ICONAG
make buildings smarter

PRESSEMITTEILUNG

Februar 2022

Gebäudeleittechnik im Rechenzentrum

Checkliste zum Einsatz einer Management- und Bedieneinrichtung (MBE) mit Energiemanagementsystem (EnMS) in Rechenzentren

Aufgabe ist das Management der Infrastruktur eines Rechenzentrums. Die MBE ist Teil des Datacenter Infrastructure Management (DCIM) mit folgenden Zielen:

- Die effektive Überwachung aller Systeme im Rechenzentrum mit einem schnellen Überblick über den Zustand der gebäudetechnischen Anlagen
- Die Sicherstellung der Betriebssicherheit beziehungsweise Hochverfügbarkeit des Rechenzentrums
- Die Transparenz für einen energieeffizienten beziehungsweise klimaneutralen Betrieb*
- Die Verrechnung von Kosten

**Gemäß dem Green Deal der EU-Kommission von 2021 soll der gesamte ICT-Sektor bis 2030 klimaneutral sein, ohne Möglichkeit, sich über CO2-Zertifikate freizukaufen. Der Weg ist grob umrissen „more energy efficient, reuse waste energy, and use more renewable energy sources“.*

Rechenzentren benötigen 16 Milliarden Kilowattstunden im Jahr 2020 (das sind 2,7 Prozent von 559 Mrd. kWh Gesamtverbrauch in Deutschland). Der Stromverbrauch eines Rechenzentrums setzt sich zusammen aus rund 50 Prozent für die IT-Komponenten und rund 50 Prozent für die Kühlung. Die Handlungsempfehlungen des Umweltbundesamtes lauten: Mehr Transparenz durch einen verpflichtenden Energieausweis und einen CO2-Fußabdruck pro Service- oder Übertragungseinheit.

Diese Punkte sollten bei der Planung und Umsetzung einer Management- und Bedieneinrichtung (MBE) mit Energiemanagementsystem (EnMS) in Rechenzentren beachtet werden

1. **Betriebssicherheit und Hochverfügbarkeit:**
   Damit das Rechenzentrum zuverlässig mit Strom für den Rechnerbetrieb versorgt wird, gilt es, die Funktion der Klima- und Kältetechnik, Netzersatzanlage (NA) und der unterbrechungsfreien Spannungsversorgung (USV) permanent zu überwachen und sicherzustellen. Auf folgende Punkte sollten Sie für Ihre MBE mit EnMS besonders achten:
   - Sie brauchen eine zuverlässige und strukturierte Übersicht über alle Störungen und Ereignisse, die die Betriebssicherheit Ihres Rechenzentrums in irgendeiner Form beeinträchtigt können. Hierfür muss Ihre Management– und Bedieneinrichtung für die Gebäudetechnik ein leistungsfähiges Alarm- und Event-Management vorhalten. Über Filter und Rollen müssen Sie sicherstellen, dass den Verantwortlichen die jeweils für

ICONAG-Leittechnik GmbH
Vollmersbachstraße 88 | D-55743 Idar-Oberstein
Tel.: +49 6781-56234-0 | E-Mail: info@iconag.com

ihren Zuständigkeitsbereich relevanten Informationen zur Bearbeitung bereitgestellt werden.

- Alarme und Events müssen nach Bereitschaftsplan und Zuständigkeit auf mobile Meldegeräte wie Smartphones oder Pager übertragen werden. Eskalationsketten müssen eingerichtet werden, um sicherzustellen, dass kritische Alarme auch sicher zeitnah bearbeitet werden.
- Ihre Mitarbeiter benötigen unter Umständen einen Fernzugriff auf das System. Hierfür sollte es als Webserveranwendung im HTML5-Format bereitgestellt werden, damit zur Fehlerdiagnose und Behebung von beliebigen Clients (Desktop, Tablet, Mobiltelefon) darauf zugegriffen werden kann. Wichtig dafür ist auch eine durchdachte und sichere Zugriffskontrolle in das Firmennetzwerk hinein, die mit der IT abzustimmen ist.
- Stellen Sie sicher, dass sowohl Ihr Managementsystem als auch die korrespondierenden SQL-Datenbanken als Cluster ausfallsicher sind. Hier sollten Sie von Anfang an eine entsprechende Redundanz vorsehen. → *ein Clusterbetrieb im Sinne einer A-/B-Redundanz hilft, wenn die Übertragungswege auch entsprechend vorgehalten werden.*
- Sorgen Sie für schnelle und zuverlässige Alarmierungs- und Eskalationswege im Falle von Störungen, zum Beispiel per SMS und/oder Mail. Diese sollten auch unabhängig von Ihrer eigenen IT-Infrastruktur funktionieren.

2. Monitoring im Sinne der ISO 27001

Die ISO27001 als Norm zur Informationssicherheit fordert, dass Daten vertraulich bleiben, deren Integrität und Verfügbarkeit sichergestellt wird. Daraus ergeben sich vielfältige Überwachungsanforderungen an die Gebäudetechnik, die in Form von Betriebsdaten und -meldungen zu dokumentieren sowie als Störungsmeldungen zu bearbeiten sind. Beispiele hierfür sind

- Monitoring der Netzersatzanlage samt der Füllstande ihrer Betriebsstoffe
- Monitoring der Netzeinspeisung
- Monitoring der USV-Anlagen
- Monitoring der Stromverteilung an den Stromschienen in den Racks
- Monitoring der Kälteerzeugung
- Monitoring der Raumluft- und Klimatechnik in den Serverräumen
- Türüberwachung zur Sicherstellung der Funktionalität von Zutrittskontrollanlagen und Einbruchmeldeanlagen, gegebenenfalls inklusive einer Integration der Videoüberwachung
- Überwachung der Betriebszustände der Löschanlage
- Überwachung auf Wasserleckage im Doppelboden
- Status der Brandmelde- und Einbruchmeldetechnik
- Grundsätzliche Auslastung der gebäudetechnischen Anlagen zur Absicherung der Notwendigkeit eines etwaigen Redundanzbetriebes.

3. Klimaneutralität und Energie-Kennzahlen

Die Sicherstellung eines energie- und ressourceneffizienten Betriebs Ihres Rechenzentrums ist zentrale Aufgabe im Kontext des Green-Deals der EU und der Klimawende. Zusätzlich sind die Energiekosten ein wichtiger Wirtschaftlichkeitsfaktor. Hierauf sollten Sie achten:

- Sehen Sie eine möglichst tiefe Erfassung von Energieverbrauchsdaten vor, insbesondere um die für die IT-Infrastruktur benötigte Energie getrennt von den gebäudetechnischen Energieverbräuchen zu erfassen.

- Sehen Sie in jedem Fall ein System vor, dass Energiemonitoring und Controlling samt Auswertungen (Energiemanagement-System) und die Möglichkeit des Eingriffs in die Anlagen als Management- und Bedieneinrichtung in einem System vereint. So können Sie bei Ausreißern im Energieverbrauch über das gleiche System unmittelbar eingreifen und Fehler abstellen. So sparen Sie Energie und Zeit.
- Achten Sie auf ein flexibles Reporting-Werkzeug, um die für Ihre Organisation relevanten Kennzahlen nach EN50600 in Ihrem Managementsystem abbilden zu können. So sollten grundlegende Kennzahlen wie die Power Usage Effectiveness im Standard einfach abbildbar sein.
- Sorgen Sie dafür, dass Sie alle notwendigen Auswertungen wie Energieausweis oder CO2-Fußabdruck pro Service- oder Übertragungseinheit auf Knopfdruck abrufen können.
- Automatisieren Sie die regelmäßige Erstellung und Verteilung von Energie-Berichten.
- Da Sie nicht davon ausgehen können, immer 100 Prozent der Energiezähler über das Netzwerk auslesen zu können, sollten Sie eine leistungsfähige manuelle Erfassung von Zählerdaten und Energieverbrauchsdaten ermöglichen.
- Ihr System muss auch die Generierung von virtuellen Messstellen auf Basis von mathematischen und logischen Funktionen ermöglichen, damit Sie die Zählermatrix Ihres Rechenzentrums abbilden können und im System wichtige Kennzahlen bilden und verarbeiten können.

4. IT-Sicherheit und Systemarchitektur

Aus den Anforderungen an die IT-Sicherheit ergeben sich die wichtigsten nichtfunktionalen Anforderungen an Management- und Bedieneinrichtungen sowie Energiemanagement-Systeme. Auf folgende Punkte sollten Sie für Ihre MBE mit EnMS besonders achten:

- Für einen effizienten Betrieb brauchen Sie ein technisches Management-System. Egal ob Sie Betreiber und/oder Bauherr sind: Machen Sie klare Vorgaben an das System, unabhängig von den Eigentumsverhältnissen.
- Überprüfen Sie, ob bei einer Virtualisierung Ihrer Management- und Bedieneinrichtung diese auch dem Redundanz-Szenario standhält. Ansonsten verzichten Sie auf eine Virtualisierung und lassen Sie den MBE-Server auf einem eigenen Rechner unabhängig vom Rechenzentrum laufen.
- Die Bedienung Ihres Managementsystems sollte ohne spezifische Softwareinstallation über Browser möglich sein. Achten Sie dabei auf eine rein HTML5-basierte Umsetzung, die von allen Browsertypen unterstützt wird und sichern Sie die Kommunikation über ein SSL-Zertifikat ab.
- Trennen Sie das tendenziell unsichere gebäudetechnische Netzwerk durch sichere Gateways von dem Monitoring-Netzwerk. So stellen Sie sicher, dass keine unberechtigten Eingriffe in die gebäudetechnische Infrastruktur erfolgen können.
- Sehen Sie eigene Bedienplätze samt für die Betriebskollegen angepasster Dashboards in den Infrastrukturräumen sowie an der Netzersatzanalage vor. So stellen Sie sicher, dass die Kollegen im Falle eines Falles alle Informationen und Möglichkeiten vor Ort zur Verfügung haben, um schnell die richtigen Entscheidungen zu treffen.
- Zur Umsetzung der allgemeinen Anforderungen an die IT-Sicherheit sollte sich Ihr Management-System in das Berechtigungssystem Ihres Unternehmens integrieren. Dies erreichen Sie zum Beispiel über eine Authentifizierung über Microsoft Active Directory
- Gleichzeitig müssen Sie häufig externen Nutzern wie Dienstleistern Zugriff gewähren können, so dass das System zusätzlich eine eigene Berechtigungsvergabe mit Rollen- und Rechtevergabe benötigt.

- Klären Sie mit Ihrer IT-Abteilung, ob für Ihr Unternehmen Cloudanwendungen für die Verarbeitung der Betriebsdaten und personenbezogenen Daten in Frage kommen. Viele Unternehmen legen Wert darauf, dass ihre Systeme komplett in der eigenen IT-Infrastruktur ohne Anbindung an externe Cloud-Dienste funktionieren. Falls das so ist, schreiben sie es entsprechend vor.

5. Standardisierung und Duplizierbarkeit

Wenn Sie mehrere Rechenzentren planen oder betreiben, ist es wahrscheinlich, dass sich die gebäudetechnische Ausstattung ähnelt. Wenn das der Fall ist, können Sie insbesondere von einer Standardisierung profitieren. Dabei sollten Sie folgendes beachten:

- Führen Sie ein einheitliches Kennzeichnungssystem ein, das auch die Benennung der Datenpunkte für jede technische Funktion umfasst (zum Beispiel eindeutige Kennzeichnung von Soll- und Istwerten, Fehlermeldungen etc.).
- Ihre Management- und Bedieneinrichtung muss es ermöglichen, Bildvorlagen zur Bereitstellung der Bedienfunktionen zum Beispiel für Anlagenbilder vorzuhalten. Dadurch pflegen Sie jedes Bild nur einmal. Über das Kennzeichnungssystem steuern Sie dann, welche Datenpunkte verknüpft werden.
- Legen Sie idealerweise für jede Anlage und jedes Aggregat verbindlich fest, über welches Automationssystem Sie zu erschließen und zu vernetzen sind (zum Beispiel BACnet oder ModBus). Legen Sie konkret fest, welche Objekte (Datenpunkte) für welche Funktionen zu verwenden sind. Bei BACnet bietet der BACtwin von Kranz/Fritzenwallner („Digitaler Zwilling der Gebäudautomation“) eine gute Grundlage.
- Wenn Sie sichere hochverfügbare und sichere Datenverbindungen zwischen Ihren Rechenzentren betreiben, macht es in der Regel Sinn, anstelle verschiedener lokaler Systeme ein entsprechend verfügbares zentrales Management-System aufzubauen. Legen Sie dieses so aus, dass Sie jederzeit einfach weitere Standorte integrieren beziehungsweise auch ausgliedern können.

6. Schnittstellen

Für die Zukunftssicherheit Ihres technischen Gebäudemanagement-Systems brauchen Sie Zugriff auf Daten. Ob zur Umsetzung eines ganzheitlichen Infrastruktur-Managements, zur Digitalisierung Ihrer Prozesse wie der Verrechnung von Energiekosten oder zur kontinuierlichen Verbesserung Ihrer Energieeffizienz nach ISO 50001: das alles wird unmöglich, wenn Ihre Daten in einem proprietären Datenfriedhof liegen und/oder nicht interpretierbar sind. Wenn Sie hier keine Vorgaben machen, verbauen Sie sich wichtige Potenziale zur Kosten- und Ressourceneffizienz. Auf folgende Punkte sollten Sie besonders achten:

- Fordern Sie, dass alle Betriebsdaten im System über offene und dokumentierte Schnittstellen (API = Application Programming Interface) für die Kommunikation mit Drittsystemen bereitgestellt werden.
- Verdeutlichen Sie sich Ihre Monitoring-Anforderungen anhand der abzubildenden hierarchischen Ebenen sowie Ihre zu unterstützenden Prozesse. Dann leiten Sie daraus ab, zu welchen Systemen Sie Schnittstellen seitens der Management- und Bedieneinrichtung benötigen. So stellen Sie sicher, dass zum Beispiel Ihr Help-Desk, Ihre ERP-Systeme zur Kostenverrechnung, Ihre Wartungsdienstleister oder andere Systeme einfach an Ihre Gebäudetechnik andocken.

Die Umsetzung der oben aufgeführten Punkte wird in der Regel nicht zu nennenswerten Mehraufwendungen führen. Im Gegenteil: bei einer konsequenten Umsetzung werden Sie Ihr Rechenzentrum kosten- und ressourceneffizienter betreiben, auch um den Anforderungen an Klimaneutralität aus dem Green Deal der EU-Kommission gerecht zu werden.

ICONAG hat mit B-CON DC (Data Center) eine Software als Management und Bedieneinrichtung speziell für Rechenzentren entwickelt.

Über ICONAG:

Die ICONAG-Leittechnik GmbH in Idar-Oberstein ist ein international agierendes Unternehmen, das sich auf die Entwicklung und Vermarktung von Softwarelösungen für die Digitalisierung des technischen Gebäudemanagements spezialisiert hat. Das Ziel seit der Gründung im Jahr 1996 ist, die Betriebsführung von Gebäuden in einer zunehmend komplexen Techniklandschaft zu vereinfachen und den Energieverbrauch zu senken. Die Grundvoraussetzung dafür lautet: alle technischen Funktionen und Informationen aller Gewerke müssen in einem Managementsystem zusammengefasst werden.

Weitere Informationen: www.iconag.com

ICONAG-Leittechnik GmbH
Vollmersbachstraße 88 | D-55743 Idar-Oberstein
Tel.: +49 6781-56234-0 | E-Mail: info@iconag.com