

Sensorkommunikation bei automatisierten Monitoringsystemen

Unterschiedliche Methoden zur Steuerung von Messsensoren im Bereich Überwachungsmessungen

Sensor Communication in Automated Monitoring Systems

Different Ways to Control Sensors in Monitoring Applications

Christian Breuer

Komplexe Messsysteme zur Überwachung von Objekten erfordern den Einsatz verschiedenster Sensoren. Zuverlässige Kommunikationswege zwischen Messsensor und Auswertesoftware sind dabei unerlässlich. Dieser Beitrag bietet eine Übersicht über die verfügbare Technik und erläutert die Vor- und Nachteile der einzelnen Verfahren.

Schlüsselwörter: Überwachung, Monitoring, Deformation

Complex survey systems used for monitoring applications require the integration of various sensors. A reliable communication between sensor and analysis software is an essential part of such a system. This article gives an overview of the available technologies and explains the advantages and disadvantages of the specific solutions.

Keywords: structural monitoring, deformation

1 HINTERGRUND

Die Themen Überwachungsmessung und Deformationsanalyse haben in den vergangenen Jahren stark an Bedeutung gewonnen. Einerseits werden immer mehr Verkehrsinfrastrukturbaumaßnahmen im innerstädtischen Bereich vorgenommen, die Überwachungsmessungen erfordern, andererseits führt das gesteigerte öffentliche Interesse an der Sicherheit dieser Maßnahmen dazu, dass Monitoring auch in anderen Bereichen thematisiert wird. Mehr Objekte werden auf ihre Standsicherheit hin überwacht, vor allem Bauwerke und instabiles Gelände. Aufgrund gestiegener Rohstoffpreise boomt auch der Bergbau, ein Wirtschaftszweig, der sich traditionell mit Deformationsanalyse beschäftigen muss.

Vermessungsprojekte, die den Einsatz von automatisierten Monitoringsystemen erfordern, wurden in der Vergangenheit häufig von spezialisierten Ingenieurbüros durchgeführt. Die Komplexität eines Monitoringprojektes erforderte Spezialwissen, vor allen Dingen im Bereich Sensorkommunikation und Auswertesoftware. Das machte

es für kleinere Vermessungsbüros schwierig, neben dem Tagesgeschäft Aufträge in diesem Bereich zu übernehmen. Dank der heute verfügbaren Kommunikationstechnik und Softwarepakete hat sich diese Situation deutlich geändert. Aus anderen Bereichen bekannte Technik und anwenderfreundliche Software erleichtern den Zugang zu diesen Anwendungen. Auch ist das Investitionsrisiko gesunken. Mussten früher spezielle Monitoring-Tachymeter angeschafft werden, die nach Projektende nutzlos wurden, so gibt es heute universelle Instrumente, die nicht nur die hohen Anforderungen von Überwachungsmessungen erfüllen, sondern auch für alle anderen Vermessungsaufgaben eingesetzt werden können. Diese Faktoren führen dazu, dass das Thema Monitoring für immer mehr Firmen interessant wird.

Großprojekte werden sicherlich auch in Zukunft von spezialisierten Ingenieurbüros betreut werden, aber die Entwicklung zeigt, dass kleinere Vermessungsbüros und Bauunternehmen immer mehr Aufgaben in diesem Bereich wahrnehmen und erfolgreich lösen.

2 ANSÄTZE

Die Hauptbestandteile eines Monitoringsystems sind eine PC-basierte Auswertesoftware und der Messsensor selbst. Die Software steuert die Sensoren, empfängt die Messdaten, wertet diese aus und speichert Ergebnisse in eine Datenbank. Bei einem geodätischen Monitoring kommen natürlich am häufigsten Vermessungssensoren zum Einsatz, Tachymeter und GNSS-Empfänger. Verbreitet werden auch Temperatur- und Neigungssensoren verwendet, sowie Wetterstationen und andere geotechnische Sensoren. In diesem Beitrag soll im Wesentlichen auf die Kommunikation zwischen einem Sensor und einem PC eingegangen werden.

Generell kann man sagen, dass eine größere räumliche Entfernung zwischen Sensor und PC die Kommunikation störungsanfälliger macht als eine kleine. Daher wird man versuchen, den PC möglichst nah am Sensor zu platzieren. Je nach Örtlichkeit ist das aber nicht immer möglich oder aus Gründen der Sicherheit nicht gewollt. Außerdem ist es unter Umständen sinnvoll, die Datenhaltung an anderer Stelle vorzunehmen, die Datenbank vielleicht auf einem Rechner im Büro zu haben. Die moderne Architektur heutiger Monitoringsoftware erlaubt es dem Anwender, sein System so zu konfigurieren, wie es das Projekt erfordert. Es besteht z.B. die Möglichkeit, die Installation der Software auf mehrere Rechner zu verteilen. Man kann also einen PC sehr nah am Sensor platzieren und dort die Software-Module installieren, die den Sensor steuern und die Daten sammeln. Auf einem PC im Büro werden die Module installiert, die die Daten dann auswerten und in die Datenbank speichern. Falls die Kommunikation zwischen den beiden Rechnern ausfällt, ist immer noch gewährleistet, dass der Sensor arbeitet und die Daten gesammelt und zwischengespeichert werden. Sobald die Kommunikation wiederhergestellt ist, können die Daten zur Auswertung weitergeleitet und in die Datenbank geschrieben werden. Anders als bei einer Unterbrechung der Kommunikation zwischen Sensor und PC gehen hier keine Daten verloren.

3 SERIELLE ODER USB-KABELVERBINDUNGEN

Eine schnelle und sichere Verbindung erreicht man durch die Verwendung von seriellen und USB-Kabeln. Fast alle Sensoren bieten auch heutzutage noch serielle Schnittstellen. Das ermöglicht eine einfache, direkte Ansteuerung, ohne dass eine zusätzliche Hardware eingesetzt werden muss. Keine aufwendige Konfiguration ist erforderlich. Sensoren mit serieller Schnittstelle sind in der Regel auch erheblich preisgünstiger als Modelle mit anderen Schnittstellen.

Großer Nachteil von seriellen oder USB-Kabelverbindungen sind die geringen Reichweiten. Serielle Kabel sollten eine Länge von zehn Metern nicht überschreiten. USB-Kabel können nur bis zu einer Länge von etwa fünf Metern verwendet werden. Das schränkt den Einsatzbereich natürlich deutlich ein. Abhilfe schaffen können da in manchen Fällen sogenannte *Range Extender* (Abb. 1). Dabei handelt es sich um Konverter, die das serielle oder das USB-Signal auf Netzkabel oder Lichtwellenleiter umsetzen. Zuverlässig arbeiten diese Konverter bis etwa 300 m bei seriellen, bis 100 m bei USB-Verbindungen. Je nach angeschlossenem Sensor können auch längere Netzkabel oder Lichtwellenleiter verwendet werden, wenn die Sensoren geringere Bandbreiten benötigen.

4 FUNKMODULE/DATENFUNK

In sehr ländlichen Gebieten ohne sonstige Kommunikationsinfrastruktur können Datenfunkgeräte, die im UHF-Bereich arbeiten, eine Alternative sein. Geräte mit maximal 0,5 W Sendeleistung dürfen in den meisten Ländern kostenfrei betrieben werden. Je nach Topografie können damit Distanzen zwischen zwei und zehn Kilometern überbrückt werden. Die maximale Datenrate beträgt dabei allerdings nur 9.600 bis 19.200 Baud, was für eine bidirektionale Kommunikation mit komplexen Sensoren



Abb. 1 | RS232 Extender der Firma Digitus

nicht ausreichend ist. Da man für fünf Sensoren zehn Funkmodule benötigen würde, ist diese Methode der Datenübertragung auch vom wirtschaftlichen Standpunkt aus gesehen wenig attraktiv.

Interessanter ist es schon, wenn Sensoren über interne Funkmodule verfügen, sodass man auf externe Kommunikations-Hardware verzichten kann (Abb. 2). Das ist besonders dann von Vorteil, wenn der Sensor an einer schlecht zugänglichen Stelle montiert werden soll oder insgesamt sehr wenig Platz vorhanden ist. Diese Möglichkeit bietet sich vor allem bei Tachymetern an. Jeder große Hersteller bietet seine Modelle auch mit interner Telemetrie an, damit die Instrumente bei normalen Vermessungsaufgaben im Robotik-Betrieb bedient werden können. Die hierbei zum Einsatz kommenden Funkmodule nutzen in der Regel den lizenzfreien 2,4 GHz-Bereich, der bei 100 mW Sendeleistung Reichweiten bis etwa 1000 m ermöglicht. Die Telemetrie kann natürlich auch für Monitoringanwendungen genutzt werden. Statt des normalerweise im Feldrechner integrierten Funkmoduls muss hier ein PC-taugliches, externes Modell verwendet werden, welches an die serielle oder USB-Schnittstelle des Rechners angeschlossen wird. Je nach Hersteller können auch mehrere Tachymeter gleichzeitig mit einem Funkmodul gesteuert werden. Die Identifikation des Instrumentes erfolgt anhand seiner Seriennummer, sodass alle Instrumente über den gleichen Kanal kommunizieren. Da eine Vielzahl von Kanälen zur Verfügung steht, lässt sich problemlos eine störungsfreie Kommunikation einrichten, die außer der Stromversorgung keine weitere Hardware am Sensor erfordert. Diese Technologie findet daher häufig Anwendung bei Projekten im innerstädtischen Bereich, wo die Instrumente auch im öffentlichen Raum montiert werden müssen.



Abb. 2 | Trimble S8 Instrumente und Funkmodul

5 NETZWERK-/INTERNETVERBINDUNG (TCP/IP)

Die verschiedensten Anwendungen nutzen heutzutage lokale Netzwerke und das Internet als Kommunikationsmedium. Selbst wenn die Signale einmal um den gesamten Globus laufen, hat man selten mehr als ein paar Sekunden Verzögerungszeit. Netzwerktechnologie bietet sich daher auch zur Kommunikation mit Messsensoren an. Sie ermöglicht einen schnellen Datenaustausch mit hoher Bandbreite und quasi unbegrenzter Reichweite. Von Vorteil ist auch, dass man eine vorhandene Kommunikationsinfrastruktur wie z.B. Firmen- und Baustellennetzwerke oder das Internet nutzen kann. Innerhalb eines Firmennetzwerkes sind die Messdaten in der Regel auch optimal vor Fremdzugriff geschützt, denn die Sicherheitsrichtlinien der meisten Firmen sind sehr restriktiv. Diese Sicherheitsrichtlinien sorgen auf der anderen Seite aber auch häufig für Probleme bei der Einrichtung eines Monitoringsystems. Eine rigorose Abschottung nach außen erschwert die Integration neuer Komponenten wie Sensoren. Es ist daher unerlässlich, die verantwortlichen IT-Mitarbeiter bereits im Vorfeld der Planung zu involvieren.

Des Weiteren muss man beachten, dass die meisten Sensoren nicht direkt im Netzwerk/Internet betrieben werden können, da sie nur über einen seriellen oder USB-Anschluss verfügen. Moderne GNSS-Empfänger beispielsweise besitzen Ethernet-Anschlüsse und integrierte Web-Konsolen, sodass sie ohne zusätzliche Hardwarekomponenten über ein Netzwerkkabel angeschlossen und auch sehr einfach konfiguriert werden können. Für Tachymeter und viele andere Sensoren gilt das nicht. Um Sensoren mit serieller Schnittstelle im Netzwerk nutzen zu können, müssen sogenannte *Serial Device Servers* eingesetzt werden (Abb. 3). Diese Geräte wandeln das serielle Signal des Sensors in das Ethernet-Protokoll um. Dabei wird dem seriellen Anschluss des Gerätes ein IP-Port zugewiesen, sodass man den dort angeschlossenen Sensor über eine IP-Adresse ansprechen kann. Je nach Art des angeschlossenen Sensors muss zusätzlich eine virtuelle serielle Verbindung über diese IP-Adresse eingerichtet werden. Entsprechende Software-Tools werden dazu mitgeliefert. Die Einrichtung ist sehr einfach und schnell.

Egal ob man einen PC am Sensor platziert oder den Sensor direkt über eine TCP/IP-Verbindung anspricht, es muss eine Netzwerk-/Internetverbindung am Sensor verfügbar sein. Im innerstädtischen Bereich oder bei Installationen auf privaten Betriebsgeländen ist es



Abb. 3 | Netzwerkverbindung unter Verwendung eines Serial Device Servers der Firma MOXA

unter Umständen möglich, einen vorhandenen Netzwerkanschluss zu nutzen, aber in den meisten Fällen muss man sich überlegen, wie man diese Verbindung einrichtet. Verschiedene Technologien können hier zum Einsatz kommen.

5.1 Kabelverbindungen

Zur Überbrückung kurzer Distanzen wird man sicherlich immer zuerst an Kabelverbindungen denken. Dazu bieten sich wieder Netzkabel und Lichtwellenleiter an. Netzkabel können derzeit bis zu einer Länge von etwa 100 m eingesetzt werden, Lichtwellenleiter bis 1000 m. Eine Kabelverbindung hat den Vorteil, dass sie, anders als eine Funkverbindung, lediglich mechanisch unterbrochen werden kann. Das setzt voraus, dass die Kabel in adäquater Weise verlegt werden können. Die Verlegung eines Kabels in offenem Gelände kann sehr aufwendig sein. Die Kabel müssen gegen Witterung, Tiere, andere Fremdeinflüsse und Fremdzugriffe geschützt werden. Außerdem können Kabel bei Bauarbeiten eventuell beschädigt werden.

Neben dem Aufwand und den Kosten für die Verlegung können auch die Kosten für die Kabel selbst erheblich sein. Je nach Anzahl der zu steuernden Sensoren, der Länge des Kabels, der Art des Kabels und der Anzahl der Schaltkästen etc. entstehen schnell große Summen, die den Einsatz von Kabeln unrentabel machen.

5.2 Kabellose Verbindungen

Die Einrichtung einer kabellosen Verbindung ist in der Regel deutlich einfacher. Die meisten IT-Anwender sind mit dem Anschluss eines *Wireless Routers* und seiner Konfiguration vertraut, denn diese Geräte sorgen nicht nur in den meisten Firmen für kabellosen Netzwerkzugang, sondern gehören auch schon in vielen Haushalten zur Standardausstattung. Mit wenigen Handgriffen kann man sich somit ein lokales, kabelloses Netzwerk (WLAN) einrichten, das bei Verwendung entsprechender Verschlüsselung gut vor Fremdzugriff geschützt ist.

Großer Nachteil dieser Technologie ist wiederum die Reichweite. Der WiFi-Breitbandfunk arbeitet im lizenzfreien 2,4 GHz-Bereich und erlaubt den Einsatz von Transmittern mit maximal 100 mW Sendeleistung. Je nach Örtlichkeit und Art der Antenne lassen sich damit bei Sichtverbindung Reichweiten bis etwa 100 m in alle Richtungen erzielen. Um größere Strecken zu überbrücken, können in bestimmten Abständen sogenannte *Repeater* installiert werden, die das Signal weiterleiten. Verteilt man diese *Repeater* gleichmäßig, kann eine ganze Fläche mit WLAN abdeckt werden. Unter Umständen erhält man im Handel auch WiFi-Transmitter mit größerer Sendeleistung (Abb. 4). Der Betrieb dieser Geräte ist allerdings in den meisten Ländern illegal. Auch wird die Reichweite nur begrenzt erhöht. Beispielsweise würde es ein Gerät mit 500 mW Sendeleistung auf nur etwa 200 m Reichweite bringen.

Will man große Distanzen überbrücken, ist der Einsatz von Richtfunkantennen erheblich effektiver. Mit dieser kostengünstigen Technologie lassen sich auch bei nur 100 mW Sendeleistung Reichweiten bis zu fünf Kilometern erzielen.

5.3 Leckwellenleitung

Eine besondere Form der Funkübertragung bieten sogenannte Leckwellenleitungen (engl. *Leaky Feeder*, Abb. 5). Leckwellenleitungen bestehen im Wesentlichen aus einem geschirmten Koaxialkabel, wobei die Schirmung in regelmäßigen Abständen unterbrochen ist. An den Punkten, wo die Schirmung unterbrochen ist, können Funksignale gesendet und empfangen werden. Je nach Frequenz und



Abb. 4 | Installation eines WiFi-Transmitters mit Richtfunkantenne in einem Kupfertagebau in Thailand

Modulation der Signale sind die Unterbrechungen in der Schirmung unterschiedlich ausgearbeitet. Diese Technik findet sehr häufig Verwendung in Tunneln. Man kann zum Beispiel feststellen, dass in manchen Straßentunneln Radioempfang möglich ist und in anderen nicht, oder dass in einigen U-Bahntunneln ein Mobilfunknetz verfügbar ist und in anderen nicht. Ermöglicht wird das durch den Einsatz von Leckwellenleitungen. Typischerweise sind etwa alle 350 m bis 500 m Signalverstärker in das Koaxialkabel integriert.

Genauso finden Leckwellenleitungen auch Anwendung in der Netzwerktechnologie. Besonders bei langgestreckten Objekten wie Tunneln und in Bergwerken ist der Einsatz dieser Technologie ideal. Eine entsprechende Leckwellenleitung wird einfach entlang des Objektes verlegt und bietet dann auf gesamter Länge Netzwerkzugang. Die Verfügbarkeit beschränkt sich allerdings auf einen kleinen Bereich mit wenigen Metern Abstand zum Kabel. Das ist aber für die meisten Anwendungen mehr als ausreichend.

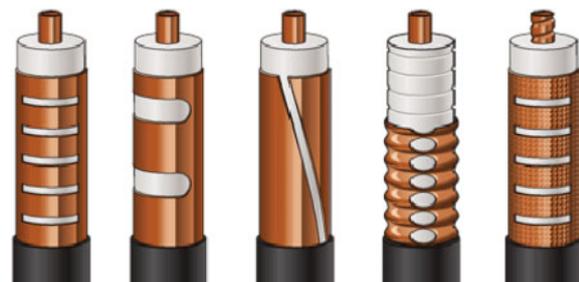


Abb. 5 | Leaky Feeder – verschiedene Ausführungen von Leckwellenleitungen

5.4 Mobiles Internet

Spätestens seit der Einführung von UMTS (HSDPA, 3G) sind auch Internetverbindungen über das Mobilfunknetz in ausreichender Geschwindigkeit und Bandbreite möglich. Auch wenn es in Europa noch keine flächendeckende Verfügbarkeit gibt, UMTS ist in fast allen Ballungsgebieten vorhanden. In den meisten Fällen legt man eine entsprechende SIM-Karte in ein Internet-fähiges Mobiltelefon oder Smartphone ein und schon kann man unterwegs im Internet surfen. Andere nutzen USB-UMTS-Adapter in ihren Notebooks zu dem gleichen Zweck. Wiederum andere verzichten mittlerweile auch zu Hause komplett auf Kabel und nutzen das mobile Internet für ihr gesamtes Heimnetzwerk. Das erfolgt dann mittels sogenannter UMTS-Router. In den Router setzt man seine SIM-Karte ein und nach dem Einschalten wählt sich dieser automatisch in das mobile Internet des Anbieters ein. An den Router lassen sich dann Rechner und andere Netzwerkgeräte anschließen.

Diese Technologie lässt sich auch sehr gut für die Sensorkommunikation einsetzen. PC, Ethernet-fähiger Sensor oder *Serial Device Server* können einfach mit dem UMTS-Router verbunden werden und sind dann über die IP-Adresse des Routers ansprechbar. Darüber hinaus gibt es Geräte, die UMTS-Router und *Serial Device Server* in sich vereinen (UMTS/3G Device Server). Diese Geräte eignen sich hervorragend, um z.B. ein einzelnes Tachymeter über das mobile Internet anzusteuern.

Ein kritischer Faktor bei Nutzung des Internets als Kommunikationsmedium, besonders beim mobilen Internet (Abb. 6), ist die IP-Adresse. Bei „normalem“ Gebrauch des Internets ist es unwichtig, welche IP-Adresse der Rechner oder das Smartphone bei der Anmeldung erhält, denn als Nutzer möchte man in der Regel Inhalte von Web-Seiten abrufen. Die IP-Adressen dieser Web-Seiten sind uns meistens unbekannt, da sie über den Domain-Namen abgerufen werden, die www-Adresse. Das gilt für einen privaten Rechner oder einen Sensor nicht. Um den Sensor ansprechen zu können, muss die IP-Adresse bekannt sein. Bei jeder Einwahl in das Internet oder spätestens nach 24 Stunden bekommt man allerdings eine neue IP-Adresse zugewiesen (dynamische IP-Adresse).

Der einfachste Weg dieses Problem zu lösen, ist mit festen, öffentlichen IP-Adressen zu arbeiten. Eine feste, öffentliche IP-Adresse kann man z.B. bei seinem Mobilfunkanbieter erwerben. Das be-

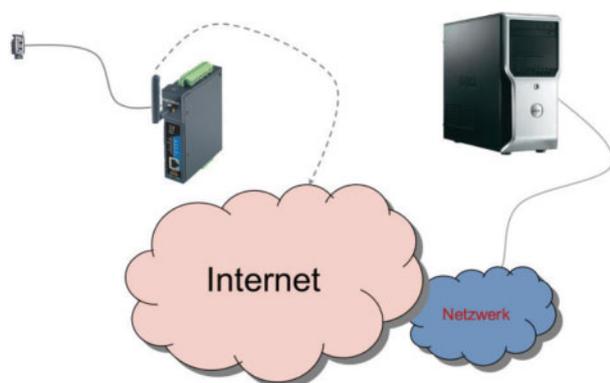


Abb. 6 | Netzwerkverbindung über mobiles Internet unter Verwendung eines MOXA UMTS Device Servers

deutet, dass dieser der verwendeten SIM-Karte bei jeder Einwahl immer die gleiche IP-Adresse zuweist und sie für andere Nutzer blockiert. Aufgrund der steigenden Anzahl von Internetnutzern werden die verfügbaren festen, öffentlichen IP-Adressen allerdings immer weniger. Daher sind die Preise momentan entsprechend hoch. Mit der flächendeckenden Einführung eines neuen IP-Adressentyps (IPv6) sollten in Zukunft ausreichend IP-Adressen für alle Anwendungen zur Verfügung stehen. Auch die Preise sollten dann wieder sinken.

Erheblich kostengünstiger als eine feste, öffentliche IP-Adresse ist da schon der Service einiger Dienstleister, die sich auf Internetkommunikation spezialisiert haben. Dieser Service erlaubt es, sich direkt in das private Netzwerk des Dienstleisters einzuwählen und dort eine feste IP-Adresse zu erhalten. Da es sich aber hierbei nicht um eine öffentlich sichtbare IP-Adresse handelt, muss sich auch der Rechner mit der Monitoring Software in dieses private Netzwerk einwählen, um die IP-Adresse auflösen zu können. Dazu werden von den Dienstleistern kostenlose Software-Tools zu Verfügung gestellt (VPN-Client, VPN = *Virtual Private Network*).

Eine dritte, kostenlose Möglichkeit ist die Nutzung sogenannter DynDNS-Dienste (dynamischer Domain-Name-System-Eintrag). Diese Dienste überwachen die dynamische IP-Adresse. Bei der Einrichtung des Dienstes gibt man einmalig die aktuelle dynamische IP-Adresse an und wählt einen alternativen Namen innerhalb der Domain des Dienstleisters. Danach sorgt der Dienst dafür, dass das Netzwerkgerät nicht nur über die IP-Adresse, sondern auch über den alternativen Namen erreichbar ist. Ändert sich die dynamische IP-Adresse, aktualisiert der Dienst in Verbindung mit dem DynDNS-Client (SW-Tool oder Konfigurationsoption im Router) die Verknüpfung mit dem alternativen Namen. Das Netzwerkgerät bleibt also immer über den gleichen Namen erreichbar.

Hat man ein Firmennetzwerk zur Verfügung, kann man auch Router einsetzen, die über einen integrierten VPN-Client verfügen. Diese sind zwar etwas teurer, bieten aber den Vorteil, dass sie sich automatisch in das eigene Firmennetzwerk einwählen können, in dem man natürlich selbst eine feste IP-Adresse vergeben kann. Der VPN-Zugriff muss auf dem Router mittels Zertifikat eingerichtet werden. Die dynamische, öffentliche IP-Adresse ist in diesen Fall uninteressant, da sie für die Sensorkommunikation gar nicht genutzt wird. Einige Sicherheitsrichtlinien von Firmennetzwerken erlauben einen solchen Zugriff allerdings nicht. Besonders hier gilt es, die IT-Mitarbeiter rechtzeitig über das Projekt zu informieren, um Lösungsmöglichkeiten diskutieren zu können.

Generell kann man feststellen, dass alle Lösungen funktionieren. Man sollte sich allerdings bewusst sein, dass man mit der Nutzung von zusätzlichen Diensten auch immer weitere mögliche Fehlerquellen zu seinem System hinzufügt. Jedes Software-Tool, jedes Netzwerk kann abstürzen. Bei Monitoringanwendungen, die hochgenaue Messdaten und korrekte Alarmierungen erfordern, wird man wohl kaum freie Internetdienste nutzen, über deren Verfügbarkeit man keine Aussage treffen kann.

6 KOMBINATIONSMÖGLICHKEITEN

Bei der Einrichtung eines Monitoringsystems wird man möglicherweise auf unterschiedliche Kommunikationsmethoden zurückgreifen müssen, für den einen Sensor jene und für den anderen Sensor eine

andere Kommunikation nutzen (Abb. 7). Die heute verfügbare Monitoringsoftware kann so flexibel konfiguriert werden, dass jeder Sensor individuell angesteuert wird. Auch können verschiedene Kommunikationsmethoden kombiniert werden. Beispielsweise kann ein Radiomodul über eine Netzwerkverbindung angesteuert werden, welches dann wiederum mit mehreren Tachymetern über Funk kommuniziert.

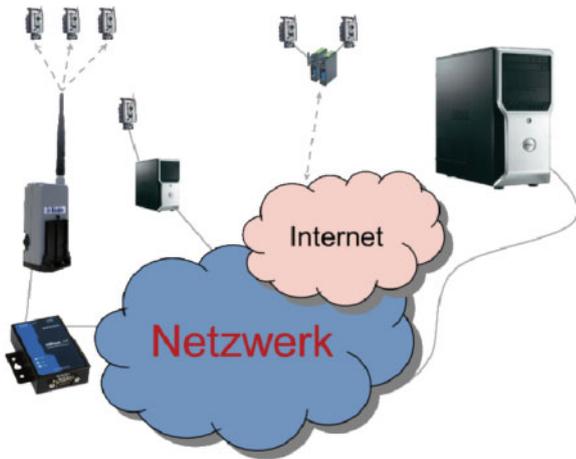


Abb. 7 | Verschiedene Kommunikationsmethoden innerhalb eines Projektes

7 ZUSAMMENFASSUNG

Für ein Monitoringsystem ist die Sensorkommunikation von elementarer Bedeutung. Machbarkeit, Zuverlässigkeit und Wirtschaftlichkeit entscheiden über die Wahl der Methode. Klassische Kabel- und Funkverbindungen werden nicht verschwinden, aber sicherlich an Bedeutung verlieren. Internet und lokale Netzwerke werden in Zukunft eine immer gravierendere Rolle bei der Sensorkommunikation spielen. Gute IT-Kenntnisse sind daher ebenso wichtig wie Kenntnisse über die am Markt befindlichen Technologien. Dieser Artikel kann nur einen kleinen Einblick in diese Technologien bieten, denn die Entwicklung in diesem Bereich schreitet schnell voran. Genauso wie heute Smartphones verschiedene Kommunikationsmethoden und eine Vielzahl von Anwendungen ermöglichen, wird der Trend sicherlich zum integrierten Sensor gehen. Die Sensoren der Zukunft werden mit immer mehr Funktionen und Kommunikationsoptionen ausgestattet werden, die den Einsatz auch in automatisierten Monitoringsystemen deutlich erleichtern werden. Bereits heute sieht man, dass sich immer mehr Vermessungsbüros und Bauunternehmen mit Monitoringprojekten beschäftigen. Diese Entwicklung wird mit neuen, leistungsfähigeren Sensoren noch weitergehen.

Dipl.-Ing. Christian Breuer

TRIMBLE GERMANY GMBH

Am Prime Parc 11 | 65479 Raunheim
E-Mail: christian_breuer@trimble.com

