pollutants such as petrochemical materials from car tyres, soot from combustion equipment, dust and debris from construction sites and many other activities. Rural locations may have more dust from loose soils and vegetation. Vacant areas and open spaces can suddenly become building sites, creating new contamination problems. Whatever the location, changes in wind direction and pressure will affect both the level of airborne contamination and its level of infiltration into the data centre building.

Vibration is another consideration, as it can cause building components to shift to dislodge existing contamination particles or create more. Road traffic, trains, aeroplanes and nearby building work can all cause vibration. Urban locations are more susceptible, but the problem arises in rural locations as well.

---

---

## Locating the computer room within the building

Hazards exist within buildings as well as outside; these should be allowed for when locating the data centre within the facility. It should be physically separate from spaces continuously occupied by building users. Dining rooms, cafeterias and toilets located above, or boiler rooms, steam pipes and garages adjacent to or below a data centre can increase its contamination level. This can be further aggravated by an accident, vandalism or act of terrorism.

Preventing contamination from entering a data centre is much more effective as well as lower cost than remediating if it does. Therefore strict data centre practices should be set up and followed to minimise contaminant ingress caused by daily activity. Food and drink must be forbidden from the room at any time. Crumbs from food, or spilled drinks, create a tangible hazard. Additionally, allowing food or drink creates a careless attitude towards other contaminants. Cardboard boxes and ICT equipment manuals should be stored in a designated location outside the data centre. Paper is a source of contamination, and it also becomes fuel in the event of a fire. Facility operators must provide a staging area for packing and unpacking equipment to support upgrade, expansion or repair operations. Tak mats should be installed immediately adjacent to any entrances into the data centre to capture dirt from shoes. The mats' resin impregnated layers should be regularly removed as they become soiled through use to ensure their continued effectiveness.

Once its location within the building is decided, the location of any openings into the data centre must be specified. As any opening will allow contamination ingress, windows – especially if they open onto the exterior – should be avoided. Exterior windows raise further problems of sunlight heat loading, and an increased security threat. If exterior windows cannot be avoided, they should be located in the lee of the building, particularly in high-wind areas. Doors into the data centre should be isolated in an attempt to establish an airlock. No door onto the building exterior should ever be open at the same time as any data centre entrance door. Contaminant influx can also be reduced through positive pressurisation from conditioned makeup air, air showers or vestibules.

### **Attached or adjacent staging areas**

Deliveries of equipment from time to time are inevitable, and this must be handled and unpacked before installation. Accordingly a staging area must be provided to allow such equipment to be unpacked, cleaned, prepared and taken into the data centre without packing material or any other unnecessary source of contamination. This staging area should be physically separate from the data centre with no air exchange allowed.

---

---

### **Attached or adjacent storage areas**

ICT equipment generates a need for spare parts and supplies. Additional, replacement or recycled systems may also need catering for. However used computers, cable reels, cardboard boxes, paper or other particulate matter (PM) sources should be kept away from the data centre in a separate storage area. It should also be possible to clean any items taken from this area before taking them into the data centre.

If equipment is packed in plastic for transport, this should be removed before allowing the equipment into the data centre. Plastic's static properties cause accumulation of PM which can be released within the data centre, especially as it is removed from the equipment.

### **Movement of people, equipment and materials**

A flow of people, equipment and materials into and out of the data centre is inevitable, so its effects must be mitigated as far as possible. The data centre environment should allow efficient trolley and foot journeys, as longer distances allow more dirt pickup by shoes and trolley wheels, which will be carried into the equipment area. Therefore, the Tak mats should be used for trolley wheels as well as shoes, and use of the data centre as a short cut to other locations should be prevented.

### **Office and operations areas**

People generate and carry large quantities of PM, so limiting the need for people to work in the data centre is essential. All operators and technicians should have a desk or operations area adjacent to but outside the data centre. If the operations area has direct doorway access to the data centre, it should be relatively negatively pressurised. Only personnel who need to work directly on the equipment should be given access to the data centre.

### **Considerations for computer room materials**

Many materials are available for designing and building data centre environments. Although their PM characteristics may not always be a primary factor in their choice, they are important. Not all materials selected for a data centre will be optimised for their PM properties. A trade-off between PM properties, cost and safety is usually necessary. However when making these choices, the cost of the materials should be compared with the value not only of the ICT equipment they will be housing, but also of the data it contains. Loss of access to the data, or worse, the data itself, would be catastrophic for the organisations relying on the data centre facility.

### **Computer room materials – wall, ceiling, underfloor and surfaces**

Construction materials such as metal, glass and plastic are good in terms of PM because they emit little or no contaminants. However, although these materials are used in some

---

---

areas, they are typically not found in wall, ceiling or floor coverings because of cost or other limitations. Instead, most data centres utilize concrete floors, drywall walls and cellulose suspended ceiling tiles. Unfortunately each of these materials generates significant PM, particularly as they are stressed during construction work. They will continue to generate PM even after construction work is finished as a result of vibration or abrasion factors.

**Underfloor seal or coating:** Concrete materials such as blended cements are ubiquitous in modern construction and used in almost every data centre environment. However these materials are also a potential source of dangerous contaminants. Exposed concrete continuously oxidises, breaking down the surface. This surface breakdown creates loose sand and lime PM, and lime dust is particularly corrosive when mixed with water or humidified. Therefore, sealing is essential to prevent disintegration of concrete surfaces. Ideally, the seal is installed before the raised-access floor is installed, but it can be applied to an existing installation. Even in an existing facility, some protection is better than none. Select a water based, volatile organic compound (VOC)- compliant sealant specifically designed for data centre applications. Most new concrete materials are treated with a curing agent to help harden the concrete, producing a better surface. These agents are often called surface sealers, although they tend to sink into the concrete rather than remaining on the surface as a surface protector.

A simple evaluation will show the existence or condition of a concrete surface sealant. This is particularly useful during acceptance testing of a new data centre facility. This examination, described below, should be carried out using safety equipment comprising at least protective glasses and hand protection.

- Using plain water, clean a 152.4 mm (6 in) diameter circle on the concrete surfaces to be evaluated, to remove any surface contamination.
- Apply two to three drops of muriatic acid on the concrete surface in the circle centre.
- If the muriatic acid remains on the concrete surface with the appearance of water, the concrete is adequately sealed for dust encapsulation purposes.
- If the muriatic acid reacts with the concrete by producing a clear or yellowish foam, the concrete is not adequately sealed. **Warning!** Do not breathe the vapour produced by the reaction.
- Clean the muriatic acid from the concrete test area, and properly dispose of the hand protection gloves as well as the clean-up wipes.
- **NOTE!** Muriatic acid is dangerous if not properly used. Do not pour more than two to three drops of acid onto the concrete floor surface. Unsealed concrete together with large quantities of acid will produce a large reaction and dangerous quantities of fumes.

---

---

**Wall coverings:** Most data centres are built using painted drywall – also called gypsum board or wall board – partition walls. These are a good choice with low PM emission, provided the drywall surface is properly prepared and high-quality paint used. This prevents the surface from chalking or rubbing off. Care must also be taken to ensure all drywall edges are properly sealed or covered, for example around outlets and other surface penetrations. Unused or abandoned holes or surface penetrations should be also be patched and painted.

Other types of wall construction and coverings are found in data centres. Fabric and other porous surfaces are not recommended, as these may capture and emit contaminants from the basic material. Such surfaces are also difficult to clean. Also, all wall coverings and surface finishes must comply with applicable local building and fire codes.

**Ceiling tiles and spaces:** Ceiling tiles can also contribute significantly to data centre contamination. Most commercially available lay-in ceiling tiles are unsuitable for data centre use since they are made from cellulose, which breaks easily into small fragments. Small movements of the panels, either intentional or through vibration can cause the panel edges to chip and break.

Panels with smooth surfaces and wrapped or encapsulated edges are acceptable: These are commonly used in food service kitchen and preparation areas. The ceiling space may also have exposed concrete: This must be sealed in the same way as the concrete underfloor area to prevent oxidation and liberation of concrete dust into the airstream. Also, any spray-on fire insulation, commonly applied to structural steel, must be sealed as it is a source of PM.

**Zinc Whiskers:** Besides metal shavings and rust particles, the most common electrically conductive contaminants found in raised-access floor areas are zinc whiskers. Zinc-whisker growth has been documented on a wide range of zinc-coated ICT equipment and raised-access floor support products. These include the underside of zinc-plated raised-access floor panels, pedestal and stringer support structures, and associated mechanical assembly hardware. Wood core and concrete panels with flat steel bottoms are most susceptible. The steel surfaces may be zinc coated either with a hot-dip galvanisation process or an electropassivation electroplating surface. Hot-dip galvanised steel typically has a spangled ‘glittery’ or mottled ‘spotted’ appearance similar to the finished surface of a tin bucket. This method of plating is generally considered to be immune from to whisker growth. However electroplated zinc typically has a uniformly dull grey appearance and will develop crystalline growths, or whiskers, of pure zinc perpendicular to the panel’s plated surface. If these small metallic particles, which are typically 0.5–1 mm in length, are dislodged from their source and into the data centre’s air stream, they

---

---

---

---

---

---

---

---

---

---

can penetrate ICT equipment through its air intakes. Here, they can cause unwanted bridging and short circuits between conductors within the equipment. This equipment can include power supplies as well as the data processing hardware, and these tend to fail in a dramatic fashion with audible popping sounds when zinc whiskers arc across high-voltage or high-current conductors.

In fact almost all electroplated zinc surfaces are potential whisker sources. Data centre sources where they have been found include:

- Raised-access floor panels, pedestals, stringers and pedestal heads.
- Steel building studs.
- Suspended ceiling T-grid components and hanger wires.
- Thin wall electrical conduit.
- ICT equipment racks and cabinets.
- ICT equipment cases and enclosures.

**Tin Whiskers:** Similar to zinc whiskers, tin whiskers are tiny, electrically conductive, pure-metal, hair-like crystalline structures that grow on components and products having electroplated tin as a final surface finish. Tin whiskers can grow in abundance, causing bridging and shorting between electrical conductors and component terminations. Exposed leads on electronic components are commonly coated with tin or a mixture of tin-lead to prevent corrosion and enhance solderability.

As more manufacturers move towards restriction of hazardous substances (RoHS) compliance, they are required to remove lead elements from the plating formula. Today, most lead-free electronic component terminations are plated using a pure tin plating process – and this is a common source of tin whisker growth. There have been many documented instances of where tin whisker growth on components has led to failures inside the ICT equipment. A good source of tin whisker information can be found on the U.S. National Aeronautics and Space Administration (NASA) website on <http://nepp.nasa.gov/whisker/>.

The cause of the tin and zinc whisker growth mechanisms is not known or well understood. Many component manufacturers and plating industry professionals have developed effective ways to work around them by modifying the plating solution with other materials. Nonpure metals tend to be less susceptible to whisker growth.

**Fit and finish:** Data centre contamination can be increased by improperly fitted and finished interiors. The amount of air moving through building cracks can be significant, and this can bring contamination either from outside the building, or from contaminated areas within. Positive pressurisation of the data centre relative to the

---

---

---

---

---

---

---

---

---

---

rest of the building can mitigate this problem. However, air conditioning systems are not usually equipped to provide this while overcoming numerous or large air leaks. Instead, such leaks bleed conditioned air from the data centre. Areas of significant concern include:

- **Ceiling** – should be sized to fit snugly at the sides and ends within the grid. Broken or chipped panels will allow air from other building areas to enter the data centre.
- **Drywall** – should be adequately caulked to the slab at its base and to the roof or slab of the adjacent floor. Building movement and expansion, as well as fire rating should be allowed for when choosing materials and caulk.
- **Columns** – these can generate significant airflows due to the chimney effect. These can carry contaminants into the data centre.

---

---

# HVAC Systems

The HVAC system found in any facility can be considered as part of the data centre room's construction. As such it is a potential source of both particulate and gaseous contamination.

## Makeup air

Fresh makeup air is a building code requirement for installations with human occupants. A typical commercial HVAC installation has minimal filtration of outside air before it is mixed into the return airstream, conditioned and supplied back into the environment. It is not unusual to find the same approach used in HVAC systems servicing data centre applications. However if such systems do not properly filter the outside air, the ICT equipment could become contaminated with all the outside air pollutants. Lack of adequate filtration would be disastrous for ICT and related support equipment if the outside air is heavily polluted. The nature and depth of air pollution varies from country to country, and between regions within countries. Pollution risks are greater within countries that do not have pollution standards. Local or regional authorities should be consulted for updated information about outside ambient conditions.

Local authorities in the UK have statutory duties for managing local air quality under Part IV of the Environment Act 1995 and in Northern Ireland, Part III of the Environment (Northern Ireland) Order 2002. They are required to carry out regular reviews and assessments of air quality in their area against standards and objectives prescribed in regulations for the purpose of local air quality management (LAQM) before undertaking Action Planning if air quality is found to breach the regulations.

## Positive pressurisation

Positive pressurisation helps prevent contaminated air from entering the data centre environment. Using positive pressurisation with outside air not only keeps out particulate contaminants but also controls corrosive gases and volatile organic compounds (VOCs). Even though most installations in typical commercial, business or clean industrial locations have an adequate quality of surrounding air, any air entering the data centre should be conditioned and filtered to ensure that its ICT equipment specifications for temperature, humidity and cleanliness are met.

---

---

# Humidification systems

The American Society of Heating, Refrigerating and Air Conditioning Engineers (ASHRAE) has published *Thermal Guidelines for Data Processing Environments*, Second Edition (ASHRAE 2009b) which includes updated recommendations for an environmental envelope suitable for data centre equipment. These specify that the relative humidity in a Class 1 data centre be controlled with a lower-bound dew point of 5.5°C and an upper-bound dew point of 15°C, or 60% relative humidity. ASHRAE Environmental Class 1 is defined as a data centre with tightly controlled environmental parameters, specifically dew point, temperature and relative humidity. Most facilities achieve the necessary humidification through special purpose humidifiers. Several technologies exist, with various trade-offs between water quality, maintenance and contamination. Because standard tap-water is rarely suitable for use in humidification systems, care is required in matching the water quality and associated treatment equipment to the selected humidifier. Water contains particles, bacteria, dissolved solids and a wide range of chemicals. These impurities can affect the humidification system and its performance. Many of the impurities remain in the water when it is converted to vapour. The question is whether to remove the impurities in the purification stages, or after they have been deposited in the humidification equipment itself, which requires more frequent maintenance.

There are five categories of water that can be used to supply the humidifier:

- **Potable water.** Which has no treatment other than filtration. Using this will significantly increase maintenance and repair costs.
- **Softened water.** This is a viable source for humidification. Water softeners are reasonably easy and low cost to run. As such they can be the ideal choice for smaller data centres.
- **Reverse osmosis.** This eliminates the majority of water borne contaminants, and provides suitable feed water for humidifiers. The process uses less chemical product than water softeners, and reduces humidifier maintenance and downtime, but it does consume considerably more water.
- **Deionisation.** This process is typically the most complex but it produces the highest quality and purist water. Very pure deionised water is an aggressive fluid. It loses this aggression on exposure to air, but it can pose a risk to some materials. Therefore, the humidifier supplier should be consulted about material compatibility if deionised water is to be used.
- **Boiler feed water systems.** These exist in many larger facilities. Generally their water, with a reduced level of contamination, is suitable for humidification systems. However, the specific water chemistry must be checked and compared to the humidification system requirements.

Any water treatment or humidifier system benefits from regular operation. It is best to rinse the system prior to use and to implement the humidifier manufacturer's recommended cleaning, operation and maintenance practices. The sizing of the water softener, reverse osmosis or deionisation system depends on both the water flow rate and the total amount of dissolved solids in the feed water. The specific manufacturer's guidance should be followed. More information is also available from ASHRAE ([www.ashrae.org](http://www.ashrae.org)).

Humidity can impact the rate of corrosion in the data centre environment as the corrosion process produces PM. In general, conductive anodic filament growth, deliquesce of hygroscopic salts or condensation can occur on computer components if the humidity level is too high.

## Air Filtration

Filtration is an integral part of any air movement device that may be part of the equipment, added to an existing system, or a standalone unit such as an electrostatic filter. Filtration and air-cleaning removes unwanted PM and gaseous materials from the airflow paths in the computer room. Some level of air filtering is essential in data centre environments. Filtering may be applied to recirculated air using the computer room air-conditioning (CRAC) units, in makeup air from the outside environment, and in some ICT equipment. In HVAC applications, this involves air filtration and in some cases, air cleaning for gas and vapour removal.

Filters can be classified by their Minimum Efficiency Reporting value or MERV rating. MERV is used to rate the ability of an air cleaner filter to remove dust from the air as it passes through the filter. MERV is a standard used to measure the overall efficiency of a filter. The MERV scale ranges from 1 to 20, and measures a filter's ability to remove particles from 10 to 0.3 micrometres in size. Filters with higher ratings not only remove more particles from the air, they also remove smaller particles. ASHRAE provides detailed information on MERV ratings and their meaning for particle removal as described [overleaf](#).

The ASHRAE filter standard ANSI/ASHRAE Standard 52.2-2007, Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size (ASHRAE 2007a) is currently used to rate filters based on their collective efficiency, pressure drop and particulate-holding capacity. This standard measures arrestance, dust spot efficiency and dust holding capacity. Arrestance is a measure of filter's ability to capture a mass fraction of coarse dust, and dust efficiency is the ability to capture particles within a given size range. ASHRAE Standard 52.2 also measures particle size efficiency expressed as a minimum efficiency reporting value (MERV) between 1 and 20. Particulate filters with a MERV rating of 8 are recommended as a minimum in ANSI/ASHRAE Standard 127-2007, Method of Testing for Rating Computer and Data Processing Room Unitary Air Conditioners (ASHRAE 2007b) and are commonly available for CRAC units. A MERV 11 or 13 filter should be used

with air-side economisers or makeup air units. ANSI/ASHRAE Standard 62.1-2007, Ventilation for Acceptable Indoor Air Quality (ASHRAE 2007c) recommends at least a MERV 6 filter upstream of all cooling coils and in outside air units in areas where PM10 is exceeded.

Higher efficiency filtration may be necessary for some ICT equipment environment installations. Filtration always impedes the airflow through the air-conditioning system as well as through ICT and infrastructure equipment; facility and equipment designs must allow for this filter impedance. Filters should be inspected, replaced or cleaned at scheduled intervals to minimise airflow impedance. Some ICT equipment uses active alarming based on differential pressure to indicate when filters need servicing. Manufacturers' guidelines may not be accurate because of wide variations in the severity of data centre environment conditions. For example if significant concentrations of VOCs are present, activated charcoal or permanganate-based filters may be necessary to reduce the VOCs to an acceptable environmental level.

Table 6.1: MERV values from ASHRAE Standard 52.2

| ASHRAE 52.2 (ASHRAE 2007a) |         |         |          |            |           |           |
|----------------------------|---------|---------|----------|------------|-----------|-----------|
| MERV                       | 3–10 µm | 1–3 µm  | 0.3–1 µm | Arrestance | Dust Spot | Dust Spot |
| 1                          | <20%    | –       | –        | <65%       | <20%      |           |
| 2                          | <20%    | –       | –        | 65%–70%    | <20%      | >10 µm    |
| 3                          | <20%    | –       | –        | 70%–75%    | <20%      |           |
| 4                          | <20%    | –       | –        | >75%       | <20%      |           |
| 5                          | 20%–35% | –       | –        | 80%–85%    | <20%      |           |
| 6                          | 20%–50% | –       | –        | >90%       | <20%      | 3–10 µm   |
| 7                          | 20%–70% | –       | –        | >90%       | 20%–25%   |           |
| 8                          | <70%    | –       | –        | >95%       | 25%–30%   |           |
| 9                          | <85%    | <50%    | –        | >95%       | 40%–45%   |           |
| 10                         | <85%    | 50%–65% | –        | >95%       | 50%–55%   | 1–3 µm    |
| 11                         | <85%    | 65%–80% | –        | >98%       | 60%–65%   |           |
| 12                         | >90%    | >80%    | –        | >98%       | 70%–75%   |           |
| 13                         | >90%    | >90%    | <75%     | >98%       | 80%–90%   |           |
| 14                         | >90%    | >90%    | 75%–85%  | >98%       | 90%–95%   | 0.3–1 µm  |
| 15                         | >90%    | >90%    | 85%–95%  | >98%       | ~95%      |           |
| 16                         | >95%    | >95%    | >95%     | >98%       | >95%      |           |
| 17*                        | >99%    | >99%    | >99%     | –          | >99%      |           |
| 18*                        | >99%    | >99%    | >99%     | –          | >99%      | 0.3–1 µm  |
| 19*                        | >99%    | >99%    | >99%     | –          | >99%      |           |
| 20*                        | >99%    | >99%    | >99%     | –          | >99%      |           |

\* Filters viruses and carbon dust

---

---

## High Efficiency Air Filtration and HEPA filters

As the MERV table above shows, a filter's rating depends on its efficiency in capturing particles of different sizes. Many data centres use High Efficiency Particle Air (HEPA) filters. A HEPA filter must have an efficiency of at least 99.97% in removing small micro-organisms and inert airborne particles of approximately 0.3 µm. HEPA filters are recommended for cleanrooms with ISO Class 6 and poorer quality. This includes data centres, which normally fall within ISO Classes 7 to 9.

HEPA filters are composed of a mat of randomly arranged fibres. The fibres are typically composed of fibreglass and possess diameters between 0.5 and 2.0 micrometer. Key factors affecting the filter function are fibre diameter, filter thickness, and face velocity. The air space between HEPA filter fibres is much greater than 0.3 µm. The common assumption that a HEPA filter acts like a sieve where particles smaller than the largest opening can pass through is incorrect. Unlike membrane filters, where particles as wide as the largest opening or distance between fibres cannot pass in between them at all, HEPA filters are designed to target much smaller pollutants and particles. These particles are trapped (they stick to a fibre) through a combination of the following three mechanisms:

- 1 Interception**, where particles following a line of flow in the air stream come within one radius of a fibre and adhere to it.
- 2 Impaction**, where larger particles are unable to avoid fibres by following the curving contours of the air stream and are forced to embed in one of them directly; this effect increases with diminishing fibre separation and higher air flow velocity.
- 3 Diffusion**, an enhancing mechanism is a result of the collision with gas molecules by the smallest particles, especially those below 0.1 µm in diameter, which are thereby impeded and delayed in their path through the filter; this behaviour is similar to Brownian motion and raises the probability that a particle will be stopped by either of the two mechanisms above; it becomes dominant at lower air flow velocities.

Diffusion predominates below the 0.1 µm diameter particle size. Impaction and interception predominate above 0.4 µm. In between, near the Most Penetrating Particle Size (MPPS) 0.3 µm, both diffusion and interception are comparatively inefficient. Therefore, the HEPA specifications use the retention of these particles to define the filter.

---

---

### HEPA Specifications

HEPA filters, as defined by the DOE standard adopted by most American industries, remove at least 99.97% of airborne particles 0.3 micrometers (µm) in diameter. The filters maximum resistance to airflow, or pressure drop, is usually specified around 300 Pa at its nominal flow rate.

The specification usually used in the European Union is the European Norm EN 1822-1. It defines several classes of HEPA filters by their retention at Most Penetrating Particle Size (MPPS).

### HEPA Filter Testing

High efficiency filters are tested after manufacture to measure their efficiency against test particles. A number of test methods across Europe and North America are commonly used. These include:

#### Military Standard 282

This USA test originally used thermally generated particles of di-octyl phthalate (DOP) with an average size of 0.3 µm to test HEPA filter efficiency. However, other oils such as poly-alpha olefin (PAO) or di-octyl sebacate (DOS) have replaced DOP. Heating these oils produces an oil mist, and the filter's efficiency against this challenge is determined.

#### Sodium Flame Test (Eurovent 4/4)

This European method for HEPA filters uses an aerosol of sodium chloride particles with a mass median size of 0.6 µm. The test aerosol is sprayed into the air as an aqueous solution and the dry particles so formed are used to determine the filter's efficiency.

#### European Standard EN 1822

This standard is used for both HEPA and Ultra Low Penetration Air (ULPA) filters and describes a method for testing the particle removal efficiency and classifying the filter.

This method includes a determination of the Most Penetrating Particle Size (MPPS) for the filter media being tested, and a measurement of the removal efficiency for that particle size. Each filter has a particular particle size that will pass through it most easily. This size is determined by variables such as the fibre content of the filter media, air velocity and its packing density. It is therefore logical to test the filter at that most penetrating particle size. The MPPS is usually between 0.1 µm and 0.3 µm.

The first stage of this test method is to determine the MPPS of the flat sheet filter medium used in the filter. This is performed at the face velocity corresponding with that produced by the filter when working at its given flow rates. The efficiency of the complete filter can then be found in two ways:

- Leak testing (local efficiency). The filter media of the complete filter is scanned to determine the amount of leakage through pinholes in the filter medium.
- Overall efficiency. The efficiency of the complete filter is determined at its rated flow.

The filter is then classified by its overall and local efficiency against its most penetrating particle.

Table 6.2: Filter housing for high efficiency filters

| Filter Class | Overall value efficiency (%) | Overall value penetration (%) | Leak test efficiency (%) | Leak test penetration (%) |
|--------------|------------------------------|-------------------------------|--------------------------|---------------------------|
| H10          | 85                           | 15                            | –                        | –                         |
| H11          | 95                           | 5                             | –                        | –                         |
| H12          | 99.5                         | 0.5                           | –                        | –                         |
| H13          | 99.95                        | 0.05                          | 99.75                    | 0.25                      |
| H14          | 99.995                       | 0.005                         | 99.975                   | 0.025                     |

When a filter leaves the factory where it has been manufactured and tested, it should be fit for the purpose required. If it has been properly packed and transported, and installed by professional personnel who understand the filter's nature, the filter's integrity should be maintained.

To ensure that there is no ingress of unfiltered air into the data centre, the filter must be fitted into a well-designed housing. This must be of wood construction and particular care must be given to the filter/housing seal. Neoprene rubber gaskets are commonly used for this.

Data centres built to cleanroom standards sometimes use a liquid seal, which is a jelly-like substance that will not flow out of the filter mounting channel.

## Fire suppression systems

Fire suppression systems use water or gaseous agents to suppress fire, so their impact on ICT equipment if they should be activated either accidentally or in the event of a fire should be considered. The most commonly found agents are:

- Water based – sprinklers, (NFPA 2007) and mist suppression (NFPA 2006).
- Gaseous based – clean agent gas suppression (NFPA 2008) and halon gas suppression (NFPA 2009).
- Foams, wet and dry chemical agents and inert gases are less commonly used in data centres.

The National Fire Protection Association (NFPA) standards 2006,2007,2008 and 2009 suggest that clean-agent and halon-type suppression systems are not a threat to ICT equipment. However, fire suppression systems should be evaluated to determine if the agents themselves, if accidentally discharged, or the by-products that form when exposed to excessive heat or fire can harm the computer equipment.

## Mechanical malfunction

CRAC and computer room air handler (CRAH) equipment can itself be a source of contamination. Fan units, bearings and pulleys can become misaligned and deteriorate rapidly during normal operation. Fan belts frequently degrade or disintegrate first when moving parts become misaligned.

There are three primary causes of excessive drive belt wear: The geometry of the actual belt design and materials used to fabricate it, drive belt alignment and tension within the equipment's application. In an ASHRAE Winter Conference 2010 study, three OEM manufacturers' drive belt geometries – raw edge, seamless and wrap-moulded design – with materials of high-end specifications are reviewed. The study shows that raw edge performs best, then the wrap-moulded belt and finally the seamless belt. It also found that non-OEM replacements, if used, have significantly shorter lives due to wear and stretching. The use of OEM belts is recommended for these reasons, and also because they are usually manufactured as a balanced set to ensure uniform belt tension and balanced loading.

Correct drive belt alignment is also critical. This means ensuring that the drive belt runs at exactly 90 degrees to the shaft being driven. Misalignment will cause side loading on the belt or imbalance between paired belts, and both conditions can cause belt heating. Belt alignment is affected not only by original factory setting but also by adjustments made in the field to vary the blower speed. This is especially true

---

---

---

---

---

---

---

---

---

---

if variable – pitch pulleys are used. As a variable-pitch pulley is adjusted, the centre distance between the pulleys is changed as well as the centre line of the pulley. This is because one side of the pulley is fixed in place while the other side is moved in and out to adjust how far the drive belt drops into the pulley groove. If possible, variable-pitch pulleys should be changed to fixed dimension units once the desired dimensions have been established. As the system runs, the drive belt heats up. This can cause the drive belt to lose tension, stretch and slip if the centre distance of the pulleys is not properly adjusted. As the belt begins to slip, heating is accelerated, causing more slip and wear.

The heat also causes the drive belt to harden. This results in belt cracking and loose particles. The airflow through the equipment will carry this particulate contamination into the data centre environment without impedance, because most CRAC and CRAH are filtered on the air inlet or return side, upstream of the drive belt location. Therefore, CRACs and CRAHs should be periodically inspected and repaired as needed to prevent equipment failure and PM contamination. Drive belts must be maintained and precisely aligned at all times. Reduced belt wear greatly reduces the potential for belt dust to contaminate the data centre environment. A better solution if available is the use of variable frequency drives or electronically commutated motors which can eliminate drive belts and their associated PM contamination hazard.

## Ceiling returns

Data centres were originally built as office type environments in which suspended ceilings were used to hide unsightly mechanical systems and provide a pleasing aesthetic appearance. Nowadays, with more densely packed equipment and greater heating challenges, data centres are more typically built without suspended ceilings. This allows hot air to rise further away from the ICT systems on its return to the cooling equipment. A number of data centre operators are simulating this approach within suspended ceiling environments by using the space above the ceiling's tiles. They are doing this by installing open diffusers over hot equipment aisles, then ducting the hot air from the ceiling space back to the cooling unit returns.

This arrangement presents new challenges for contamination control. The ceiling space above the suspended tiles is now an active airflow return area and as such is subject to contamination accumulation. All airflow returns collect PM contamination and require periodic cleaning to prevent this from affecting the data centre environment. Cleaning this space can be problematic due to the nature of the area, difficulty of access, and density of components and surfaces on which contaminant can settle. Also, extreme caution must be used in cleaning this space since it is directly over the operating ICT equipment.

---

---

---

---

---

---

---

---

---

---

## Computational Fluid Dynamics (CFD)

Computational Fluid Dynamics software is now being used as part of the data centre design and building process. Computational fluid dynamics uses 3-D software to model the airflow within a facility and provides a graphic analysis of how hot and cool air flows. This information can be used to improve data centre design efficiency.

CFD can be used to assess the performance of an existing facility. It can also be used during new build projects to predict how efficiently an air flow management scheme will work. It creates precise temperature and airflow models which are useful as a common reference point for the designers of a data centre and its future users. CFD can pre-empt costly problems such as hot-spots or other airflow issues, so that solutions can be designed in at an early stage.

## Data centre operations and security procedures

If the data centre is well located, properly constructed and has a well designed and well maintained air handling and filtration system, it has the best potential to provide a contamination free environment for the ICT equipment it houses. But to fulfil this potential, it is essential to set up appropriate operational procedures, and police them to make sure all staff and visitors abide by them.

## Record keeping

Most management decisions are based on data. Without data, decisions are random and unreliable. This is true of the data centre and its surrounding environment, where recording various activities as they occur can generate valuable data on which future decisions can be made. There is frequently a direct correlation between a number of activities in and around a data centre and contamination-related problems.

Recording equipment anomalies and failures is particularly important. Subtleties and trends can only be spotted if there is recorded data to analyse. Opportunities to solve long term problems have often been missed when data centre operators disregard failures as random events and fail to record these because of their limited effect. In fact, a failure may be part of a larger failure trend that could have been detected if records had been kept and analysed.

---

---

## Monitoring

Even under the best managed contamination control regimes, some ingress of gaseous and PM contamination is inevitable. Therefore, monitoring and recording the condition of the data centre environment can provide valuable feedback on the effectiveness and adequacy of existing decontamination prevention and control measures.

Visual observation and physical inspection are inexpensive, yet make the best tools for this strategy. First, examine surfaces in the data centre where PM may accumulate, especially in hard to reach places, just as for a domestic setting. Look closely at built-in filters and air intake paths within the data centre. Carefully remove tiles from any suspended ceiling and examine the topsides for PM. After any work is completed within the data centre, check the work area for dirt, dust, wire clippings, metal shavings and other types of contamination. If PM rapidly appears or starts to accumulate faster than usual, there is a reason for this which should be investigated. Such unexpected accumulation is frequently the result of equipment failure or a control or separation barrier breakdown.

Both occurrences are serious and should be corrected. One example could be CRAC drive belt deterioration, as discussed in Section 6 – HVAC Systems. Appropriate response and correction is necessary to maintain PM within acceptable levels for the data centre.

## Severe equipment failure monitoring

Commercial ICT and infrastructure equipment are now very robustly designed products. Failures are rare, but when they do occur it is usually because of a lack of maintenance or poor environmental operating conditions. Monitoring symptoms and causes of equipment failures is an excellent way of identifying underlying or long term problems. Data centre operators and owners should practice environmental monitoring, analysis and risk management within their standard operating procedure. Most data centre decontamination specialists can provide monitoring and failure analysis as part of their services.

## Non-severe equipment failure monitoring

Many contamination related failures first appear as intermittent faults. Tracking intermittent abnormalities, which requires data centre shutdowns and/or reboots is an excellent method of identifying problems. Collecting and aggregating incident reports from multiple failure events can identify contamination-related trends. Once contamination is found to be the cause of one or more failures, help should be sought if necessary to identify its type and nature.

---

---

## Access control

Anyone entering the data centre area is a source and contributor of contamination. Therefore, it is logical to limit access to only staff or visitors who have a valid reason for entry. A number of steps can be taken to set up and control an access management strategy:

- Install a data centre access control system to physically manage entry into the equipment space. Many people enter the data centre simply because they are unrestricted.
- Access should be restricted to facility maintenance staff and service providers necessary to support the ICT equipment and environmental infrastructure.
- Periodically review access security control records to ensure that only those who are required for data centre operations are granted access. It is not uncommon for employees and service providers to remain on approved lists long after their assignment has changed or access is no longer required.
- Review service and work processes, and change procedures to allow only tasks that must be performed inside the data centre. Many tasks that previously required physical interaction with the ICT equipment can now be accomplished remotely. Encourage to use remote access tools as much as possible.
- Consider locating people and equipment within a concentrated area inside the data centre. By grouping activities and equipment, the need for people to move around within the data centre can be significantly reduced. The concentrated area should be as far from the most sensitive ICT equipment as possible.
- Establish an access control audit team and ensure that their requirements are met in the design process.

## Contamination control mats

People and the equipment they transport can contribute significantly to PM levels within data centres. Part of this is due to dirt carried in on footwear, and on the wheels of sack barrows, trolleys or other transportation aids.

Contamination control mats, also known as tak mats, can be installed near entrance areas in data centres where their mildly sticky surface can capture dirt from shoes or wheels. These mats are tough, non-slip, and designed with a low profile surround to prevent tripping and problems with trolley wheels. The mats are freestanding and comprise 36 resin impregnated woven cotton layers in a rigid plastic disposable surround.

---

---

---

---

---

---

---

---

---

---

Low profile tak mats, comprising 30 layers but otherwise the same as standard tak mats, are available for areas where a low profile is needed.

As each layer becomes soiled by traffic, it can be peeled away to expose a clean new sheet. Effective contamination needs at least six footfalls, three for each foot, or three full wheel rotations. Using an average person's walking stride, the matting length required is approximately 4.6 m. Ideally, this distance would be applied to all contamination control mats. However this is not always possible due to space limitations.

### Considerations for people allowed into data centre areas

Clearly a degree of access to the data centre area and its ICT equipment is essential and people with legitimate and approved reasons for entry should be admitted. However there are many aspects to their presence, clothing and behaviour that will impact contamination levels. Accordingly, a set of conditions for staff and visitors' entry into the data centre should be compiled and implemented.

### Limit numbers

People when walking can produce about 1,000,000 particles of 0.5 µm or more in size as well as several thousand microbe-carrying particles per minute. Numbers of people within the data centre should be limited as far as possible, and visitors discouraged. It may be useful to arrange a viewing window so that visitors such as users of co-location services offered by the data centre can be given sight of the data centre's capacity and technology without needing to enter the actual ICT equipment area.

### Human body contamination sources

Smokers should not have smoked for several hours before entering the data centre. If they have, then drinking water can reduce the number of particles given off. Cosmetics, talcum powder, hair sprays, nail polish and similar materials are also contaminant sources. Hair should be washed after haircuts to prevent hair clippings entering the data centre's airflow. Highly contaminated or dirty individuals should put on oversuits, or denied access to the data centre.

### Items to ban from the data centre

Ideally, nothing should be allowed into the data centre apart from tools, equipment and materials essential for the work to be performed. In any case, the following items should be banned:

- Food, drink, sweets and chewing gum.
- Cans or bottles.
- Smoking materials.
- Radios, CD players, MP3 players, mobile phones, pagers, etc.
- Newspapers, magazines, books and paper handkerchiefs.

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 
- Pencils and erasers.
  - Writing implements such as fibre-tipped pens that could scratch paper or whose ink contains contaminating chemicals.
  - Paper correction fluid.
  - Wallets, purses and similar items.
  - Disposable items such as swabs and labels that are not data centre or cleanroom compatible.

### Discipline within the data centre

People entering a data centre should only use doors designated as entrances rather than, say, emergency exits that do not have tak mats. Doors should be closed after entry, as air can be transferred both by normal turbulence and by temperature differences between the data centre area and adjoining rooms. However doors should not be opened or closed quickly, as this can pump air from one room to another.

Generation of contamination is proportional to activity, so unnecessary movement should be kept to a minimum. A motionless person can generate about 100,000 particles ≥ 0.5 µm/min, while a person with head, arms and body moving can generate about 1,000,000 particles ≥ 0.5 µm/min. A person walking can generate about 5,000,000 particles ≥ 0.5 µm/min.

### Bringing equipment into data centres

Any new equipment delivered to the facility must be unpacked in a staging area immediately outside the data centre. Cardboard packaging material can itself be a source of contamination fibres, as well as being subjected to dust and dirt contamination on its journey via air, rail, road and intermediate storage and handling prior to arrival. The plastic inner wrapping can also become a source of contamination, although the problem is less severe if the plastic is manufactured from antistatic material.

Trolleys chosen to wheel the equipment into the data area should only be used in areas of similar cleanliness, or should be wheeled across an external tak mat before traversing the data centre's.

## Data centre change control

Many data centre disasters have been caused by poorly planned or poorly timed maintenance or upgrade activities. Setting up and enforcing change control processes and logically questioning all aspects of the internal procedures and requests for access should be an integral part of data centre management. This can ensure that all activities are reviewed and assessed for possible impact on ICT equipment before they are allowed to take place. For example, what are the contamination risks created by using a ladder to open a ceiling tile above an ICT equipment rack? What additional contamination

---

---

---

---

---

---

risk will be incurred by any activities then performed above the suspended ceiling? Who in the data centre's organisation will be responsible for assessing the potential contamination risk to the equipment? Who will be notified if a problem occurs? Answers to these questions should be obtained and available before the proposed activity is authorised to go ahead.

## Managing non routine events

The earlier part of this Section has focused on setting up and implementing plans to limit contamination risks arising from daily activities as staff and visitors work to keep the data centre updated and running. However, non routine events ranging from building work to disasters can happen and should be planned for accordingly.

### Maintenance, repair and re-organisation activity

Maintenance, installation, repair and re-organisation work is not as significant as structural construction, but it can still involve heightened activity in the data centre area, unfamiliar contractors in the room, more frequent entrances and exits, and more disturbance and movement of equipment around the area. All of this can create extra PM, which is increasingly likely to become airborne and find its way into ICT equipment if it isn't cleared away.

It is therefore essential that the data centre management strategy allows for these circumstances by requiring and specifying clean-up arrangements as part of the authorisation to work. Service providers and contractors should be held responsible for controlling the amount of contamination they generate, and for cleaning it up after they have finished their job. This cleaning should be to established standards and may need a specialist data centre cleaning contractor.

### Construction and other major events

Compared with installation and maintenance tasks, construction work involves more aggressive and disruptive activity, particularly drilling and wire-cutting. Drilling should be performed outside the data centre where possible. If drilling within the data area is essential, a powerful vacuum and HEPA filter should be used adjacent to the drill bit to capture as much chip or dust PM as possible before it escapes into the environment. The area around the drill site should be masked as comprehensively as possible to contain debris that the vacuum misses. If drilling into the concrete floor beneath a raised-access floor used for air delivery becomes necessary, the drill site should first be surrounded by air dams to prevent the airstream from blowing and scattering the concrete dust. Drilling should not start until an above floor hand vacuum appliance is ready for use around the drill site. Some drilling work, such as core drilling, can be performed wet. This minimises dust, but the amount of water must be controlled. After drilling is finished, the resulting slurry must be carefully and completely removed before it dries and becomes dust.

During and after major construction work close to the data centre, it is important to closely examine the data centre's environmental protection systems to ensure their

---

---

---

---

---

---

fitness to handle the extra volume and types of PM that will be created. Improved filtering may be needed, provided that this does not overly restrict airflow. Filters may need changing or cleaning more frequently than usual. Walls should be checked for damaged sealing, separation, cracking and penetrations. Any such conditions should be repaired immediately on detection – before construction starts if at all possible. Tak mats should be installed at additional locations around the centre and changed more regularly. Areas around the data centre should be regularly cleaned before construction dust can enter the data centre and the ICT equipment within. For major or prolonged construction work, using a professional data centre cleaning contractor may be necessary at regular intervals throughout the project. Project specifications should require contractors to provide for PM mitigation and cleaning as part of their bid.

If construction work is performed above the data centre, the possibility of PM being released through vibration of the ceiling area should be considered. Also, contractors should take special precautions to prevent any possibility of water leakage or smoke contamination from welding operations into the data centre area.

### Disaster response and contamination control

The data centre function is usually vital to the continued operation and probably long-term survival of the organisation it serves. Therefore, data centres thoroughly deserve investment in their design and ongoing management to ensure protection from both regular and unusual contamination sources. However disasters or contamination from unexpected causes can strike even the best designed and managed facilities. A realistic data centre management strategy should acknowledge this by including disaster recovery plans in case the worst does happen. These plans should be tested and held ready for immediate implementation, returning the data centre to full and reliable operation as soon as possible.

Data centre owners, operators and designers should partner with qualified external resources as necessary to ensure a quick return to full operation. Such specialists can be expected to offer a range of services including recovery strategies, damage assessment, cleaning, equipment restoration and media data recovery. The majority of disaster recovery and support providers can supply specially trained on-site response teams within hours of a disaster.

In selecting such specialists, data centre operators should recognise that there are currently no industry standards or agency certification schemes to ensure that data centre environmental service providers are trained and competent. During planning, the operators should investigate and clearly understand the services being offered and how they compare with known industry best practices. Only service providers whose employees fully understand and comply with ISO 14644-1 for critical environments as described in Section 3 should be considered for selection. Once disaster plans are developed, established and tested, it is critical that all data centre staff and support personnel understand, follow and practice contamination control procedures.

---

# Data centre decontamination

Through much of this Handbook there is a theme that shows how keeping data centre contamination down to an acceptable level is a ‘whole life’ process that ideally starts before the data centre is built, and continues throughout its operational life.

Data centre cleaning activities play a key role in this ‘whole life’ decontamination process. In fact, these cleaning activities should be scheduled as part of a structured, ongoing plan that accommodates the data centre’s requirements as they change over time. Different cleaning programmes should be designed and used as appropriate for events that affect the data centre, as well as for its environment and the nature of the ICT equipment it supports. A schedule of cleaning programmes that could cover a data centre’s transition from a building site to an online resource for its owners could include:

## **Enhanced Builders’ Clean (EBC™)**

The data centre’s first specialist clean, carried out when the room is secure and ready to accept installation, but no ICT equipment has been installed yet. This presents an opportunity that will never exist again because access to all areas of the room will never be so easy after cable trays, cabinets and other infrastructure items have been positioned.

## **Initial Deep Clean (IDC™)**

An Initial Deep Clean, similar to an Enhanced Builders’ Clean is performed after **fitout** of the ICT cabinets, cable trays and cables and other support infrastructure has been completed.

## **Initial Clinical Clean (ICC™)**

This is performed when the data centre is complete and ready for switch-on. After the Initial Clinical Clean, the data centre environment’s contamination levels should be within acceptable limits. In terms of particulate contamination, this means conformance to ISO 14644-1, Class 6–9. Proof of this conformance may be essential in the event of any future equipment warranty claims.

Although a particle count may show that the data centre meets ISO 14644-1 at the moment of sampling, this conformance will be lost over time. PM lying on surfaces within the room, or from the outside environment will find its way into the room’s airflow and potentially into the ICT equipment. Maintenance or installation work, or ICT or HVAC equipment failure could add to the contamination loading as well. Therefore, once the data centre is up and running, a planned preventative maintenance (PPM)

---

**\*Note:** “authority” here means delegated authority to the individual by his employer to carry out a certain function or duty

---

schedule should be implemented. This typically comprises an appropriate mix of **Maintenance Deep Clean** and **Maintenance Surface Clean** programmes.

## Elements of cleaning programme design

No two cleaning programmes are likely to be identical. In addition to the ‘lifetime’ variants covered above, each data centre will have its own profile of size, history, equipment and external environment. Accordingly a specialist data centre decontamination contractor will take these factors into account when he proposes a cleaning schedule matched to the particular data centre’s needs.

Despite these differences, specialist data centre cleaning programmes are subject to, and drawn from a number of common elements. These include the type of staff necessary for work in sensitive data areas, the equipment, materials and procedures they use, the issues they will encounter in the data centre, and the methods used for testing and documenting the data centre’s status and any problems found. After reviewing these elements, we will see how decontamination specialists can build them into a plan suited to the data centre to be decontaminated.

## **Specialist decontamination contractors and their staff**

Although data centre decontamination is sometimes referred to as ‘cleaning’, it should not be confused with general office cleaning activities. An untrained office cleaner could all too easily cause serious equipment damage or data loss through carelessness or lack of training. An electrically noisy vacuum cleaner plugged into a ‘clean’ power circuit feeding ICT equipment, a switch knocked out of position on a live server, water or chemicals spilled into a termination box, or a general purpose cleaner stripping a computer room floor of its anti-static properties are just some of the potential hazards.

Worse than this, bearing in mind the sensitive nature of most if not all data centre installations, is the possibility of hostile or malicious damage. If a data centre operator has no knowledge of the decontamination contractor he is using, or of the staff the subcontractor is supplying to his site, he is exposed to an unknown risk. It therefore makes sense for him to ask potential contractors about their staffing policies, with questions including:

- **Are the staff supplied to my site permanent employees of the decontamination contractor?**
- **How long have they been employed and how well do you know their employment history?**

---

---

- **Have they been Police (Criminal Record Bureau) vetted?**

- **Do they have Baseline Personnel Security Standard (BPSS) – formerly Basic Check (BC) clearance?**

A Baseline Personnel Security Standard (Basic Security Check) will evidence current criminal record and unspent convictions under the Rehabilitation of Offenders Act 1974. A BPSS (BC) provides a level of assurance to the trustworthiness and integrity of individuals whose work involves access to confidential assets or information. There are no access restrictions for this level of disclosure and the result may be sent to the applicant or the employer.

- **Do they have a Security Check (SC)?**

The Security Check (SC) is the most widely held security clearance for posts involving long-term, frequent and uncontrolled access to secret assets and occasional and controlled access to top-secret material.

An SC level involves a BC security clearance check, plus checks against the UK criminal and security records (and if appropriate, of overseas countries) and a credit check.

- **Do they have CSCS (Construction Skills Certification Scheme) cards?**

CSCS was set up to help the construction industry to improve quality and reduce accidents. CSCS cards are increasingly demanded as proof of occupational competence by contractors, public and private clients and others. The test examines knowledge across a wide range of health and safety topics to improve safety and productivity on site. It also proves the holder's competence in the field covered by their card.

- **Are they PASMA (Prefabricated Access Suppliers' and Manufacturers' Association) trained to work at height?**

The Work at Height Regulations 2005, require that the assembly, dismantling or alteration of Mobile Access Towers should only be undertaken by a **competent person**, or if being trained, under the supervision of a **competent person**.

A **competent person** is a person who can demonstrate that they have sufficient professional or technical training, knowledge, actual experience, and authority\* to enable them to:

- carry out their assigned duties at the level of responsibility allocated to them;
- understand any potential hazards related to the work (or equipment) under consideration;

- detect any technical defects or omissions in that work (or equipment), recognise any implications for health and safety caused by those defects or omissions and be able to specify a remedial action to mitigate those implications.

PASMA therefore sponsors training courses provided by authorised training members. The training courses are based on a format and content agreed by all PASMA members and draws upon their collective, first-hand experience. It provides successful delegates who pass a written and practical test with a competency certificate and an encapsulated, credit card sized PhotoCard.

- **Do they have IPAS (International Powered Access Federation) training?**

The International Powered Access Federation (IPAF) promotes the safe and effective use of powered access worldwide. Set up in 1983, IPAF is a not-for-profit members' organisation that represents the interests of manufacturers, distributors, users, and rental and training companies.

The IPAF training programme for platform operators is certified by TÜV as conforming to ISO 18878. Successful trainees are awarded the PAL Card (Powered Access Licence).

- **Do they have First Aid training? Does the team assigned to your site include a designated, qualified First Aider?**

All technicians should be aware of Health & Safety requirements and able to identify requirements and carry out their duties in an orderly and sensible manner.

- **Is their job related training up to date?**

Any technicians should go through regular training sessions should be aware of the importance of data centre equipment. They should be fully aware of the repercussions of errors that could be caused through switches, cable connectors, panels, etc on equipment or under the floor.

Technicians should be aware of all types of computer equipment and able to identify specialised areas such as fibre optics, robotics, mainframes, servers and all the delicate services underneath the floor or in the ceiling void.

All technicians should be trained by induction course, office based courses and on the job one to one training at any deep cleaning company.

They should all be issued with a training plan and only when they have been signed off and fully trained should they be allowed to work on any client project.

---

---

---

---

---

All technicians should be fully trained on the use of all chemicals.

- **Technicians should always wear a uniform and have a smart appearance on site.**
- **Technicians should wear security badges showing their name, job title, security number and a passport size photograph.**
- **A list of technicians due on site along with any other information required should be supplied prior to work commencing.**

### **Choosing the specialist decontamination contractor**

The above criteria demonstrate how data centre cleaning requires trained staff with up to date skills and competencies for the job. It is also essential that the data centre decontamination contractor employing these staff is equally well qualified. Although there is no industry standard or agency certification to cover these contractors, there are benchmarks that can be used to judge their competence and suitability. Accordingly, the following criteria should be applied when considering contractor candidates for the specialist data centre decontamination function. These are in addition to the normal checks as carried out on any prospective new supplier.

### **Health and Safety**

Any deep cleaning organisation should be members of at least the following organizations, who vet health and safety policies and procedures:

- CHAS (Contractors Health and Safety Assessment Scheme).
- Safe Contractor Scheme (Copies of the certificates should be provided).
- PASMA.
- IPAF.

The on site **teamleader** should always carry a first aid kit which is clearly identified to the team.

All on site staff should have full PPE, safety shoes and clothing as appropriate.

How well does the deep cleaning organisation comply with the Health and Safety at Work Act 1974? What steps is it taking to update or improve its compliance?

### **Quality standards**

A deep cleaning organisation should have achieved at least ISO 9002 (Quality) and ISO 14001 (Environmental) accreditations.

---

---

---

---

---

---

---

### **Confidentiality**

All organisation employees should sign a contract to declare that they will not disclose confidential information seen on site. Breaches of this contract must be dealt with appropriately.

The deep cleaning company should be registered by the Data Protection Act 1998.

### **Insurance and indemnities**

A deep cleaning company should have at least £10 million public and products liability insurance.

### **Hours of business**

A deep cleaning company should offer seven days a week operation, including night work, to minimise disruption to the data centre's on line activity.

### **Record keeping**

A deep cleaning company should maintain good standards of record keeping, covering all aspects of its activities, including COSHH for chemicals handling, Health and Safety records, Risk Assessments, and Statements of Work – both General and specific to individual sites.

### **Decontamination equipment, materials and procedures**

Within the data centre, the decontamination technicians need to perform their work effectively and without risk to themselves or others. Their training as described above will help them achieve this, but they will also need materials and equipment which has either been specifically designed for, or approved and tested for data centres' specialist requirements. They will also need to follow suitable procedures, such as tucking a vacuum hose behind a vacuum cleaner to avoid accidentally changing the setting of a live server control.

### **Vacuum cleaners**

Ordinary domestic or office vacuum cleaners are entirely unsuitable for data centre cleaning, as they tend to blow more particles into the airstream than they collect from the vacuumed surfaces. Instead, micro-filtered vacuum cleaners should be used, which can filter 99.9% of 0.3 micron diameter dust taken in through three layers of filters. These dust particles remain inside the machine preventing the escape of contamination back into the atmosphere.

These micro-filtered vacuums should have long attachments and tools to gain access to awkward areas, where possible. The vacuums should also be RF suppressed, and fitted with an anti-static device and plastic pipes that dissipate any static problems.

---

---

---

### Rotary cleaning machines

These should have a built-in vacuum to trap dust from vinyl or other floor surfaces as they are cleaned.

### Portable tools

Those that are connected to the main power supply should be fitted with a 110 VAC transformer where possible, and a circuit breaker used.

### Electrical equipment maintenance

All electrical equipment should be tested by a qualified electrician every three months for a Portable Appliance Test (PAT) and labelled PASSED if OK. Any equipment that fails should have a DO NOT USE label attached and taken out of service immediately.

All equipment should be fitted with an RCD as well as inspected visually every time it is used.

### Power supplies

Mains operated equipment should be 110 VAC wherever possible, driven if necessary via a transformer from the 240 VAC mains supply.

Decontamination equipment taken into a data centre should only be connected to a 'dirty' supply as identified by the data centre operator. It should never be connected to a clean supply that may also be feeding EMC susceptible ICT equipment.

### Use of liquids and chemicals during data centre cleaning

Do not use water for cleaning in a data centre.

Chemicals used for office cleaning are unlikely to be suitable for data centres. This is because many are chlorine-based, phosphate-based, petrochemical-based or bleach-enriched products which can damage electronic equipment, with gases from these products or direct contact causing component failure.

Cleaning solutions used in data centres should be:

- Non-toxic.
- Non-flammable.
- Reasonably fast-drying.
- Not harmful to data centre surfaces.
- Does not create particulate or gaseous contamination that could damage ICT equipment.

- 
- Effective in removing undesirable contamination.
  - Reasonably priced.

Appropriate PPE should be worn whilst handling cleaning chemicals. Chemicals must be stored in suitable containers.

All containers must be stored in boxes whilst on site. All chemical mixing must be done off site and not in the computer room.

Use a blue polythene sheet on the floor as an area to stand blue or red chemical boxes.

All decontamination contractor team leaders should maintain a COSHH folder of all chemicals used within his health and safety file.

Ideally, chemicals used should be water based and not classed as hazardous under CHIP.

### Working at height

Using Ladders, Podium Steps and Towers.

- Only PASMA trained staff to erect towers. No one to work within the vicinity of the tower.
- Operators to be mindful of not overstretching.
- Care to be taken climbing tower – be aware of obstacles above.
- Before use stepladders must be checked for the condition of: treads, stiles, hinges, restraining rope or struts between both legs. Damaged step ladders must be taken out of use for repair or destruction.
- Ensure the steps are erected on a firm, level base. Ensure the steps are spread to their fullest extent. Do not work from the top third of the steps. Ensure that the steps are at right angles to the work. Steps are not designed to take any degree of side loading.
- Mini scaffolding must be erected and stabilised in accordance with the manufacturers or suppliers handbook.
- Prior to use check equipment for defects. Report defective equipment and remove it from service.
- Prior to use wheels must be in the locked position and barriers closed.

Using Mobile Elevated Work Platform (MEWP).

- Only IPAF trained staff to operate.
- Room must be made available to operate: Width of lift plus two metres each side.
- Hazard tape and cones must be used in work area.
- An experienced banksman must be on hand at all times during the operation of the MEWP.
- The platform must be visually inspected on a daily basis before commencement of operation with any defects being recorded and reported to the Supervisor.
- The platform must have a current test certificate and be up to date for routine maintenance. The Supervisor must be advised of these test and maintenance dates.
- PPE consisting of a Lanyard, Fixed Harness, Helmet, High Vis-Vest, Steel Toe Capped Boots and Goggles must be worn at all times by the operator and banksman during MEWP operations.
- The platform must not be moved in an elevated position and must not be operated within 6 metres of live overhead power lines. If closer operation is required then power must be turned off and locked off in the overhead line.
- A Ten (10) metre exclusion zone must be established where practicable to prevent vehicle and pedestrian access into the working area.
- Take care to avoid overhead lights and other obstructions whilst elevating platform.

Working on Aerial Lift.

- No one to be beneath the work area.
- Wear safety harness.
- Vacuum cleaners must be tied to platform. No more than two vacuum cleaners to be used.

#### **Scheduled activities before, during and after an onsite decontamination session**

When the data centre decontamination specialist has staff trained as described, with knowledge of and access to suitable cleaning chemicals, access and cleaning equipment as specified above, he is ready to put a decontamination team and equipment on to your site. Before he does so, he should agree on a programme with the data centre owner which includes preparation for arrival and cleaning up afterwards as well as the deep cleaning tasks themselves.

#### **Pre-session**

During the week beforehand, the data centre operator should be sent an email and/or fax detailing which technicians are coming to site and their scheduled times on site.

A procedure sheet should be completed before any work is commenced. This details all information that needs to be obtained when the deep cleaning team arrives on site, before they enter the room.

Once on site, a specialist deep cleaning company should carry out a risk assessment for each area: floor void, floor surface, Equipment (i.e. Cabinets) High Levels, Low Levels and Doors/Ledges. The Senior Team leader should make all the technicians on site, and the client, aware of any possible hazards within the room.

Technicians should be aware of all types of computer equipment and able to identify specialised areas such as fibre optics, robotics, mainframes, servers and all the delicate services underneath the floor or in the ceiling void.

A formal procedure sheet should be completed before any work is commenced.

This typically covers the questions as below:

- Has the health and safety box been positioned?
- Cones, barriers positioned?
- Caution signs displayed?
- Have the technicians been shown fire exits?
- Position of fire extinguishers?
- Have the risk assessment sheets been issued and completed?
- Have the fire detectors been covered?
- Has the fire detector cover sheet been completed?
- Staff informed verbally of all above procedures?
- Staff informed verbally of all work to be done?

#### **During the decontamination session – work areas within the data centre**

Once the specialist decontamination team enters the data centre, it will carry out decontamination activities in different areas. These are typically identified as:

- High Levels – Cable Trays.
- High Beams, Lights and Trunking.
- Ceiling Void and Infill Bags.

- Ceiling Void.
- Ceiling Surface.
- Walls, Doors and Ledges.
- Equipment (cabinets and servers) – internal and external.
- Floor Void.
- Floor Surface – Solid floors.
- Floor Surface – Vinyl.
- Floor Surface – Carpet.
- Floor Surface – Concrete and Wood.

Each area calls for its own procedures, which are described below:

#### **High levels – cable trays**

- 1 Gain access by using the correct equipment that complies with Health and Safety regulations.
- 2 Clean using micro-filtered vacuums with long attachments and tools to gain access to awkward areas, where possible.
- 3 Wipe with anti-static solutions. Wipe from left to right in a zig-zag motion, change wipes regularly.
- 4 Discard wipes when finished.
- 5 All solutions to be used in one area only to avoid cross contamination.

#### **High level beams, lights and trunking**

- 1 Gain access to the beams by using a mechanical lift platform with safety harness that complies with Health and Safety regulations.
- 2 Lay boards on the flooring in order not to damage the raised flooring.**
- 3 Clean using micro-filtered vacuum cleaners with long attachments and tools to gain access to awkward areas. It is important to use the correct attachments.
- 4 Wipe with anti-static solutions. Wipe from left to right in a zig-zag motion, change wipes regularly.
- 5 Discard wipes when finished.

#### **Ceiling void and infill bags**

- 1 Vacuum and anti-statically wipe the infill bags using micro-filtered vacuum cleaners.
- 2 Clean the ceiling void including above, below and inside all accessible supports; service pipes; cable trays; ductwork; etc using vacuum cleaners with the correct long handled attachments.

#### **Ceiling void**

- 1 Clean the ceiling void including above, below and inside all accessible supports, service pipes, cable trays, ductwork, etc using micro-filtered vacuum cleaners with the correct long handled attachments.

#### **Ceiling surface**

- 1 Gain access to the ceiling surface by using the correct equipment that complies with Health and Safety regulations.
- 2 Clean the ceiling surface using micro-filtered vacuum cleaners with long attachments and tools to gain access to awkward areas. It is important to use the correct attachments to ensure that the tiles are not damaged. Wipe with anti-static solutions.

#### **Walls, doors and ledges**

- 1 Vacuum ledges, etc including door frames and polish using anti-static solutions.
- 2 Vacuum and tak-cloth walls.
- 3 Wipe from left to right in a zig-zag motion, changing wipes regularly.
- 4 Discard wipes when finished.

#### **Equipment – external**

- 1 Clean the outer casings of the equipment.
- 2 Anti-statically clean the equipment with impregnated cloths.
- 3 Include all areas where accessible. Equipment will be vacuumed with the hoses towards the side or back of the machines to avoid knocking a control panel.
- 4 Control panels, switches, buttons, etc will not be cleaned to eliminate the risk of accidental activation.

---

---

### Equipment – internal

- 1 Unlock the cabinet doors under the supervision of the client contact.
- 2 The equipment top surfaces should be vacuumed from behind or the side, if accessible, with the vacuum cleaner hose safely tucked out of the way to avoid accidentally knocking a control panel.
- 3 Do not clean switches or control panels to avoid the risk of knocking a switch.
- 4 Only clean areas that are visible: Do not blindly vacuum or wipe an area that could be hiding cables or switches.
- 5 Seek the data centre operator's approval before cleaning glass, ledges and equipment.
- 6 Once a particular area has been cleaned the decontamination specialist should seek approval for the work from a senior member of the data centre owning organisation.

### Floor void

This service is important not only for ensuring that equipment is kept in a clean environment, (particularly when there is a down flow system). It is also to remove contamination in the floor void which could otherwise be picked up by the airflow and circulated around the computer room. The contamination could then settle on tops of ledges, equipment, etc or more hazardously be drawn into computer equipment possibly causing media or hardware related problems.

- Carry out a full risk assessment.
- Cordon off a section of the floor void to avoid accidents. Remove panels using suction (for vinyl) or spiked lifter (for carpet) either singly or in rows. It is not recommended that more than three panels are lifted in any particular area.
- Panels are removed by lifting them by only the depth of the floor panel and then turning them at an angle to ensure that they do not fall into the aperture and damage any cables in the void.
- Panels should be placed in a safe place and stacked. Use barriers to prevent access to the work area. Cones must be placed at all entrances to the work area.
- Identify the fibre optic cables and other sensitive areas. Make all technicians aware of these and mark their location on a plan of the computer room. Fire detectors should be covered and marked on a plan. These should be checked off at the end of the day to ensure that they have all been removed.
- Remove contamination from all areas of the void including underneath, inside the cable trays, underneath pipes, services, etc using a three stage micro-filtered vacuum cleaner with 99.9% (0.3 micron) filtration. Wipe with an impregnated cloth and anti-static solutions that are safe to use on cables and services.

- 
- 
- If debris and contamination are allowed to accumulate on the pedestal heads the floor could become unbalanced and therefore dangerous.
  - Replace panels, paying particular attention to panel edges and replace in the same order as lifted.

### Solid and vinyl floor cleaning

- Carry out a full risk assessment.
- Anti-static vinyl floors should never be polished, as this destroys their dissipative qualities. They should only be buffed with specialist anti-static solutions.
- Remove loose dirt by vacuuming using the correct attachments to avoid damaging the vinyl.
- Strip off the contamination with an electric rotary machine with built in vacuum. The vacuum ensures that the loose vinyl dust is eliminated as it could cause problems if circulated throughout the room.
- Remove scuff marks using the correct solutions and a nylon pad.
- Then thoroughly buff and polish with an electric rotary machine.

### Carpet cleaning

- Soil within the carpet will abrade the carpet fibres and accelerate the ageing process. 90% of carpet soiling is exterior contamination transferred via foot traffic. The long-term appearance of any installation will substantially improve by regular cleaning.
- Carry out specialised tests to identify the type of carpet that requires cleaning. These tests prevent costly mistakes being made, i.e. discolouring of carpet from use of wrong chemicals, shrinkage and balding of carpet from excessively vigorous scrubbing to remove stubborn stains.
- Remove spot stains and other soiling, where possible, with chemicals.
- Vacuum thoroughly with micro-filtered cleaners.
- Re-stick any loose carpet pads with suitable adhesive.
- Clean the carpet to the manufacturers' specifications by pre-spraying with low-foam solutions, lift off the contamination with a rotary machine and finish with an anti-static solution to prevent static build up. This process of cleaning the floor surface leaves the carpet virtually dry and is safe to use inside the computer room as no water is used.

### Concrete and wood floor surface cleaning

- Remove loose dirt with a three-stage micro filtered vacuum cleaner. Use the correct attachments to avoid floor damage.

---

### After finishing the decontamination session

After the deep cleaning session is finished, the decontamination contractor should always confirm with the data centre operator that he is satisfied with the standard and extent of work performed. If any problems do arise during the session, these should be reported to the data centre staff on duty immediately, to allow a timely solution. If this is not possible, any problems should be reported by telephone, and followed up with a written report and/or action plan.

A quality questionnaire should be issued to the data centre operator to complete at their leisure. Results from these questionnaires should be documented and acted upon if necessary.

A specialist waste management company should be used to destroy magnetic media and documents. The waste management company should then provide a certificate of destruction.

### Summary

In this Section we have seen how data centre decontamination, sometimes referred to as data centre cleaning, or data centre deep cleaning, is a highly specialist activity which cannot be performed by general purpose office cleaners. Technicians from a data centre decontamination contractor must be trained and certified in all relevant disciplines, which include Health and Safety aspects as well as technical expertise. Because of the sensitivity of data centres, their equipment and the data they hold, all decontamination technicians must be vetted and clearly identifiable. The decontamination organisation they work for must similarly be of excellent, proven provenance.

The technicians must apply this expertise, using suitable equipment, tools, cleaning materials and PPE as appropriate around the different areas and levels of the data centre. How intensively they work, and in which areas, depends on the nature of the programme agreed. As described at the beginning of the Section, the work activities can be built into an Enhanced Builders' Clean (EBC™), Initial Deep Clean (IDC™), Initial Clinical Clean (ICC™), Maintenance Deep Clean (MDC™) or Maintenance Surface Clean (MSC™). These programme types allow the work to be profiled for the needs of the data centre as they change over time. For example, an EBC™ programme would be proposed to a data centre during or after the final facility construction stages, whereas MDC™ or MSC™ programmes would be proposed as appropriate during the operating life of the data centre.

---

# Testing and assessing contamination levels

The last Section described how decontamination programmes can be designed to meet a data centre's needs. And these needs are ultimately defined by how much contamination exists within the data centre. It is also essential to measure and record the levels of contamination within a data centre to demonstrate its compliance with ISO 14644-1 specifications. So the first stage in decontamination planning involves an investigation of these levels, to determine:

- How the density of the contamination varies across the data centre area.
- How – or if – the contamination density varies with time.
- The composition of the contamination – solid or gas, what are the chemical constituents?
- The composition of the contamination – in terms of particle size distribution.

A complete investigation can involve both visual inspection and a range of instruments which are available to perform more detailed and accurate measurements. Visual inspection is usually performed as the first stage, because it can provide an overall idea of contamination levels within the data centre, and indicate a plan of action for the rest of the investigation. However the information provided is limited, because it is neither quantitative nor accurate. Also, much contamination comprises particles too small to be visible to the naked eye unless they aggregate. A human hair is about 100 µm in diameter, and particles become invisible at diameters smaller than about 25 or 30 µm. Compared with this, ISO 14644 sets limits for particles down to 0.1 µm diameter.

The visual inspection will help to establish where to place monitoring devices to measure the airborne particle count, total suspended particles and volatile organic compounds. It will also show where to collect settled dust samples. The inspection should reveal:

- **The environmental history of the data centre**, including its ICT equipment and infrastructure hardware failures, temperature and humidity records, and complaints about odours. Gas or settled dust acting on printed circuit boards is often found to be the root cause of failures in equipment returned from the field. A data centre survey can help to reveal the sources of such particulate or gaseous contamination.
- **The ventilation system and layout of the data centre** should be mapped to show the airflow pattern throughout the area. This mapping should also show the

---

---

positions of all computer hardware – servers, tape drives, disk drives and printers. It should also show administration areas and all air conditioning and handling units. Air handling and movement considerations include:

- **Air distribution scheme for the building**, including the level of filtration, the areas with shared air return, the proportion of outdoor air used, and the outdoor air intake locations.
- **Air filters** – direct visual inspection of dust loading or measurement of differential pressure across them, to ensure they are well maintained.
- **Air humidifiers** – these can release salts from the water used for humidification, which can cause problems such as electrical short circuits on ICT equipment printed circuit boards.

This mapping information can be used to plan where to locate contamination monitors and collect dust samples.

Air monitoring devices should be placed

- Immediately downstream of filters, modular air-conditioning Units (MACUs), HVACs and humidifiers.
- At the data centre entry doors.
- Between the administration areas and the ICT equipment.
- Around the ICT equipment and printers.

Dust samples should be collected from

- Internal surfaces of the ICT equipment.
- Internal surfaces of the humidifiers.
- Under raised-access floor surfaces, the floor support grids and stanchions.
- Internal surfaces of ducting near the ICT equipment.

This sampling can be performed using a range of different instruments and procedures as described below.

---

---

### Airborne particle counts

Airborne particle counters (APCs) count the number of particles in a unit volume of air. Some APCs can also analyse the particles counted into a particle size distribution, reporting on particle densities for different size ranges. An APC has a pump that draws air into a fixed volume at a constant rate for a known period of time. A laser beam illuminates the airborne particles and light is redirected or absorbed. A detector measures the amount of light scattered to determine the particle quantity.

There are three main types of particle counters: Handheld, portable and remote. Handheld counters are useful for rapid measurements in different areas of the data centre. A typical handheld counter has a 2.83 LPM flow rate and measures particles in the size range 0.3 to 10 µm, and has a USB output for data collection.

Portable counters are bigger than handheld devices and are typically powered from a wall outlet or internal batteries. They are frequently used for monitoring an area over a long period of time. Data can be stored within the counter for later analysis. A typical portable instrument can store 10,000 records, handle up to six channels simultaneously for different particle sizes, then display the sampling information in ISO 14644-1 compatible format. With USB and Ethernet ports, it can operate as a stand-alone device or be integrated into a facility monitoring system.

Remote particle counters are designed primarily to act as collection points in a distributed sampling system. An Ethernet port can provide both a connection to a central PC and power, using Power over Ethernet. The PC or a remote web browser can be used for configuration.

Within a data centre, there is rarely a need for continuous particle count monitoring. A survey is more likely to be required if a contamination problem becomes evident, to demonstrate the contamination level in the area, or in preparation for a decontamination exercise. Whereas a handheld instrument can be useful for periodic checkups, a portable device, with its multichannel sampling for multiple particle sizes, is usually best for troubleshooting and more in-depth surveys.

---

---

---

---

---

---

Surveys should be run for one or two weeks, and if possible conduct these throughout the year as particle counts can be affected by changing weather and seasons. Take as many readings as possible throughout the data centre, particularly including the following areas:

- Entrances: Take one or two sets of readings at each entrance.
- High traffic human activity areas: Take one sample set in each area of major activity – desks, chairs, workstations, etc.
- Under an air diffuser: Take one set of readings for makeup air particle count.
- Air Handling Unit (AHU): Take one set of readings at an AHU inlet, and another set at the AHU's outlet. This will identify any problems associated with the filter efficiency.
- General data centre characterization: Take a set of readings in at least three random locations across the data centre. For larger data centres, divide the area into imaginary sections and take at least two readings in each section.
- Outside: If possible take several outdoor readings a day at the makeup air inlet point.

The outdoor air readings are important to normalize the data taken at different times of day or in different seasons. Outside air can greatly influence indoor air quality under certain circumstances. If a noticeable spike in indoor air particle count occurs, this can be checked for correlation with outdoor air conditions. Correlation would indicate that the increased contamination is originating from an outdoor source, whereas absence of correlation would indicate that the source is internal to the data centre.

After a set of data has been collected, prepare a chart of the particle sizes. Check for extremes in each size range. Compare data for each set of measurements taken, such as for different areas of the data centre or different times of year. See if any extremes are showing up between data sets. These extremes can provide valuable clues as to where or when more testing needs to be done. This will help to identify or possibly prevent a problem that appeared during analysis.

#### **Other methods of measuring airborne particle levels**

Other methods exist for measuring airborne particulate levels – photometry, adhesive disks, impactors and piezobalances.

Photometers can be used because they can measure light scattering. The light scattered from a cloud of particles suspended in an examination area is converted into a voltage. This is compared to a benchmark standard to give a value for the total suspended particles (TSP). The photometer takes measurements from the particle cloud rather than individual particles, and is ineffective for particle sizes greater than 10 micron. Accordingly if the dust has clumped rather than being evenly dispersed throughout the photometer, the photometer measurement will be less than the true density of dust.

---

---

---

---

---

---

Another method is useful when the chemical composition as well as the density of the airborne particles must be investigated, for example when heavy contamination is being created by an unknown source. Air is pumped onto a special adhesive disk, so that particles captured on the disk can be analysed using a scanning electron microscope (SEM). Major elements revealed by the analysis can be matched to known sources such as outdoor dust, salts and chemicals in humidifier water, concrete dust or smoke.

The mass concentration of airborne particles can also be measured using a device called an impactor. Contaminated air is accelerated through a nozzle into the impactor, which comprises a cylindrical tube with several removable plates spanning part of its diameter. The airstream turns sharply before hitting a perpendicularly placed plate. Large particles cannot make this turn and are therefore deposited on the plate. Smaller particles continue within the air stream until meeting the next impactor plate stage. The plate stages are repeated for the particulate sizes required, such as PM10 or PM2.5. The dimensions of the particulate stages govern the size of the particles deposited. These particles can then be analysed gravimetrically or chemically.

A piezobalance can also be used to directly measure particle mass concentrations. A single stage impactor is used to trap particles of a certain size or larger. The remaining smaller particles, i.e. those of interest, are passed through a nozzle and become charged. A crystal at the base of the tester is made to oscillate. The charged particles settle on the crystal, increasing its weight and lowering its oscillation frequency. This change in frequency can be correlated to a mass concentration.

#### **Testing particulate matter for corrosive properties**

Very few types of particulate matter, acting in isolation, cause ICT equipment to corrode to the point of failure. However a method exists for assessing the corrosiveness of different PM materials.

- Wires are soldered to interdigitated cards using rosin mildly activated flux.
- Cards are inserted into a 40% relative humidity (RH) 50°C chamber and stabilised.
- The interdigitated comb areas are sprinkled with particulate matter and debris.
- 15 V is applied across the comb coupons, and leakage current is plotted against time.
- RH is raised every three days in 10% increments, and the RH at which the leakage current rises to reflect 100 M $\Omega$  surface insulation resistance is noted.
- The particulate matter is deemed corrosive if it causes the comb area surface resistance to decrease below 100 M $\Omega$  in an environment with 90% RH compared to the level in a data centre environment.

---

---

### Volatile Organic Compounds (VOCs)

VOCs, which cause unknown odours are difficult and expensive to identify in data centres. VOCs are organic chemical compounds with high enough vapour pressures under normal conditions to significantly vaporise and enter the atmosphere. Originating from a broad range of data centre sources, VOCs are detected by first adsorbing them into charcoal filters and then analysing these filters using gas chromatography/mass spectrometry (GC/MS).

VOCs can be collected by pumping air through carbon filters, or passively by adsorption through diffusion over a longer period of time. Passive monitoring uses no pumps, lasts for typically a month, and is only used in extreme situations where the VOC source is unknown.

### Monitoring of gaseous contaminants

Real-time gaseous monitoring comprises direct gas monitoring and real-time corrosion measurement. Direct gas monitoring can be done on a real-time basis with electronic devices that respond to gas composition changes in matters of minutes. Levels of many gases in the parts per billion (ppb) ranges can be detected. Real-time monitors can detect ammonia, hydrogen sulphide, hydrogen chloride, nitrogen oxides, ozone, sulphur dioxide and total volatile organic compounds (TVOCs). Lower detection limits for these gases are in the 0.1–1 ppb range, except for the TVOCs which have a 20 ppb limit.

ISA S71.04-1985, published by the Instrumentation, Systems and Automation Society, is a document that classifies the level of airborne contamination that is safe for electronics. Called *Environmental Conditions for Process Measurements and Control Systems: Airborne Contaminants* (ISA 1985), it is a popular guideline for warranties of electronic and electrical equipment.

This ISA standard specifies four severity levels for gas corrosion in reactive environments, defined as below:

- **Class G1: Mild** – Corrosion is NOT a factor in determining equipment reliability.
- **Class G2: Moderate** – Corrosion is measurable.
- **Class G3: Harsh** – It is probable that corrosion will occur.
- **Class GX: Severe** – Only specially designed and packaged equipment will survive.

The ISA standard describes ways to measure the level of airborne contaminant gases using *reactivity monitoring*. A data centre's ISA Class is dependent upon the rate of corrosion buildup (corrosion thickness over time). Corrosion thickness is measured in Angstroms (one ten-billionth of a meter). According to ISA, a G1 environment has less than 300Å of corrosion buildup in 30 days, G2 has <1000Å, G3 has <2000Å, and GX > 2000Å.

---

---

Corrosion classification coupons and monitors can be used to determine a room's ISA classification. A copper corrosion classification coupon consists of a copper-plated metal strip mounted on a Plexiglas panel. Copper coupons, Copper-Silver coupons and Copper-Silver-Gold coupons are available. Sulphur dioxide alone will corrode silver to form silver sulphide, whereas sulphur dioxide and hydrogen sulphide when combined will corrode both copper and silver.

To measure corrosion, place the copper coupon in a data centre or other area housing sensitive ICT hardware, but not within any equipment racks or cabinets. Over the test period of 30 days, the coupon will tarnish. A laboratory can then analyse the coupon to determine the room's ISA class. The coupon's corrosion film thickness and chemistry reflects conditions within the data centre.

Although this reactive monitoring method gives the average corrosion rate over the 30-day test period, it does not detect any short-term variations in the data centre's gaseous contamination levels. By contrast, corrosion monitors can report on small changes in gas levels and corrosion rates as they occur in real time, allowing remedial action such as shutting off the outside air entry to be made immediately. Such monitors can provide information on corrosive gas levels as low as 1 ppb.

### Settled dust analysis

Analysis of dust found settled in a data centre serves two purposes. Firstly, an understanding of the dust's chemical composition allows an assessment to be made of its potential to cause short circuits at different voltages and currents if it settles on electronics printed circuit boards. Secondly, an understanding of the dust's chemistry can help to identify its origin.

Settled dust for analysis can be collected on a sticky tape stud, which can then be examined using a scanning electron microscope and energy-dispersive X-ray analysis (EDX). The generated EDX spectrum can identify the dust elements and provide a rough indication of their concentration. Characteristics of the dust's chemistry will also indicate its potential for causing short-circuiting of electronics circuit board connections and tracks, especially in conditions of elevated humidity.

Analysis of the settled dust can also help to reveal its source. Particles from the concrete pavement outside the facility or dry soil from nearby farmland may have entered the data centre on visitors' clothing or through the air conditioning system. Water used to humidify the data centre's air may also contain chemicals that contribute to the dust in the data centre.



