Alles im Griff: mit Machine to Machine-Netzwerken

Everything under control: machine-to-machine networks

Der Wunsch, Maschinen und Anlagen aus der Ferne zu steuern und zu überwachen, wächst und wächst. Die Gründe dafür sind vielseitig: Erhöhung der Verfügbarkeit, Kostenreduzierung oder Ausbau neuer Service-Geschäftsmodelle.

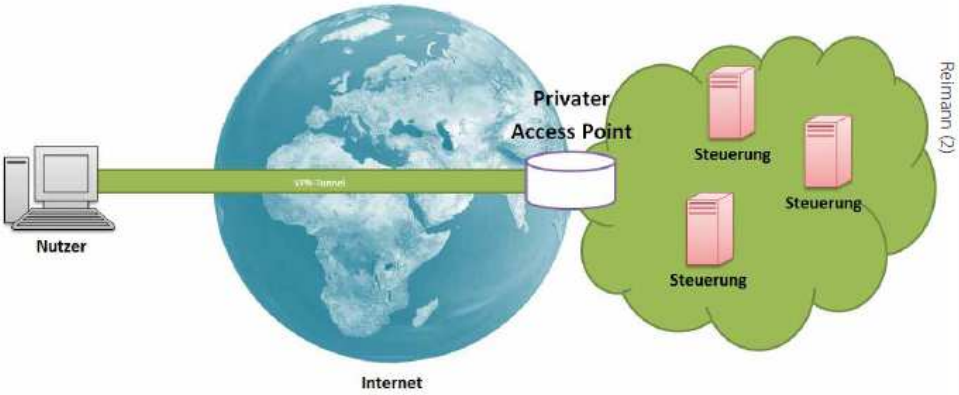
Ein Fernzugriff auf Maschinen und Anlagen wurde bisher im Regelfall über das Festnetz ermöglicht. Dabei können aber unlösbare Probleme auftreten, wenn sich etwa die zu steuernde oder zu überwachende Komponente auf einem mobilen Gerät befindet, kein Festnetzanschluss vor Ort vorhanden ist oder der spätere Endkunde dem Anlagenlieferanten die Nutzung seines lokalen Netzwerks untersagt. In allen drei Fällen kann eine Mobilfunkkommunikation die beste Lösung sein.

Auch mit der neuen Betriebssicherheitsverordnung wächst das Interesse an solchen Machine to Machine (M2M)-Lösungen. Damit Anlagen jederzeit von überall auf der Welt überwacht werden können, benötigen sie dann lediglich eine Internetverbindung, die über einen Webserver errichtet werden kann. Der Webserver kann sowohl in der Aufzugsanlage integriert als auch extern über entsprechende Hard- und Software realisiert werden. Darüber hinaus wird zur Kommunikation mit dem World Wide Web noch ein Mobilfunkrouter benötigt.

Zugang zum Mobilfunknetzwerk

Für die Umsetzung eines solchen M2M-Netzwerks über das Mobilfunknetz gibt es mehrere Strukturen. Am häufigsten möchte man in der Industrie von einer Zentrale aus auf die Anlagen zugreifen. SIM-Karten, die in den Außenstationen eingesetzt werden, besitzen aber im Normalfall keine festen IP-Adressen, worüber die Anlagen erreicht werden können. Es gibt zwar auch Möglichkeiten, die aktuell vergebene IP-Adresse herauszufinden, jedoch ändert sich die IP-Adresse in bestimmten Intervallen. Außerdem wird der Zugriff aus dem Internet auf den mobilen Teilnehmer im Normalfall von Mobilfunkanbietern verhindert wegen mangelnder Sicherheit und hohen Kosten für die übertragenen Daten.

Das erschwert die Nutzung des Mobilfunknetzes für M2M-Anwendungen.



Reimann (2)

Hierfür gibt es im Wesentlichen zwei Lösungsansätze: entweder man erfragt beim Mobilfunkanbieter eine SIM-Karte mit einer festen IP-Adresse oder man nutzt ein VPN-Netzwerk.

SIM-Karten und deren IP-Adressen

Es gibt SIM-Karten mit einer sogenannten festen öffentlichen IP-Adresse. Die sind aber kostenintensiv und dazu kann jeder Internetnutzer Zugriff auf die IP-Adresse und somit auf die Anlage erhalten. Das stellt ein großes Sicherheitsrisiko dar. Eine wesentlich kostengünstigere Lösung ist die Verwendung einer sogenannten privaten IP-Adresse. In dieser Variante wird in einem privaten Netz gearbeitet, das nur bestimmte Nutzer zulässt: Das Internet wird umgangen. Zudem ist dieses Netzwerk auch gut vor unbefugten Zugriffen geschützt.

Gesichertes Virtual Private Network

Auch mit Hilfe eines VPN-Netzwerks lässt sich ein M2M-Netzwerk aufbauen. Dafür werden einfache Daten-SIM-Karten verwendet, was die laufenden Kosten niedrig hält, und ein eigenes VPN-Netzwerk aufgebaut. Man richtet einen VPN-Server ein,

The desire for remote control and monitoring of machinery and systems is growing continually. There are many different reasons for this, such as increasing availability, cutting costs or expanding new service business models.

Previously, remote access to machinery and systems was normally facilitated via the fixed line network. However, insoluble problems can occur in this connection, for example, if components to be controlled or monitored are on a mobile device, there is no landline connection on the spot or the later end-customer forbids usage of its local network to the system supplier. Mobile communications may be the best solution in all three cases.

Interest in such machine-to-machine (M2M) solutions is also growing due to the new Operational Safety Ordinance. To enable systems to be monitored from anywhere in the world, all they then need is an Internet connection, which can be set up via a web server. The web server can be integrated both in the lift as well as realised externally via corresponding hard- and software. In addition, a mobile communications router is also needed for communication with the World Wide Web.

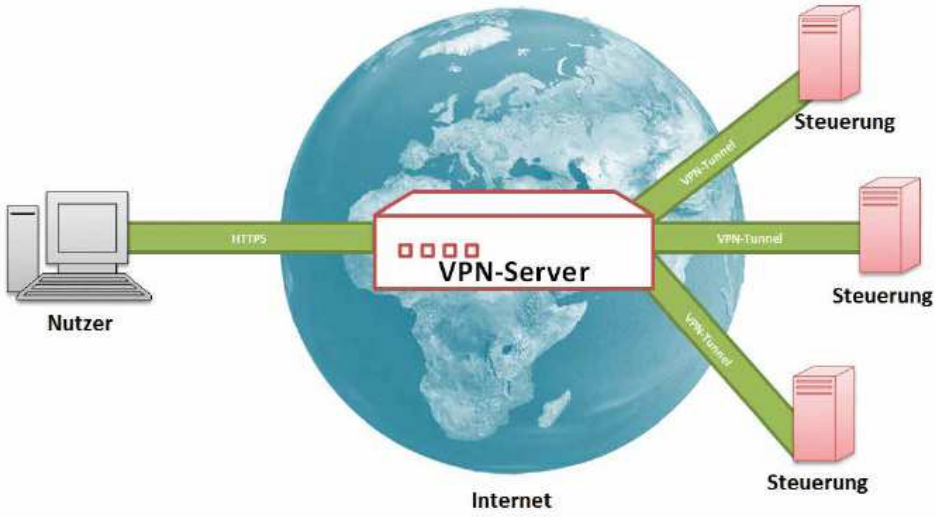
Access to mobile communications network

There are several structures for implementing such an M2M network via a mobile communications network. In industry, what is most in demand is accessing the lifts from a control centre. However, SIM cards used in the outer stations normally have no fixed IP addresses via which the lifts could be reached. Admittedly there are ways to find out the currently assigned IP address, but the IP address changes at particular intervals. Moreover, access to the mobile participants from the Internet is normally prevented by mobile communications providers on account of the lack of security and high costs for the data transmitted.

This complicates the use of the mobile communication network for M2M applications. There are basically two solutions for this: either you request a SIM card with a fixed IP address from the mobile communications provider or you use a VPN network.

SIM cards and their IP addresses

There are SIM cards with a so-called fixed public IP address. However, these are cost intensive and in addition, every Internet user can access the IP address and as a result the lift. This represents a major security risk. Using a so-called private IP address is a much more affordable solution. In this version you operate in a private network that only permits particular users, thus



auf den dann die Clients, also die Anlagen, zugreifen. Somit wird die Blockade der Mobilfunkanbieter umgangen, da die Anlagen einen gesicherten VPN-Tunnel zum VPN-Server aufbauen. Durch die Tunnel ist eine Kommunikation im gesamten VPN-Netzwerk möglich.

Mit Hilfe der regelmäßig übertragenen Daten kann auch die Überwachung der Anlagen dokumentiert und Nachfragen zu Störungsbeseitigungen oder Garantieansprüchen schneller geklärt werden. Die Information über den Zustand der Anlagen erfolgt nicht nur im Fehlerfall, sondern es ist möglich, ständig auf alle Daten der Anlagen zuzugreifen.

Thomas Reimann,
CEO Ingenieurbüro Reimann

www.reimann-online.biz

avoiding the Internet. In addition, this network is also well-protected against unauthorised access.

Secured virtual private network

An M2M network can also be developed with the help of a VPN network. Simple data SIM cards are used for this purpose, which keeps the regular costs down, and an independent VPN network is developed. You set up a VPN server, which the clients, i.e. the lifts, then access. The blockade of the mobile communications providers is evaded in this way, since the lifts develop a secured VPN tunnel to the VPN server. Communication is possible throughout the entire VPN network through the tunnel.

Monitoring of the lift can also be documented and queries regarding the elimination of defects or guarantee claims can be clarified quicker with the assistance of the data regularly transferred. Information on the condition of the lifts is not just provided in the event of malfunctions - rather, it is possible to access all data of the lifts constantly.

Thomas Reimann,
CEO Reimann Engineering

www.reimann-online.biz