ISSN: 3139-0862

Data Center Operational and Maintenance Specifications and Procedures

Wing Cheung TANG

BEng(Hons), MEd. PCEd. MSc, MBA, PhD, MCGI, CMgr, FCMI, FIMA, CPMC, FIMC

Adjunct Professor of Jesselton University College, Sabah, Malaysia

tang957031@gmail.com

Abstract—
Data centers have become key infrastructure assets for modern organisations in supporting business continuity, digital service delivery and protection of information assets. This article offers a comprehensive review of data center operation and maintenance (O&M) practices, combining technical specifications, safety procedures, and risk mitigation strategies that are crucial for the resilience of facilities. The analysis is based on five interrelated categories based on industry standards and engineering guidelines: fire protection systems (VESDA systems, gas flooding systems, pre-action sprinkler systems), physical security and access control systems, environmental monitoring by means of Building Management Systems, cooling optimisation (cold/hot aisle arrangements, computational fluid dynamics modelling) and systematic preventive maintenance procedures. The article also discusses the disaster recovery frameworks, safety assessment in the workplace and power system diagnostics. Results indicate that an integrated approach for successful data center O&M is needed considering the need for business continuity (e.g. continuous service delivery, data integrity) and asset protection needs recognising the trade-offs among detection sensitivity, choice of suppression agent and collateral damage risks. There is still knowledge gaps related to long-term performance data on clean agents, standardised benchmarking of O&M effectiveness, and quantitative relationships between maintenance frequency and system reliability metrics.

Keywords—building management systems, cooling optimization, data center operations, disaster recovery, fire suppression systems, preventive maintenance

I. INTRODUCTION

A. Background and Significance

The modern organisational environment is fundamentally reliant upon data center infrastructure to enable mission-critical business processes, digital service delivery, and management of information assets. Data centres are critical business facilities [1] that require continuous services, high reliable electricity backup and fire services. The characterisation points to the high-risk profile of these facilities, which are also high value and high-risk property that require sophisticated operational strategies.

Several converging pressures have driven the evolution of data center operations. First, the accumulation of digital assets requires large investments in data collection, processing and storage (investments that cost lot of time and money). Second, the regulatory frameworks and industry standards (including the ASHRAE [2] TC9.9 specifications) have defined definitive operational parameters that facilities need to satisfy. Third, as information technology equipment becomes denser, it generates more heat than traditional building ventilation can handle, so you need specialised cooling architectures.

B. Scope and Objectives

The article presents a synthesis of technical materials from the training documentation for the professional activity of maintenance and operation of data centers, in terms of five functional areas: fire protection engineering, physical security and access control, environmental monitoring via BMS, cooling system optimisation and preventive maintenance.

The analysis seeks to:

(a) explain the technical features and operational principles of active and passive fire protection systems in data center environments
(b) review security architectures including mantraps, CCTV surveillance and biometric access controls,
(c) analyze cooling strategies, in particular airflow management and thermal efficiency,
(d) document systematic maintenance procedures for critical subsystems including uninterruptible power supplies (UPS), generators, and switchgears, and
(e) identify knowledge gaps and limitations in current practice that warrant further investigation.

C. Methodology and Limitations

The article employs a synthetic review methodology, synthesising and interpreting the technical content of training materials, while pointing out several limitations inherent in it. The source materials are training materials for practitioners, not peer-reviewed empirical research. Thus, there is no systematic reporting of quantitative performance data, longitudinal reliability statistics or comparative effectiveness analyses. Where specific performance metrics are provided (for example, detection thresholds for Very Early Smoke Detection Alarm (VESDA) systems), they are reported as stated, although independent validation data is not available in this source.

The materials also have structural shortcomings: some slides have incomplete figures (e.g., cutting off the “VESDA” page), duplicated information on several slides, and references to appendices or calculation tools that are not provided. These gaps are not filled by assumption but are explicitly noted,

ISSN: 3139-0862

preserving the integrity of the original documentation and making it clear that it is not a research source.

II. FIRE PROTECTION ENGINEERING FOR DATA CENTERS

A. The Fire Triangle

The fire protection strategy described in the training materials begins with basic combustion science, namely the fire triangle model. Fire needs three things at the same time: heat, oxygen, and fuel vapour. Eliminating any one of these components extinguishes the combustion reaction. Data center environments present unique constraints on which suppression mechanisms are appropriate.

According to the materials, the different suppression agents are directed at the components of the fire triangle. Sprinkler systems work by the very high specific heat capacity of water and latent heat of vaporisation to draw heat away. On the other hand, flooding petrol systems remove oxygen and fuel vapour while maintaining the non-conductive properties that are essential for protecting electronic equipment. Passive fire protection configurations use fire retardant and resistance materials to "prevent fire spread out" using compartmentalisation strategies.

B. Fire Classification and Agent Selection

The source materials clearly differentiate between fire class and its suppression requirements, which has significant implications for the design of data centers. Class A fires involve combustibles such as wood, paper and textiles Class B fires [3]: Hydrocarbon fuel fires: Gases or Flammable liquids. Class C fires are electrical fires. This is the one most applicable to data center operations. The classification does note that electrical fires usually include combustible materials as secondary fuels.

In the training documentation the selection matrix says that the water agent is for Class A fires but not for Class B fires and not for Class C fires. Foam agents work well for Class A and B fires, but not for Class C. Gas flooding is specified in Class B & C fires especially for computer/server rooms, office, and workshops not for Class A fires. Interestingly, gas flooding systems are not effective on fires involving ordinary combustibles (paper, wood and textiles) that could be present in data center support areas. This emphasises the importance of hybrid protection strategies or clear compartmentalisation of fuel types.

C. Gaseous Suppression Agents

The training materials include comprehensive technical specifications for several gaseous suppression agents, each with a different environmental, safety and performance profile.

The major disadvantages with Carbon Dioxide (CO_2) are suffocation and loss of visibility. CO_2 is an effective fire suppressant, but it poses unacceptable life safety risks in occupied spaces and is therefore limited to unoccupied equipment rooms or spaces with strict access control during discharge.

FM-200 (heptafluoropropane) absorbs heat, not oxygen. FM-200 [4] is safe in occupied spaces and concentrations up to 9% of volume. The atmospheric lifetime is 31-42 years. It is very persistent in the atmosphere, which has raised environmental concerns and regulatory scrutiny. The agent is still widely used in existing installations.

Inergen (an inert gas mixture, nitrogen-based) works by oxygen reduction with breathable atmospheres. According to the source, inergen removes oxygen from the air but people can still breathe easily; concentration 37.8% minimum, zero atmospheric lifetime. Inergen has zero atmospheric lifetimes, no ozone depletion or global warming potential and is therefore environmentally preferable to fluorocarbon-based agents.

Novec-1230 (fluorinated ketone) [5] is a stored fluid under low pressure, which vaporises when discharged. Materials say it is good for localised flooding, directional spray. Concentration at 4-6%. 5-day atmospheric lifetime. The short atmospheric lifetime offers a significant environmental advantage, but the agent requires special engineering for its discharge dynamics that are different from that of a compressed gas system.

Ecaro-25 is briefly listed as suitable for use in occupied spaces, concentration not to exceed 9%, although the materials provide few further details.

D. Very Early Smoke Detection Alarm (VESDA) Systems

The Very Early Smoke Detection Alarm system is a significant step forward from conventional smoke detection systems. According to the training documentation, VESDA provides the "earliest indication of smouldering before visible smoke," creating critical response windows for disaster procedures. This early warning capability is made possible through high-sensitivity smoke detection (Hwang et al., 2024) technology capable of detecting smoke concentration as low as 0.01% obscuration per metre, whereas conventional smoke detection is 35% only—a difference of two orders of magnitude.

VESDA's operational architecture is based on air sampling through pipe networks: Piping – to draw air through piping to take air samples from the area to be protected with a fan. This contrasts with passive detectors which rely on smoke migration to sensor locations. The display & control panel shows the smoke levels and sounds alarm, and can signal to dry pipe system or pre-action system, integrating detection with suppression activation.

E. Pre-Action Sprinkler Systems

The training materials describe three interlocking configurations for pre-action sprinkler systems, each of which balances the risk of water damage against the certainty of fire suppression.

Non interlocked systems allow the water to dry the pipe upon receiving an activating signal or when a sprinkler activates. This layout offers the quickest application of water but has a potential for water damage from inadvertent sprinkler activation (e.g., mechanical damage of sprinkler heads).

In single interlocked systems, water is introduced into the dry pipe upon receipt of the activating signal, but the system must be verified by the detection system before the pipe is filled. In this configuration, activation of the sprinklers will cause trouble instead of immediate water discharge. This

ISSN: 3139-0862

adds another layer of protection against accidental water discharge while still providing fire suppression capability.

Double interlocked systems have the most rigid safeguards, in that they admit water into the dry pipe when they receive an activating signal and a fusible sprinkler element. This requires both confirmation by the detection system and the thermal activation of sprinkler heads. The spec says that an activation signal will trigger a fire alarm. Opening a sprinkler will trigger a supervisory condition. So, they provide separate notification paths for different failure modes.

F. Active Versus Passive Fire Protection

The materials make a clear distinction between active and passive fire protection systems, a distinction that has regulatory and insurance implications. Active Systems that require activation (automatic or manual) to function, such as a fire sprinkler system or a clean agent fire suppression gaseous system. Smoke detection has multiple active functions for calling for investigation, power interruption (EPO) and manual fire suppression;

Passive fire protection refers to static architectural features like fitting fire walls and fire stopping to openings. These passive measures restrict fires to compartments, reduce oxygen availability and protect egress routes. This is achieved without the need for mechanical activation. The materials indicate that sprinklers are used for structure protection and building life safety, and clean agents are used for business continuity and asset protection, suggesting different protection objectives (life safety versus business interruption prevention).

No collateral damage or cleanup is a key point in the characterisation of clean agents as producing no water. This is an important consideration in the trade-off of fire protection in data centers. Water-based fire protection systems provide reliable and effective fire suppression for structure protection but have risks of consequential damage to electronic equipment. Clean agents provide direct asset protection but may be less effective for deep-seated Class A fires.

III. PHYSICAL SECURITY AND ACCESS CONTROL

A. Layered Security Architecture

The training materials illustrate a multi-layered security model with surveillance, access control, and physical barriers. This multi-layered approach acknowledges that data center security must encompass digital (data) and physical (hardware, media) assets as “digital data safe and physical security are important” for complete protection.

The surveillance layer consists of CCTV monitoring, motion detection, lighting maintenance and recording. Access control includes a variety of mechanisms: doors, fences, gates, man trap, key and padlocks, access cards, guards and escorts, proximity badges, biometric passes. The redundancy means that the compromise of one control does not result in a complete loss of security.

B. Mantrap Configurations

The man trap is a specialised access control device (a revolving “door” to control people access) that addresses the common security failure of tailgating (unauthorised persons following authorised entrants) and piggybacking (unauthorised persons accompanying authorised entrants with or without collusion).

The materials state that data centres demand high requirements for data centre door functions like; separating the public space and hall of data centre, increasing fire safety, optimal burglar resistance, fast opening and closing speed, great access control [6] preventing tailgating and piggyback.

Operational logic is controlled volumes. Typically, there is only one person in the man trap and they need to authenticate at the entry portal, the outer door closes completely, and the inner door requires secondary authentication before the person is allowed into the secure area. Mathematically, this situation prevents piggybacking because the volume cannot contain more than one person at the same time undetected.

C. Access Control Hardware Specifications

The training documentation describes specific access control hardware components with measurable parameters. They are:

- Access card, proximity readers, keypads, RF readers, phone entry, video intercoms
- Audio alert units: Sirens, Strobes, Annunciator panel
- Secondary power backup (important for fail-secure operation during utility outages)
- Break glass release, fire release (including emergency egress override)
- Magnetic lock 150 kg, 300 kg, 600 kg, 900 kg; magnetic contact;

Lock force specifications (from 150 to 900 kilograms of holding force) indicate that security requirements vary by zone within the facility, with higher-force locks protecting the most sensitive areas. The inclusion of both fire release and break glass release mechanisms acknowledges the conflict between security (restricting egress) and life safety (ensuring rapid egress) and provides legal compliance mechanisms for emergency evacuation.

D. CCTV System Architecture

The CCTV specifications include the following analogue and Internet Protocol architectures: The categories of components are:

- Remote video surveillance system
- Digital Video Recorder (DVR) Multi channel
- Types of Cameras: Panoramic, Dome, Pan/Tilt/Zoom, Fixed, Wireless CCTV
- Infrared Illuminators
- PTZ Keyboard Controller Console
- Distribution equipment: Camera Controllers, Video Distribution Amplifiers, Video Switchers, Video Screen Splitters, IP/Networking

Infrared illuminators indicate the need for 24-hour surveillance, and pan/tilt/zoom (PTZ) capabilities allow the ability to do general surveillance of large areas, and forensic analysis of specific events.

E. Environmental Security Considerations

The materials also cover facility sitting and protection of external equipment, as well as active security systems. If equipment for cooling, generators, fuel tanks, or access providers is located outside of the customer space then this equipment should be adequately secured. This acknowledges that peripheral equipment can provide attack surfaces, even if the main data hall is properly secured.

Cameras should be watching common areas such as parking lots, loading docks and building entrances. Critically,

ISSN: 3139-0862

the building should not be in high crime areas—a siting requirement that may conflict with other operational requirements (e.g., proximity to telecommunications infrastructure, power availability, or staff transportation).

IV. BUILDING MANAGEMENT SYSTEMS AND ENVIRONMENTAL MONITORING

A. Functional Capabilities of Building Management Systems

Training materials indicate that Building Management Systems (BMS) are integrated systems that enable remote or centralised monitoring, and they offer improved Human Machine Interface (HMI) capabilities. The documented functions are:

• Control or monitor a comfortable level of the working environment
• Record and monitor Events or Alarms for losses
• Timer or programmable control
• Gather data for trend analysis and reports
• Alarm management for sophisticated systems
• Architecture that scales
• Integration of other building systems for centralised monitoring

The emphasis on expandability and integration suggests that data center BMS implementations will have to accommodate future equipment additions and interconnection of subsystems, without wholesale replacement of the system.

B. Integrated Subsystems

According to the materials, BMS shall incorporate the following building subsystems:

• light system
• electric power control system
• heating installation
• ventilation system
• microclimate system
• conditioning apparatus
• monitoring and security system
• system of access and magnetic cards
•fire alarm systeem
• lifts, lifts etc.
• other engineering systems,

The integration provides centralised visibility and control, but also single-point-of-failure risks if the BMS itself fails or if network communications are interrupted. The materials do not explicitly address BMS redundancy requirements, although typical practice would be redundant servers, dual network paths and fail-safe control logic for critical subsystems.

C. Power Monitoring Specifications

The power monitoring subsystem documentation describes the technical parameters for data collection:

(a) Monitored parameters -- Voltage, Ampere, kVA, kW, kWh, max. demand (kVA), DPF – Displacement Power Factor, TPF – Total Power Factor, THD - Total Harmonics Distortion (THDv, THDi preferred) The preference of THDi (current distortion) over THDv (voltage distortion) is a reflection of the practical reality that data center power quality issues are usually caused by non-linear loads (switching power supplies, UPS input rectifiers) creating current harmonics.

(b) Sampling requirements -- Resolution / Sampling Rate (double of resolution) i.e. Sampling rate 1024/cycle Resolution = (1024/2) -1 = 2ms Half Cycle of 50Hz = 1/50 x ½ = 10ms This is enough temporal resolution to capture sub-cycle events, but the materials mention that 15 minute base is preferred for trend analysis, implying that high resolution data is typically aggregated for long term storage.

(c) Data retention -- Memory size depends on number of data and storage period, minimum 36 months (per BEEO). The monitoring system shall backup the data to Central Server for having 36 months data. The three-year retention requirement supports failure analysis, warranty claims, and regulatory compliance. The materials do not specify which regulation requires this length of time.

D. HVAC Monitoring Parameters

The monitoring requirements for heating, ventilation and air conditioning (HVAC) systems are:

• Measuring flow rate, water temperature and pressure at suction (inlet or supply) and discharge (outlet or return)
• Air temperature and pressure at supply and return and rate of flow
• Outdoor temperature and humidity and fresh air flowrate
• Same power parameters as defined for general power monitoring (Voltage, Ampere, kVA, kW, kWh, max. demand, DPF, TPF, THD)
• Same sampling rate (15 minutes based preferred) and retention (36 months) requirements

By defining both suction and discharge parameters on water circuits, it is possible to calculate heat transfer rates using the fundamental equation $Q = \dot{m} \times c_p \times \Delta T$ (where Q is heating transfer rate, $\dot{m}$ is mass flow rate, c_p is specific heat capacity, and ΔT is the temperature differential).

E. Sensaphone Remote Monitoring

The Sensaphone system is described as a specialised remote monitoring and alarm notification system. Features of alarm include:

• Recorded Voice Message
• Codes for text
• Telephone reading of parameters
• Voice or Pager Outdial
• Customizable timing: Call delay, intercall, max calls, rings prior to answer, call back acknowledge
• Events and Alarms history
• Alarm acknowledgement or notification and reporting capabilities

The system has automated notification pathways that remove the need for constant human monitoring of BMS workstations, allowing for after-hours alerting to on-call personnel through multiple communication channels (voice, text, and pager) with escalation logic.

V. COOLING SYSTEMS AND AIRFLOW MANAGEMENT

A. Data Center Cooling Fundamentals

Cooling is an important operational parameter of the training materials and thermal management directly impacts equipment reliability, energy consumption, and facility capacity. The fundamental problem is that a lot of heat generating IT stuff is crammed into enclosed spaces and electronic components do not like high temperatures.

ISSN: 3139-0862

The materials have the following operational requirements: Dry bulb temperature 18-27 degC, Relative Humidity 60%. These parameters are consistent with those recommended by ASHRAE TC9.9 for data center environmental conditions. The materials do not specify the range of allowable humidity (typically 40-60% relative humidity to balance electrostatic discharge risks vs condensation concerns).

B. Cooling Equipment Taxonomy

The documentation differentiates between different types of cooling equipment:

Chiller systems: Available in Direct Expansion (DX), air cool and water cool configurations. DX systems use refrigerant expansion to cool the air. Chilled water systems use chilled water from central plants.

Air distribution units: Fan Coil Unit (FCU) or Air Handling Unit (AHU) + Variable Air Volume (VAV) for general building cooling not specialised data center equipment.

Specialised cooling for data centers:

• Chilled water for Computer Room Air Handler (CRAH)
• Computer Room Air Conditioner (CRAC) with refrigerant

The distinction between CRAH and CRAC units reflects the heat rejection medium: CRAH units use chilled water coils and require central chiller plants, while CRAC units are self-contained DX systems with integral compressors. The materials say: “CRAC units use centrifugal fans – high pressure to overcome the static pressure of underfloor distribution systems.

C. Un-Notified Cooling Issues

The materials suggest several modes of operational failure that occur when data centers are situated in spaces that were originally designed for general office occupancy:

• These systems are off overnight & weekends (if controlled by building automation systems programmed for office hours)
• Systems designed to operate 5×8 vs. Continuous Operations (weekdays, 8 hours per day, vs. 24×7×365)
• No humidity control and no adequate filtration for IT equipment
• Air used to ventilate buildings eliminates excess moisture, creating the risk of static discharge
• IT equipment overheats due to lack of airflow (Airflow designed for comfort not correct delivery for IT)

These failure modes represent a critical knowledge gap, namely, the assumption by facility managers that general building HVAC can support data center loads without modification. The materials implicitly endorse dedicated data center cooling separate from building comfort conditioning.

D. Cold Aisle or Hot Aisle Configuration

The materials are very explicit about cold aisle or hot aisle arrangement as the basic airflow management strategy. The principle goes:

• Employ cold aisles to route cool air to heat load, and utilise perforated floor tiles to provide conditioned air directly to equipment air intakes
• Hot Aisle – no remix of hot air to server through hot aisles where the equipment exhaust is contained and returned to the cooling units

Operational benefits include prevention of recirculation (hot exhaust entering equipment intakes) and bypass (conditioned air going back to the cooling units without passing through equipment). The materials specify several implementation requirements:

• Position CRAC unit’s perpendicular to hot aisles to pull hot air down the hot aisles
• No vent tiles adjacent to CRAC unit, minimum 0.8-1m" (to prevent short-circuiting)
• Blank plate for efficient air cooling by blocking the air flow to hot equipment
• Fill the gaps in rows and seal the cable cutouts

E. Advanced Airflow Management

The materials document more sophisticated strategies than basic cold/hot aisle arrangements:

(a) Physical containment -- Rigid enclosures that fully separate heat rejected from the rear of the IT rack and cool air intake from the front — either hot aisle containment (enclosing the hot aisle) or cold aisle containment (enclosing the cold aisle). Containment virtually eliminates recirculation, allowing for higher supply temperatures and less fan energy.

(b) Underfloor pressure management -- The materials warn that too high-pressure result in higher fan cost, more energy, more leakage and short circuit of cooling air while too low pressure result in hot spots at the area’s most distant from cooling supply or overcool. The underfloor pressure balance requires careful design of perforated tile distribution, underfloor obstructions and variable fan speed control.

(c) Computational Fluid Dynamics (CFD) -- For a large data centre, a Computational Fluid Dynamics [7] model may be feasible. CFD modelling allows for the quantitative prediction of airflow patterns, temperature distributions, and pressure profiles, thus enabling design optimisation before physical implementation.

F. Emerging Cooling Technologies

The materials document briefly two advanced cooling approaches.

(a) Rack Top Cooling/Spot Cooling -- Localised cooling units at rack level that address hot spots without overcooling entire rows.

(b) Rack Mount Cooling or Inner Cooling -- Cooling built into the rack enclosure, maybe even at the server level. The materials don't provide a lot of technical specifications for this approach.

Also, the materials mention “Winter Mode” in a hybrid cooling arrangement, indicating economiser operation in which outside air provides cooling without mechanical refrigeration—but the documentation does not detail control strategies or geographic applicability.

VI. PREVENTIVE MAINTENANCE AND OPERATIONAL PROTOCOLS

A. Maintenance Philosophy

The training materials describe a holistic philosophy [8] of preventive maintenance based on periodic intervention, not reactive repair. The idea is that the cost of a data center outage is exponentially higher than the cost of regular maintenance and that it makes sense to have a plan for inspections, testing and scheduled replacement of components.

ISSN: 3139-0862

The documented activities cover different subsystems with different periodicities, from daily operator rounds to multi-year major overhauls. Documentation, log-keeping, and qualification of maintenance personnel are emphasised as important elements of effective programs in the materials.

B. Generator Maintenance

The maintenance schedule of the generator is recorded with the following periodicity:

(a) Routine (daily) checks -- fuel level, battery voltage, no fluid leak, generator on 'AUTO' mode, circuit breaker in CLOSE position, no alarm and keep records in logbook

Monthly running tests to charge the battery, all fans/pumps are running properly, all parameters of ventilating system, cooling system, silencer and exhaust system, fuel consumption, temperatures and electrical output parameters are working properly

(b) Quarterly inspections -- Belt tension and wear; clean battery terminals and connections. Check condition of machine, battery and charger, Automatic Transfer System (ATS), spare parts and repair any rusty issue(s)

(c) Annual service -- Change all air/fuel/oil filter, clean/change sparking system, clean radiator system, clean fuel tank, inspect alternator and engine, clean fuel supply system, check all switchgears and room, check the solenoids, check all connections, full load test

The move from daily checks to yearly overhauls is a risk-based prioritisation. Components with high failure rates (belts, filters, batteries) are checked frequently. Components with longer life (alternator windings, engine block) are checked once a year.

C. Uninterruptible Power Supply Maintenance

UPS maintenance requirements emphasise the competence of operators: Operators shall be familiar with O&M manual, operating procedures, equipment setting; keep wiring diagrams, maintenance schedules and maintenance records.

The timetable is as follows:

(a) Daily -- Monitoring, logging and analysis of the system status: system voltage, battery status, output loading, UPS operating status through the UPS monitoring modules

(b) Quarterly -- Visually check for any loose connections, burnt insulation or signs of wear.

(c) Semi-annual -- Visual check for liquid contamination from batteries and capacitors, clean enclosure check room environment (temperature and humidity)

(d) Annual -- Thermal scan to identify hot spot; operational tests; battery rundown test

(e) Biannual -- Transfer switch, circuit breaker and maintenance bypass testing

Thermal scanning is needed during annual inspection due to concern for connection resistance and the possibility of component failure. Temperature rise often precedes catastrophic failure by weeks or months.

D. Cooling System Maintenance

The maintenance of the cooling system is classified into two categories: operational checks and shutdown tests [9].

(a) Operational checks include -- any unusual noise, check of inlet and outlet air temperature (fluid temperature if possible), switching of operating groups, check of pressure and/or flow of coolants, check of running ampere of cooling units, check of position of valve openings, check of all parameters and conditions of central chiller system and condensing units both visually and monitoring system

Shutdown tests (requiring system isolation) consist of:

- Mechanical and electrical are tied closely together
- Lubricate all rotating parts and check belt tensions
- Clean the fans" and "Check or replace the filters or strainers of the cooling unit
- Clean cooling coil or external and internal air path
- Test or calibrate or re-enable all safety features
- Clean and clear drain pipe works and drain pan
- Check for corrosion, moulding
- Clean the pipelines and flush the system (once a year or as per schedule)

E. Switchgear Maintenance

Maintenance of electrical switchgear concerns the transition between utility power, generator power, UPS systems and facility loads. The activities which are recorded are:

- Visually inspect for obvious damage or wear
- Lamps test / periodic test as required / abnormal noise
- Signs of moisture and signs of overheating
- Clean the switch gears and remove dust
- Check the settings, check the connections, check the contacts
- Periodic functional checks or manual operations
- Calibration of Sensors, Measuring Instruments, VT & CT, and Protective Relays
- Periodic inspection, test and certification (PITC)
- Inspection and maintenance log records

The calibration of voltage transformers (VT) and current transformers (CT) shows that measurement accuracy degrades with time which can affect the accuracy of billing (if utility meters are involved) and protection coordination.

F. Work Control Systems: Request to Work and Permit to Work

The materials describe formal work control systems for maintenance activities affecting critical systems:

(a) Request To Work (RTW) system requirements -- working scopes Working period List out affected area / parties and inform stakeholders Safety analysis Risk analysis Technical competents and relevant licenses

(b) PTW system requirements -- Start time, end time, locations, Nos. of persons and personal details, tools carrying, instruments calibration certificates, parts to be replaced and parts returned, confirm the working scopes, inform all stakeholders, Safety at work, briefings, approval from relevant managers.

Separating RTW (planning and scoping) and PTW (authorisation and tracking) provides an audit trail of maintenance activities and ensures that all stakeholders (including IT operations, security, and facility management) are aware of upcoming work that may impact system availability.

G. Log Recording Requirements

The materials require a specific log format for incident recording

- Case no. – preferred date & time format (YYMMDDHHMM)

 ISSN: 3139-0862

• Time of accident – as precise as possible
• Location, accident and impact area details
• Cause investigation – daily/period progress
• Follow up – time, actions taken daily / specific period
• Including check of similar circumstance
• historical records, note / update
• Injury / complaint / indemnity
• PM review / A&A works / Report study / Risk analysis / Professional review
• Report reference (escalated)

The structured format helps in root cause analysis, trend identification, regulatory reporting and in safeguarding the institutional knowledge in case of personnel change.

VII. DISASTER RECOVERY AND BUSINESS CONTINUITY

A. Defining Disaster in Data Center Context

The training materials use a functional definition of disaster that focuses on the disruption of services rather than on specific causes. Disaster includes: fire or flood type disaster that can wipe out a facility, failure of system components, cable cut, and massive local power failure, anything that interrupts service is a disaster, service outages of unknown duration, no disaster recovery plan.

The importance of this definition is that it shifts from dealing with causes to dealing with consequences. Regardless of what the cause of service interruption is, if there is no ability to recover then the disaster condition is met.

B. Consequences of Data Loss

Documented impacts of data loss include: Cascading business impacts:
• Loss of customer goodwill
• Delayed delivery of goods
• Poor decision making
• Negative publicity
• Cash flow problems
• Reputational damages
• Customer churn (misspelt as “churn” in original)
• Financial loss

The inclusion of tangible (cash flow, financial loss) and intangible (goodwill, reputation) consequences points to the importance of considering disaster recovery investments in terms of the total business impact, not simply the direct recovery costs.

C. Hot Standby Versus Cold Standby Configurations

If it is critical services (military, medical) or high value services then hot standby sites are specified this is. The costs are openly admitted in the materials: Hot standby sites are expensive, and include duplicated hardware, duplicated software, duplicated licenses, maintenance, duplicate trunking etc. In addition, periodically testing the hot standby to ensure it is working is expensive and disruptive.

Cold standby systems have duplicate hardware but are offline, are less expensive, but have similar hot standby concerns with testing and maintenance.

Warm standby configurations (intermediate states with some systems online but not fully operational) are not specified in the materials, which is a gap in the coverage of recovery alternatives.

D. Equipment and Service Failure Recovery

In addition to site-wide disasters, the materials address failures at the component level:
• High MTBF (Mean Time Between Failure) system, the higher the MTBF the longer the service time between failures
• Modular system design allows the addressing of major failure by swapping a module.
• Selection of vendor is KEY i.e. local vendor, stock spare parts, emergency call and contingency plan
• Backup data and store it off-site on a routine basis"
• Hardware redundancy BUT is it worth it for your business? — acknowledging that any duplication must be justified by risk assessment
• Failure of services can be solved by alternative networks
• Cloud service useful during services failure

The vendor selection material acknowledges that equipment reliability (MTBF) is only one consideration, and that maintainability (Mean Time to Repair, parts availability) and quality of support may be equally important factors for operational continuity.

VIII. WORKPLACE SAFETY AND HAZARD ASSESSMENT

A. Data Center-Specific Safety Hazards

The training materials identify a full set of safety hazards specific to data center environments, making the analysis different from general workplace safety guidance:
• All persons will be required to wear Personal Protective Equipment (PPE)
• Right handtools, insulated tools for electrical works, testing instruments
- Training programme for the relevant staffs
(a) Environmental risks:
• Noisy – fans, drives, air-conditioning, UPS etc. – possibly exceeding occupational exposure limits
• Insufficient space, narrow rack space – ergonomic and access risks
• Static electricity: shock hazard to personnel and equipment damage hazard
• Cold and windy, may be dusty
• Low illuminance (light shallowed into the rack) or during power outages
(b) Electrical hazards:
• Dual power sources create isolation issues and potential shock hazards – a large hazard only in data centers where equipment might still be energised by alternative sources when primary power is isolated.
• Poor earthing
(c) Operational risks:
• Distance from EXIT and narrow entrance – egress barriers
• Housekeeping issues (tools are too far or no track record)
• Power tools.
• Works in adverse weather conditions (for external equipment or facilities with outdoor plants)
• Works under pressure and overtime hours
• Not multi-discipline to know all systems – knowledge gaps = unsafe actions

B. Hazard Assessment Categories

The materials identify hazard assessment domains including:
• Health and Safety for Yourself

 ISSN: 3139-0862

• Fire Protection
• Flood
• Safety
• Nuisance
• Temperature / Humidity
• IAQ [Indoor Air Quality], environmental issues
• Unusual conditions
• Change to alternative sources
• Power failure
• Air infiltration
• Hot Spots

This assessment framework covers safety, operational and environmental issues. Hazards may be latent (e.g. developing hot spots) and not immediately dangerous.

C. Power System Diagnostic Logic

Materials include a troubleshooting table for power system malfunctions that leads from symptoms to possible causes:

Symptom	Failure Logic
One equipment malfunction	Equipment failure; Fuse burnt
Power script no power	Fuse of power script burnt; Unplugged; Breaker trip at PDU
Racks system A power lost	PDU, UPS, LV system issues
UPS power running	Both primary power and secondary power not available; Check if secondary power available within ONE minute; If both primary and secondary power failed, start emergency procedures within UPS backup time
Generator power running	Utility power failure; Continuous running if fuel supply keeps

The diagnostic logic stresses the need for time-critical decisions: if secondary power is not restored within one minute, operators must prepare for UPS battery depletion and possible generator start (or load shedding).

IX. SYNTHESIS AND IDENTIFIED GAPS

A. Thematic Synthesis

Cross-cutting themes across the five technical domains considered (fire protection, security, environmental monitoring, cooling, and maintenance) are:
(a) Integration versus isolation -- Effective data center operations require integrated subsystems (BMS linking fire, security, power and cooling) with isolated failure modes (fire compartments, electrical separation, cooling circuit independence) This tension demands careful architectural decisions as to when integration provides benefits and when isolation is necessary for reliability.
(b) Detection sensitivity / response time -- The VESDA specification (0.01% obscuration detection versus conventional 3-5%) is an example of a broader trend: earlier detection provides more options for response but a higher risk of false alarm. Similar trade-offs can be observed in pre-action sprinkler design (non-interlocked vs double-interlocked) and gas flooding agent choice (suppression rate vs environmental persistence).
(c) Risk mitigation strategy – preventive maintenance -- Systematic intervention prevents catastrophic failures, as detailed maintenance schedules for generators, UPS systems, cooling equipment and switchgears show. That said, the materials do not offer quantitative justification for particular periodicities (e.g., why annual battery rundown tests, not semi-annual), implying a reliance on industry convention rather than empirical optimisation.
(d) Human factors and organisational learning -- The RTW/PTW work control systems, structured log formats, and training requirements embody the appreciation that technical systems alone are not enough. Human performance, documentation, and continuous improvement are needed for operational resilience.

B. dentified Knowledge Gaps

There are a few major gaps in the source materials that limit the completeness of the analysis:
(a) Missing quantitative reliability metrics -- MTBF is mentioned, but no numeric MTBF figures are provided for any type of equipment in the materials, no Mean Time to Repair figures, or achieved availability figures, or any quantitative relationships between maintenance frequency and failure rates. This gap does not allow cost-benefit analysis of maintenance investments.
(b) Validation data for the detection system is not available -- VESDA sensitivity specifications (0.01 percent obscuration) are provided without false alarm rate data, nuisance alarm frequency, or field performance validation. These metrics are necessary to evaluate the practical utility of high sensitivity detection.
(c) Incomplete specification of environmental parameters -- The operational requirements specify "Relative Humidity 60%" with no acceptable range (e.g. ±10%), dew point limits or justification for why 60% is the optimum. The ASHRAE TC9.9 reference suggests these details are in the source standards, but they are not replicated in the training materials.
(d) Unreferenced regulatory references -- The 36-month data retention requirement is attributed to “BEEO” (unknown acronym) with no citation. Fire installation certification “FS251” (no jurisdiction specified). The documentation provided does not permit verification of these references.
(e) Incomplete figures and missing appendices -- Some figure references seem to be place-holder or incomplete content. References to Design Calculation, Design Tool, Sprinkler Notes and other appendices (1.0.70 through 1.0.82) are included, but no content.
(f) Limited treatment of emerging technologies -- The materials discuss rack-level cooling and CFD modelling, but provide no guidance for implementation, cost estimates, or comparative effectiveness data. "Cloud service helps during services failure" is not elaborated on which services, which failure modes, or which contractual architectures.
(g) Lack of economic analysis -- No cost data are given for any system or maintenance activity. Thus, it is not possible from this source alone to assess the relative cost-effectiveness of different fire suppression agents, security configurations or cooling strategies.

C. Methodological Limitations of Source

This is a training document, not peer-reviewed research, with natural limitations for academic synthesis:
(a) Authority and verification -- References to external standards (ASHRAE, EMSD CoP Wiring Regulation [10]) suggest alignment with recognised authorities, but are not elaborated in full.
(b) Generalisability -- The Hong Kong context (referenced

ISSN: 3139-0862

through EMSD CoP, Hong Kong Observation) may affect applicability to other regulatory jurisdictions. Electrical codes (50Hz reference, implying European/British derived systems), fire codes, building codes are all very different from region to region.
(c) Recency -- The undated materials may not reflect current technologies (e.g., Novec-1230 introduced around 2007, VESDA available since the 1990s). There is nothing on recent developments in lithium-ion battery UPS systems, liquid immersion cooling, and AI-driven BMS analytics.

X. IMPLICATIONS FOR PRACTICE AND RESEARCH

A. Practice Implications

The synthesised materials support multiple practice recommendations for data center operators and facility managers:
(a) Add detection and suppression to operating procedures -- Documentation shows that VESDA can provide an earlier warning than traditional smoke detection, allowing for a response before there is visible smoke to see. But this capability is only useful if procedures for investigation, decision and possible manual suppression are in place prior to automatic system discharge. Drills should test the entire chain of responses, not just whether the equipment works.
(b) Select agent based on risk profile -- The tradeoffs between gas flooding agents (CO_2 suffocation risk, FM-200 atmospheric persistence, Inergen zero environmental impact but higher required concentration, Novec-1230 short atmospheric life but lower concentration) must be in line with organisational priorities about life safety, environmental footprint, and suppression effectiveness. No single agent is best on all criteria.
(c) Validation of cooling assumptions measurement -- The un-notified cooling issues (systems designed for 58 operations, insufficient filtration, and inadequate airflow for IT equipment) indicate that building HVAC capabilities must be validated, not accepted. Replace dependence on design documents with perforated tile air flow measurements, underfloor pressure mapping and rack inlet temperature monitoring.
(d) Implement work control systems for all maintenance -- The RTW/PTW framework in the materials should not be restricted to major interventions but expanded to routine activities that might affect system availability. Even filter changes or battery inspections can trigger alarms, affect cooling distribution or introduce safety hazards if not well-coordinated.

B. Research Implications

The gaps identified suggest a number of research priorities for academic researchers:
(a) Quantitative studies of maintenance optimization -- There is a lack of empirically derived maintenance periodicities, indicating a need for reliability-centered maintenance (RCM) studies focused on data center equipment. Possible research questions are: What is the optimal battery testing frequency, that is, that can maximise the detection of failures and minimise the battery cycle life? How does change in filter frequency affect energy efficiency of cooling system? Do recommended service intervals correspond to observed failure distributions?
(b) Comparative effectiveness of detection methods -- Field studies comparing the false alarm rate, response time and maintenance requirements of VESDA against conventional smoke detection would assist with technology selection decisions. Likewise, an investigation of pre-action sprinkler configurations (non-interlocked vs. single vs. double interlocked) in terms of both fire protection effectiveness and accidental discharge rates would close an important knowledge gap.
(c) Economic valuation of resilience investment -- The materials mention redundant hardware and hot standby configurations but do not provide a cost-benefit framework. Research on decision-support tools for resilience investments (including outage costs, equipment failure probabilities, recovery time objectives and investment costs) would enable more rational allocation of data center capital and operating budgets.
(d) Human factors in data centre operations -- The safety hazards identified (dual power sources causing isolation problems, not multi-discipline to familiarise all systems) suggest research opportunities in training effectiveness, alarm response under stress, and cognitive load during emergency procedures. Experimental studies of data center simulators may help identify interventions to reduce operator error during high-consequence events.

C. Policy and Standards Implications

Regulatory references are lacking and jurisdictional ambiguity provides opportunities for standards development:
(a) Harmonised standards Maintenance documentation -- The materials' log format (YYMMDDHHMM case numbering, structured incident fields) could serve as a basis for industry-wide maintenance data standards, enabling benchmarking and failure mode analysis across organizations.
(b) Performance based maintenance requirements -- Current regulations are often based on periodicities (e.g., annual full load test) rather than performance metrics (e.g., generator shall start and accept full load within 10 seconds of utility failure, demonstrated quarterly). Research that links maintenance actions to performance outcomes could enable evolution toward performance-based standards.

XI. CONCLUSION

This article synthesises technical documentation on data center operations and maintenance in five functional areas: fire protection engineering, physical security and access control, building management systems and environmental monitoring, cooling system optimisation, and preventive maintenance protocols. The analysis shows that successful data center O&M is a combination of several specific subsystems, keeping the independent failure modes separate, finding the right trade-off between high detection sensitivity and risk for false alarms, and having in place well documented systematic preventive maintenance programs rather than reactive responses.

The source materials provide extensive technical detail on fire suppression agent specifications (FM-200, Inergen, Novec-1230, CO_2, Ecaro-25), detection system capabilities (VESDA providing 0.01% obscuration sensitivity versus conventional 3-5%), security architectures (mantraps, magnetic locks from 150 to 900 kg holding force), cooling configurations (cold/hot aisle, containment, CFD modelling),

ISSN: 3139-0862

and maintenance schedules (generator monthly runs, UPS annual thermal scanning, switchgear periodic inspection and testing certification).

However, there remain significant gaps in the documented knowledge base, including no quantitative reliability metrics, no false alarm rates of detection systems, incomplete regulatory citations, and no economic analysis of any sort. The materials are based on current practice as documented in professional training rather than validated empirical research. The Hong Kong context may limit generalisability to other regulatory environments.

The materials support practitioners in implementing integrated detection-and-response procedures, risk-aligned agent selection, validated cooling assumptions, and comprehensive work control systems. The identified gaps point to research priorities for researchers, such as quantitative maintenance optimisation studies, comparative effectiveness research on detection technologies, economic valuation frameworks for resilience investments, and human factors research in data center operations.

The robustness of the operation of data center infrastructure depends ultimately not only on the technical specifications of individual subsystems, but on their integration into coherent operational strategies supported by trained personnel, documented procedures and continuous improvement processes. The materials synthesised herein provide the basis for such strategies while at the same time highlighting the significant research required to optimise them.

REFERENCES

[1] Ahmed, K. M. U., Bollen, M. H., & Alvarez, M. (2021). A review of data centers energy consumption and reliability modeling. *IEEE access*, *9*, 152536-152563.

[2] ASHRAE Technical Committee 9.9. (2015). *Data Center Networking Equipment – Issues and Best Practices*. American Society of Heating, Refrigerating and Air-Conditioning Engineers.

[3] Husar, B., Kovalyshyn, V., Marych, V., Lozynskyi, R., & Pastukhov, P. (2019). Combined extinguishing of class D, class A and class B fires. *Fire Safety, 35*, 30-34.

[4] Fan, R., Wang, Z., Guo, W., & Lu, Y. (2022). Experimental and theoretical study on the suppression effect of CF3CHFCF3 (FM-200) on hydrogen-air explosion. *International Journal of Hydrogen Energy*, *47*(26), 13191-13198.

[5] Liu, S., Zhang, X., & Zhou, X. (2024). Fundamental mechanism and potential optimization methods for the overpressure phenomenon of Novec 1230 and 2-BTP. *Combustion and Flame*, *269*, 113704.

[6] Botchway, E. A., Agyekum, K., Pittri, H., & Lamina, A. (2024). Deployment of physical access control (PAC) devices in university settings in Ghana. *Frontiers in Engineering and Built Environment*, *4*(1), 1-14.

[7] Vinuesa, R., & Brunton, S. L. (2022). Enhancing computational fluid dynamics with machine learning. *Nature Computational Science*, *2*(6), 358-366.

[8] Kundu, K., Cifone, F., Costa, F., Portioli-Staudacher, A., & Rossini, M. (2022). An evaluation of preventive maintenance framework in an Italian manufacturing company. *Journal of Quality in Maintenance Engineering*, *28*(1), 37-57.

[9] Abdel-Aziz, M. H., Hussien, M. F., El-Ashtoukhy, E. S. Z., Sedahmed, G. H., & Gheriany, I. E. (2025). Kinetics of mineral scale removal/dissolution for effective cooling system maintenance. *Chemical Papers*, *79*(2), 761-774.

[10] Electrical and Mechanical Services Department. (2025). *Code of Practice for the Electricity (Wiring) Regulations*. Hong Kong SAR Government.