Oktober 2025

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

LoRaWAN in der Smart City

von Frederik Stückemann
Das Thema Smart City gewinnt zunehmend an Bedeutung und wird immer mehr zum Aushängeschild für eine Stadt. Viele Städte setzen bereits Maßnahmen um, sammeln Daten, um Abläufe zu optimieren und idealerweise Kosten zu sparen. Das Problem dabei: Nicht jeder Abfalleimer oder Parkplatz lässt sich per Kabel anbinden. Daher bedarf es hier einer Alternative.

Seite 10

Die Unterscheidung zwischen IT und OT ist nicht mehr zeitgemäß

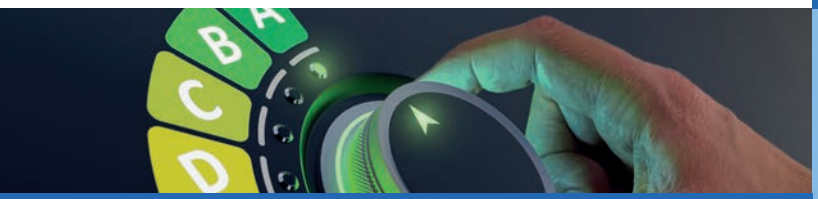
von Dr. Behrooz Moayeri
Seit Jahren gehen meine ComConsult-Kollegen im häufig besuchten Seminar IT-Infrastrukturen für Smart Buildings auf die Verschmelzung von IT (Information Technology) und OT (Operational Technology) ein. Die Unterscheidung zwischen IT und OT ist nicht mehr zeitgemäß.

Seite 2

Ceph in Proxmox – verteiltes Storage im praktischen Einsatz

von Chantal Haidl
Die Wahl der richtigen Storage-Lösung ist für jede Virtualisierungsumgebung entscheidend. Gerade bei Clustern kann die Speicherperformance darüber entscheiden, ob ein System produktiv genutzt werden kann oder nicht.

Seite 15



Webinar der Woche

EnEfG und energetische Optimierung

Seite 28

Schiffe sind die besseren Smart Buildings!

von Dr. Joachim Wetzlar
Haben Sie schon einmal an einem Kreuzfahrtschiff hochgeschaut? Oder sind Sie sogar schon darauf mitgefahren und haben vom obersten Deck aus heruntergeblickt? Jedenfalls übertreffen die Dimensionen in der Regel die eines Hochhauses.

Seite 29

Die Unterscheidung zwischen IT und OT ist nicht mehr zeitgemäß

von Dr. Behrooz Moayeri

Historische Unterscheidung

Als in den 1980er-Jahren mein Berufsleben begann, fanden Computer in den zwei Bereichen Administration und Fertigungsautomatisierung bereits Anwendung. Aber innerhalb einer Firma waren diese beiden Bereiche weitgehend getrennt. Die Trennung war so ausgeprägt, dass sogar Rechnerarchitekturen, Netze und Lieferanten der Technik für die beiden Bereiche kaum Überschneidung aufwiesen. Eine typische Aufteilung war der Einsatz von Großrechnern mit angeschlossenen Terminals vor allem in Büros für die Administration und den damals neuen Ethernet-basierenden Netzen in der Fabrik. Nicht ohne Grund war die erste Variante von Ethernet ein robustes gelbes Koaxialkabel (Yellow Cable), entwickelt für die Verlegung in der Fabrikhalle.

Es gab noch eine dritte Computer-Welt, entstanden in den Universitäten, genannt das Internet. Wenige haben geahnt, dass die Internet-Protokollfamilie ab Mitte der 1990er-Jahre das Bindeglied zwischen den Administrations- und den Fertigungsnetzen werden würde.

Warum erwähne ich die Kombination von Büro- und Fabriknetzen? Weil die Industrie historisch und aktuell der Vorreiter von OT ist. Das später so genannte Internet of Things (IoT) war spätestens seit den 1980er-Jahren für die mit moderner Industrie Vertrauten nichts Neues, sondern nur die Weiterentwicklung der vernetzten Fabrikhalle.

Unterschiede im Betrieb

Ich weiß nicht, welcher Anteil derjenigen, die diese Zeilen lesen, noch die Begriffe White Collar und Blue Collar kennen. Die Leute mit weißen Kragen waren im Berufsleben des 20. Jahrhunderts und davor gegenüber den Arbeitern mit blauer Kleidung privilegiert, hatten einen auf normale Arbeitszeiten beschränkten Arbeitsalltag und bekamen auch mehr Gehalt. Sogar die Entlohnung hatte mit Gehalt und Lohn unterschiedliche Namen. Die Computer in den Büros mussten nur zu den normalen Arbeitszeiten am Leben gehalten werden, weil abends, nachts und am Wochenende kaum jemand damit arbeitete.

Dagegen gibt es seit der Entstehung der modernen Fabriken in diesen einen Schichtbetrieb. Alles, was für die Industrie unerlässlich ist, muss während aller Schichten, oft rund um die Uhr und an allen Tagen des Jahres, funktionieren. So auch die Computer, die vor 40 bis 50 Jahren in die Werkhallen einzogen.

D.h. die Büro-EDV (Elektronische Datenverarbeitung) und die Prozessdatenverarbeitung (PDV) waren nicht nur technologisch, sondern hinsichtlich ihrer Betriebsprozesse sehr unterschiedlich.

Die Welten wachsen zusammen

Was ich über die historische Trennung zwischen Büro-IT und Industrieumgebungen geschrieben habe, galt mit zeitlichem Versatz auch für andere OT-Umgebungen, zum Beispiel für die

LoRaWAN in der Smart City

von Frederik Stückemann

Das Thema Smart City gewinnt zunehmend an Bedeutung und wird immer mehr zum Aushängeschild für eine Stadt. Viele Städte setzen bereits Maßnahmen um, sammeln Daten, um Abläufe zu optimieren und idealerweise Kosten zu sparen. Das Problem dabei: Nicht jeder Abfalleimer oder Parkplatz lässt sich per Kabel anbinden. Daher bedarf es hier einer Alternative.

Smart City, was bedeutet das überhaupt?

Eine Smart City wird anhand unterschiedlicher Kriterien identifiziert. Dazu gehören die Digitalisierung von Verwaltungsaufgaben, wie etwa die An- und Abmeldung von Fahrzeugen über Online-Formulare, ebenso wie die Erfassung von Daten – etwa zum Füllstand öffentlicher Mülleimer, zur Belegung von öffentlichen Parkplätzen, zur groben Zählung von Personen bei Veranstaltungen oder zur Überwachung der Bodenfeuchte öffentlicher Grünflächen. All diese Szenarien tragen dazu bei, Prozesse effizienter zu gestalten.

Die kabellose Realisierung per LoRaWAN

Um Anwendungen wie die oben genannten zu ermöglichen, ist Sensorik notwendig, die Daten erfassen und übertragen kann. Das klassische Kabel scheidet dabei aus logistischen und finanziellen Gründen aus. Entsprechend müssen Funktechnologien eingesetzt werden, die für diese speziellen Einsatzzwecke geeignet sind. Häufig wird in diesem Zusammenhang „LoRaWAN“ (kurz für „Long Range Wide Area Network“) genannt – eine der am weitesten verbreiteten Funktechnologien im Bereich Smart City. Die wichtigsten Gründe hierfür sind die folgenden:

- LoRaWAN ist stark auf Reichweite und Akkulaufzeit optimiert.
- Die notwendigen Komponenten sind für unterschiedlichste Use Cases verfügbar.
- LoRaWAN ist seit 2015 auf dem Markt und entsprechend erprobt.
- LoRaWAN hat sich bereits in vielen Umgebungen bewährt.
- Es sind mehrere Dienstleister auf dem Markt, die diese Technologie anbieten.

Diese Eigenschaften haben dazu geführt, dass der Verbreitungsgrad von LoRaWAN gestiegen ist. Viele Städte und Unternehmen nutzen bereits diese Technologie, um unterschiedlichste Use Cases zu realisieren.

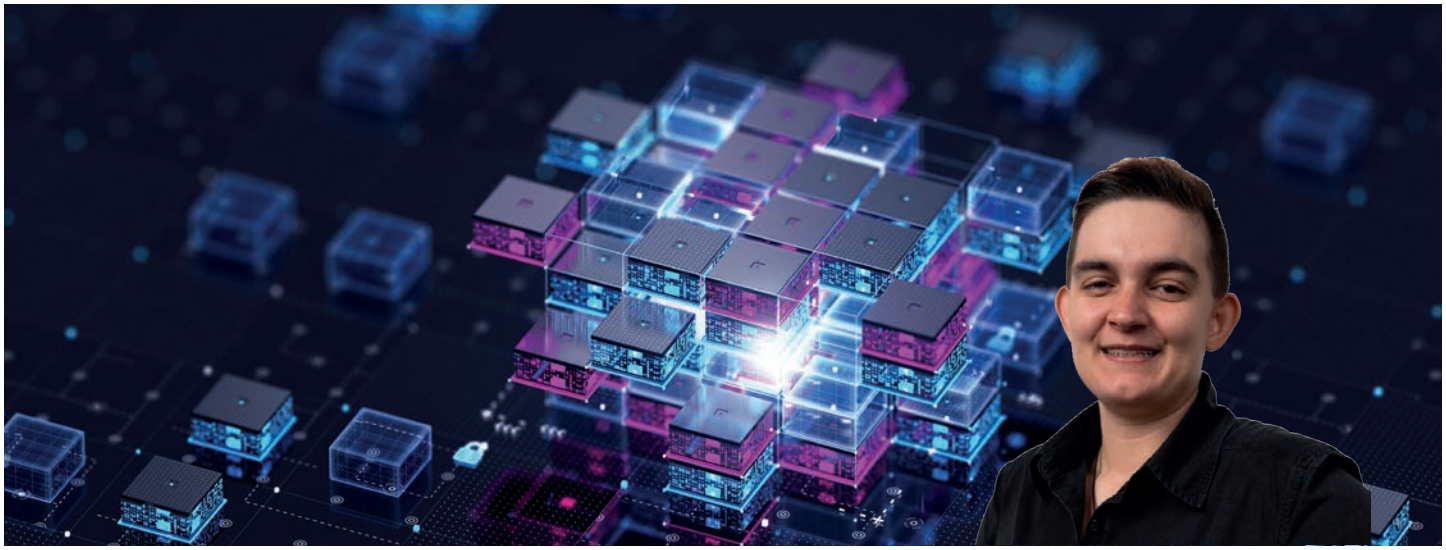
Natürlich haben LoRaWAN und Funktechniken nicht nur Vorteile, sondern auch folgende Nachteile:

- Batteriebetriebene Endgeräte müssen irgendwann gewartet werden.
- Störungen und Kollisionen auf der Luftschnittstelle sind möglich und verhindern die Übertragung der Daten.
- Es muss eine ausreichende Funkversorgung sichergestellt werden, damit alle Daten von den Endgeräten empfangen werden können.
- Eine Überführung der Nutzdaten der Sensoren in nachgelagerte Systeme ist häufig mit Aufwand verbunden.
- Beschädigungen und Diebstahl von Sensoren sind nicht immer vermeidbar.

Aus diesen Gründen ist eine sorgfältige Vorabplanung von Kosten, Nutzen und Realisierung notwendig, um sicherzustellen, dass ein solches Unterfangen am Ende ein Erfolg und kein Reinfall wird.

Das LoRaWAN-Ökosystem

Um eine LoRaWAN-Infrastruktur erfolgreich einzusetzen, sind einige Systeme notwendig, die entweder vollständig vom betreffenden Unternehmen oder durch einen Dienstleister betrieben werden müssen. Eine Abwägung der Kosten muss durchgeführt werden.



Ceph in Proxmox – verteiltes Storage im praktischen Einsatz

von Chantal Haidl

Die Wahl der richtigen Storage-Lösung ist für jede Virtualisierungsumgebung entscheidend. Gerade bei Clustern kann die Speicherperformance darüber entscheiden, ob ein System produktiv genutzt werden kann oder nicht. Bei der Migration unserer Testumgebung von VMware auf Proxmox (siehe Netzwerk-Insider 07/25) stand daher auch für uns die Frage im Raum, welche Storage-Technologie die Richtige ist.

Proxmox bietet mehrere Optionen: klassische NAS- oder SAN-Ansätze mit Replikation und Ceph. Für unsere Testumgebung suchten wir eine Storage-Lösung, die unserem bisher eingesetzten VMware vSAN möglichst nahekommt: ein verteiltes, hochverfügbares Objekt-Storage-System, welches flexibel und skalierbar ist und eine automatische Lastverteilung zur Verfügung stellt. Unsere Wahl fiel daher auf Ceph.

Doch was ist Ceph eigentlich? Wie richtet man dies in Proxmox ein und welche Stolperfallen lauern bei der Umstellung? Dieser Artikel zeigt, wie wir Ceph in unserer Proxmox-Umgebung umgesetzt haben, auf welche Probleme wir dabei gestoßen sind und wie wir diese erfolgreich lösen konnten.

Was ist Ceph?

Ceph ist ein Open-Source-Storage-System, welches Daten redundant auf vielen Servern verteilt speichert und somit ein hochverfügbares und fehlertolerantes System schafft. Die Basis bilden sogenannte OSDs (Object Storage Daemons). Jeder OSD verwaltet in der Regel eine einzelne Festplatte und übernimmt Aufgaben wie die Speicherung, Replikation und Wiederherstellung von Objekten. Zudem wird er einer bestimmten Geräteklasse (Standard-Klassen oder einer eigenen) zugeordnet, worüber eine gezielte Zuweisung zu den jeweiligen Datenpools erfolgt. Die OSDs arbeiten mit der BlueStore-Architektur und verwalten somit Objekte direkt auf Blockgeräten, ohne ein Dateisystem zwischenzuschalten. Pro OSD können drei verschiedene Geräte zum Einsatz kommen: Primary Data Device, WAL (Write-Ahead Log) und DB (Datenbankgerät). Auf dem Primary Data Device liegen die tatsächlichen Objekt-Daten. Darauf werden die Daten zuerst geschrieben und anschließend die Metadatenbank aktualisiert. Der WAL ist im Prinzip ein internes Journal von BlueStore und wird genutzt, um hohe Schreibperformance sicherzustellen. Auf dem DB-Device werden die Metadaten gespeichert.

Wie die Daten im Cluster verteilt werden, bestimmen die CRUSH-MAP und die PGs (Placement Groups). Die CRUSH-MAP wird für die direkte Kommunikation zwischen den Ceph-Clients und den OSDs genutzt und beschreibt die logische und physische Struktur des Clusters. Die Struktur selbst wird über erstellte Regeln aufgebaut, worüber unter anderem die Zuordnung von Geräteklasse zu Ceph-Pool realisiert wird. PGs fungieren als logische Container innerhalb eines Ceph-Pools. Sie bündeln viele Objekte und ermöglichen so eine effizientere Verwaltung, bessere Lastverteilung und vereinfachte Recovery-Prozesse.

Damit der Cluster zuverlässig arbeitet, werden zusätzlich Monitor Daemons (MONs) und Manager Daemons (MGRs) benötigt. Der MON überwacht den Cluster-Zustand und verwaltet die Cluster-Map, wohingegen der MGR weitere Monitoring- und Management-Funktionen bietet.

Darüber hinaus kennt Ceph noch andere Komponenten: Der MDS (Metadata Server) wird benötigt, wenn man das CephFS-Dateisystem verwendet. Er verwaltet und koordiniert Metadaten

Mikrosegmentierung: Herausforderung in komplexen Netzwerkstrukturen

Mit Simon Oberem sprach Christiane Zweipfennig

Die klassische Netzsegmentierung teilt Netzwerke grob in Zonen auf und setzt auf zentrale Kontrollen wie Firewalls, um den Datenverkehr zu regulieren, die Sichtbarkeit zu erhöhen und Risiken zu begrenzen. Insbesondere bei Organisationen, für die regulatorische Anforderungen wie die BSI-KRITIS-Verordnung greifen, reicht diese Maßnahme oft nicht aus und herkömmliche Segmentierungsmethoden stoßen in großen, komplexen Infrastrukturen an ihre Grenzen: Die getrennten Netzbereiche sind zu grob, die Angriffsfläche bleibt zu groß, und die Sicht auf die Kommunikationswege zu unvollständig. Mikrosegmentierung geht hingegen einen Schritt weiter: Sie zerlegt das Netzwerk in feine, granulare Segmente, die sich auch über sehr dynamische Umgebungen hinweg präzise steuern und überwachen lassen. Die Planung eines Mikrosegmentierungsprojektes ist komplex und erfordert eine sorgfältige und detaillierte Vorbereitung.

Simon Oberem ist seit 2013 bei ComConsult tätig und kann auf eine langjährige Erfahrung im Bereich der IT-Sicherheit zurückblicken. Seit Beginn seiner Laufbahn beschäftigt er sich intensiv mit Sicherheitsregularien und dem Management von Informationssicherheitsrisiken, insbesondere im Rahmen von Informationssicherheitsmanagementsystemen (ISMS). Er hat sich zunehmend auf Netzwerksicherheit spezialisiert und war unter anderem an großen Projekten wie dem LAN Design Guide eines großen Automobilkonzerns, der grundlegenden Einführung eines ISMS bei einer Versicherung sowie diversen Netzsegmentierungsprojekten beteiligt. Heute ist er bei ComConsult der Experte im Bereich Firewall-Technologien und unterstützt insbesondere bei der Umsetzung von Netzsegmentierungsprojekten, die seit jeher das Kerngeschäft von ComConsult prägen.

Verschiedene Standards und Gesetze stellen hohe Anforderungen an den sicheren Netzbetrieb und eine wirksame Netzsegmentierung. Welche sind das?

Durch die zunehmende Bedrohungslage sowie verschärfte Regularien hat sich die Bedeutung von Sicherheitsmaßnahmen wie Netzsegmentierung und Einsatz von Firewalls in verschiedensten Formen massiv erhöht, weshalb sich Netzsegmentierungsprojekte in den letzten Jahren stark verändert haben. Die wichtigsten Standards sind vor allem die ISO 27001 und der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Die ISO 27001 legt grundsätzlich fest, dass man sich um die Sicherheit des Netzbetriebs kümmern muss, gibt aber im Detail weniger präzise Vorgaben an die Netzsegmentierung. Der BSI-IT-Grundschutz ist hier deutlich konkreter und enthält spezifische Bausteine, an deren Entwicklung ComConsult mitwirken durfte. Wei-

> Sicherheitsstandards wie ISO 27001 und BSI-IT-Grundschutz fordern erhöhte Sicherheitsmaßnahmen.

Schiffe sind die besseren Smart Buildings!

von Dr. Joachim Wetzlar

Haben Sie schon einmal an einem Kreuzfahrtschiff hochgeschaut? Oder sind Sie sogar schon darauf mitgefahren und haben vom obersten Deck aus heruntergeblickt? Jedenfalls übertreffen die Dimensionen in der Regel die eines Hochhauses. Hier in Bremerhaven liegt derzeit ein solcher Riese an der Ausrüstungspier. Fast 350 Meter lang und 46 Meter breit ist es und soll bis zu 9000 Menschen Platz bieten. Viele Gemeinden in Deutschland sind kleiner.

Tatsächlich verfügt ein solches Schiff neben den offensichtlichen Einrichtungen zur Restauration und zum Hotelbetrieb über jegliche Infrastruktur, die wir von Gemeinden an Land kennen: Es gibt Strom sowie Kalt- und Warmwasser. Hierfür fahren ein Kraftwerk, ein Wasserwerk und eine Kläranlage mit. Die Müllabfuhr trennt und kompaktiert Abfälle so, dass sie umweltgerecht entsorgt werden können. Räume müssen be- und entlüftet sowie geheizt oder gekühlt werden. Es gibt Fernsehen und Internet. Und das alles wird von Menschen verwaltet und betrieben, die dafür entsprechende Infrastruktur benötigen.

Mancher Passagier mag in Anbetracht von Größe und Komfort zeitweise vergessen, dass er sich auf einem Verkehrsmittel befindet anstatt in einem Hotel. Dieses Verkehrsmittel verfügt über eine Antriebseinheit, die bei Bedarf auch als Lenkung oder Bremse eingesetzt wird. Gefahren wird es von der Abteilung „Nautik“. Sie findet den Weg mit einem hochkomplexen Navi, das hier als „Electronic Chart Display and Information System“ (ECDIS) bezeichnet wird.

Sie ahnen es bereits: All dies lässt sich derzeit nur noch mit einem hohen Automatisierungs- und Vernetzungsgrad betreiben. Womit wir beim Thema Sicherheit sind. Insbesondere die Verfügbarkeit ist in der Seefahrt traditionell ein hohes Gut. Ich habe selten so viele und so gut durchdachte Redundanzen gesehen wie auf Schiffen. Das betrifft auch die IT-Systeme. Bei denen sind überdies Vertraulichkeit und Integrität zu beachten.

Bereits 2020 hat sich die Internationale Maritime Organisation (IMO) der IT-Sicherheit angenommen. Der sogenannte ISM-Code (ISM steht für „International Safety Management“) soll einen in jeder Hinsicht sicheren Schiffsbetrieb regeln. ISM Cyber Security [1] ist seither Teil des ISM Code und fordert, dass Maßnahmen zur IT-Sicherheit in das bestehende Safety Management System (SMS) der Reedereien aufgenommen werden.

Hier in Deutschland soll man sich an den Standards des BSI für Informationssicherheit orientieren. Ein IT-Grundschutzprofil für Reedereien [2] hilft, entsprechende Maßnahmen aus dem IT-Grundschutzkompendium abzurufen. In den vergangenen Jahren wurde die Umsetzung solcher Maßnahmen sporadisch im Rahmen von Audits überprüft. Ich habe mir von Kapitänen berichten lassen, dass es für eine positive Bewertung meist schon ausreichte, wenn keine Kennwörter an Bildschirmen oder unter Tastaturen notiert waren.

Ungeachtet dessen werden inzwischen auch Schiffe und Reedereien Ziel von Cyber-Attacken. Die seit einigen Jahren zunehmenden geopolitischen Spannungen tun das ihre dazu. So wird in [3] berichtet, dass eine Hacker-Gruppe die Kommunikationsfähigkeit von mehr als 100 iranischen Öl-Tankern gleichzeitig unterbrechen konnte. Auch von Störungen der Satelliten-Navigation (Global Navigation Satellite System, GNSS) wird inzwischen regelmäßig berichtet.