

## Sicherheitstechnik und Netzwerke

A. Kraheck, Troisdorf

In [1] bis [6] wurden bei einzelnen sicherheitstechnischen Anlagen die Verbindungen mit Netzwerken und die dabei auftretenden Probleme jeweils kurz angesprochen. In diesem Beitrag geht es um die Verbindung der Sicherheitstechnik als Gesamtsystem mit Netzwerken jeglicher Art. Die Form und der Umfang, wie Sicherheitstechnik und Netzwerke miteinander verknüpft werden, sind verschieden und können von akzeptabler Ersatzlösung bis zu völlig indiskutablen Verschmelzungen reichen.

### Ersatzlösungen

Die teilweise (Mit-)Verwendung eines vorhandenen Netzwerkes kann aufgrund von unverhältnismäßig hohen Kosten sinnvoll sein. Beispielsweise mussten in einem weitläufigen Industrieobjekt aus der Petrochemie entlang der Außengrenze einzelne Zugänge für die Mitarbeiter geschaffen werden. Hier sollte neben der Zutrittskontrolle (ZK) auch eine Videoüberwachung (VÜ) an den jeweiligen Personenvereinzelnungsanlagen installiert werden. Die Verbindung der Komponenten an den Außenstellen mit den Zentralen der beiden Systeme hätte bedeutet, dass sowohl unter Fahrbahnen als auch unter der mehrgleisigen Werksbahn hindurch neue Kabel hätten verlegt werden müssen, was in keinem Verhältnis stand. Eine akzeptable Lösung stellte die Anbindung der ZK- und VÜ-Komponenten an das jeweils nächstgelegene Werksgebäude dar, um von dort über das interne Netzwerk eine Verbindung zu den Zentralen zu schaffen (Bild 1). Die Datenrate des ZK-Systems war dabei vernachlässigbar klein. Die Datenmenge aus der Videoüberwachung dagegen stellte für das vorhandene Netz-

werk bereits ein Problem dar, weil dieses veraltet und weitgehend ausgereizt war. Probleme in einer derartigen Netzwerkstruktur können dazu führen, dass kein Videobild mehr zum Überwachungsplatz übertragen wird und dass die Zutrittskontrolle nicht funktioniert. Das Fehlen des Videobildes kann, auch wenn es am Monitor direkt erkennbar sein sollte, über eine Bildausfallerkennung zu einem Alarm führen. Es muss sofort darauf reagiert werden. Der Ausfall der Zutrittskontrolle bedeutet, dass sich die Mitarbeiter zum nächsten Zu-/Ausgang begeben können, um dort die Außengrenze zu passieren. Was passiert aber, wenn ein Fehler in der Personenvereinzelnungsanlage auftritt und ein Mitarbeiter in der Schleuse eingeschlossen ist? Über eine Anweisung kann festgelegt werden, dass beim Erkennen des Ausfalls eines Systems sich ein Sicherheitsmitarbeiter unmittelbar zu dem entsprechenden Standort begibt und dort eine Kontrolle durchführt. Somit besteht bei einem Netzwerkausfall ein nur geringes Restrisiko, das jedoch vertretbar ist.

### Verknüpfungen von Sicherheitszentralen

Dezentrale Absicherungen einzelner Objekte in einer weitläufigen Industrieanlage bedeutet, dass alle Einzelanlagen miteinander verbunden werden müs-

#### Autor

Adolf Kraheck, Troisdorf, ist freier Fachautor auf dem Gebiet unabhängiger sicherheitstechnischer Beratung und Planung.

## Jetzt Verteiler-Aufbaupläne erstellen!



Pläne erstellen so leicht wie nie – normgerecht, schnell und zuverlässig!

**instrom<sup>pro 3.0</sup>** ist eine speziell für die Elektrobranche entwickelte Software für die Planung, Berechnung und Dimensionierung von Niederspannungsanlagen.

Erstellen Sie eine komplette Dokumentation mit detaillierten Anlagenplänen – ganz ohne einen Plan zu zeichnen.

Für jeden Anlagenplan können Sie beliebig viele Verteiler-Aufbaupläne erstellen und diese für zukünftige Projekte verwenden.

Mit den vielen flexiblen Druckvarianten für Ihre erstellten Projekte ist **instrom<sup>pro 3.0</sup>** das optimale Planungsprogramm.

Mehr Informationen unter: [www.instrom.de](http://www.instrom.de)

**ep** ELEKTROPRAKTIKER **10 % Preisvorteil** für ep-Abonnenten. ep**PLUS**-Abonnenten erhalten **20 % Preisvorteil** und können kostenfrei die Demoversion herunterladen.

**Testen Sie jetzt 25 Tage instrom<sup>pro 3.0</sup>!**

**shop huss**  
**HUSS-MEDIEN GmbH**  
 10400 Berlin

**Direkt-Bestell-Service:**  
 Tel. 030 42151-325 · Fax 030 42151-468  
 E-Mail: [bestellung@huss-shop.de](mailto:bestellung@huss-shop.de)  
[www.huss-shop.de](http://www.huss-shop.de)

### Jetzt bestellen!

Ich bestelle zur Lieferung gegen Rechnung zzgl. Versandkosten zu den mir bekannten Geschäftsbedingungen beim **huss-shop HUSS-MEDIEN GmbH 10400 Berlin**

Expl.	Bestell-Nr.	Titel	€/Stück
	7341-1542	<b>instrom pro 3.0 Basismodul</b> (Wohnungsbauprojekte)	249,00
	7341-1536	<b>instrom pro 3.0 Basismodul und Erweiterungsmodul</b> (Wohnungs- u. Gewerbebauprojekte)	499,00
	7341-1539	<b>instrom pro 3.0 Demoversion</b> (uneingeschränkte 25-Tage-Vollversion aller Module)	12,50

KUNDEN-NR. (siehe Adressaufkleber oder letzte Warenrechnung)

Alle Preise zzgl. MwSt.

Firma/Name, Vorname

Branche/Position z. Hd.

Telefon Fax

E-Mail

Straße, Nr. Postfach

Land/PLZ/Ort

Datum Unterschrift ep 0904

Preisänderungen und Liefermöglichkeiten vorbehalten

sen, um sie dann einem Alarmmanagementsystem zuzuordnen. Auch hier spielen Kosten eine vorrangige Rolle, warum die Verbindungen der Unterzentralen mit der jeweiligen Hauptzentrale über vorhandene Leitungen gewünscht wird. Da bei vielen Systemen eine Netzwerkanbindung möglich ist, liegt es nahe, das vorhandene Netzwerk mit zu nutzen (Bild 2).

Netzwerke sind keine Sicherheitssysteme. Folglich ist nie sichergestellt, dass alle relevanten Daten mit nur minimalster Verzögerung von einem Punkt zum nächsten übertragen werden. Wer sich in sein Auto setzt, um von A nach B zu fahren, darf nicht davon ausgehen, dass er dort auch tatsächlich oder zu einem bestimmten Zeitpunkt ankommt. Es gibt zu viele Variablen, auf die der Fahrer keinen Einfluss hat. Beim Netzwerk verhält es sich ebenso. Viele Personen greifen außerhalb der Sicherheitsanlagen auf das Netzwerk zu. Jeder kann zu jedem Zeitpunkt, auch ohne Vorsatz, das Netzwerk stilllegen. Mit vorsätzlichen Manipulationen ist ebenso zu rechnen.

Im Gegensatz zum vorherigen Beispiel geht es beim Ausfall des Netzwerkes nicht mehr darum, dass ein Mitarbeiter vielleicht verspätet seinen Feierabend antreten kann, sondern u. U. um die brandmeldetechnische Überwachung einer Produktionshalle, in der zufällig nicht gearbeitet wird und ein Brandausbruch vor Ort nicht entdeckt werden kann.

Ein nur verspätet gemeldeter und bearbeiteter Brandalarm kann schon dazu führen, dass ein Objekt nicht mehr zu retten ist und ein Schaden entsteht, der bei funktionierendem Netzwerk hätte deutlich geringer ausfallen können. Aktuelle Gerichtsurteile zeigen, dass dann vorrangig die Frage zu klären ist, hat die BMA so funktioniert, wie es mit dem Kunden vereinbart war bzw. wie der Kunde es erwarten konnte? Netzwerkstörungen und -ausfälle sind aber vorhersehbare Ereignisse, so dass eine für sich gesehen einwandfrei funktionierende BMA im Verbund mit einer Hauptzentrale und einem Managementsystem plötzlich einen gravierenden Mangel aufweist.

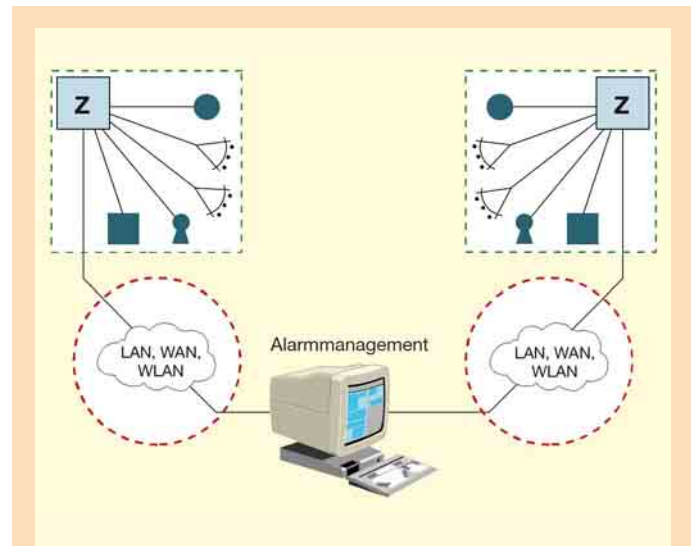
## Outsourcing

Dem Trend der Zeit folgend, werden im Netzwerkbereich immer mehr Dienstleistungen an externe Unternehmen vergeben. Vorrangig ist hier die Auslagerung von Daten auf externe Server zu nennen. Wer berät seinen Kunden darüber, welches Gefahrenpotential entsteht, wenn im Rahmen alleine von Backups über das Internet sicherheitsrelevante Daten, Informationen, Videodokumentationen usw. das zu sichernde Unternehmen „verlassen“? Kann überhaupt sichergestellt werden, dass die ausgelagerten Daten nicht gegen das zu schützende Unternehmen eingesetzt werden? Absolute Sicherheit bei der Übertragung und Speicherung der Daten außerhalb des Unternehmens gibt es nicht. Dieses zeigen die Datendiebstähle und Hackerangriffe der vergangenen Jahre, von denen i. d. R. nur die spektakulärsten Fälle an die Öffentlichkeit geraten.

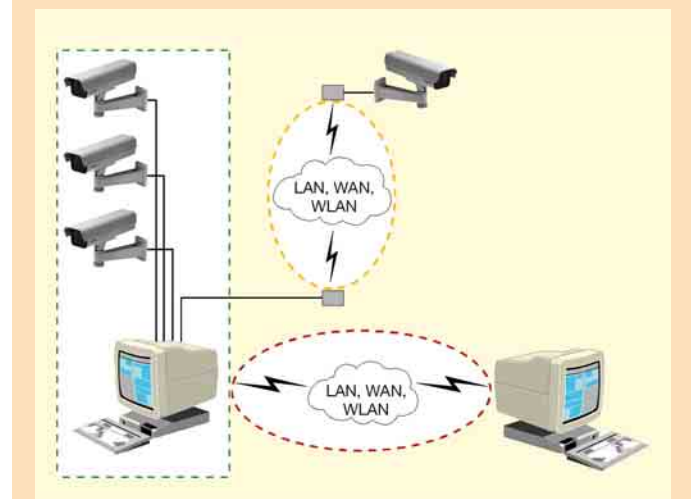
**Zutrittskontrolle.** In einer Fachzeitschrift aus dem Sicherheitsbereich war zu lesen, dass sich in einem Forum jemand darüber auslässt, dass deutsche Unternehmen (im Gegensatz zum Ausland) noch zu wenig ihre Zutrittskontrolle auf externe Dienstleister übertragen. Als Verkaufsargument für das Outsourcing von Zutrittskontrollsystemen verständlich, aber vielleicht sind die deutschen Unternehmen doch sicherheitsbewusster als ausländische.

**Kontrolle durch Unternehmen.** Unabhängig vom Datenschutz bedeutet es, dass alle Daten, die für die Kontrolle von Zutrittsberechtigungen auf einem externen Server gelagert sind. Eine Person, die sich an einem Zugang identifiziert, löst eine Datenübertragung zu diesem Server aus und von dort erfolgt die Freigabe oder Abweisung. Unabhängig davon, dass das ursprünglich zu schützende Unternehmen keine Kontrolle über die Vorgänge hat, ist die jederzeitige Funktion des Systems nicht sichergestellt.

**Verfügbarkeit.** Zwar argumentieren die Befürworter damit, dass bei den heutigen Netzwerken ein einwandfreies Funktionieren mit nur minimalsten zeitlichen Ver-



1 Anbindung der ZK- und VÜ-Komponenten an das jeweils nächstgelegene Gebäude, um über das interne Netzwerk eine Verbindung zur Zentrale zu schaffen



2 Vorhandene Netzwerke sind keine Sicherheitssysteme – die Datenübertragung ist nicht sichergestellt

zögerungen gewährleistet sei. Doch problematisch wird es dann, wenn an irgendeiner Stelle der gesamten Netzwerkstruktur eine Unterbrechung oder Manipulation stattfindet.

**Beispiel.** Mitarbeiter, die morgens zur Arbeit wollen, können das Firmengelände nicht betreten, weil die Zutrittskontrolle nicht funktioniert. Hier kann es zu einem nicht vorhersehbaren Schaden durch Produktionsausfälle kommen. Wer haftet dann? Der Unternehmer hat alle notwendigen Freigaben im Vorfeld veranlasst. Die Mitarbeiter sind arbeitswillig, können ihren Arbeitsplatz aber nicht erreichen. Der externe Dienstleister be-

kommt wegen der Netzwerkunterbrechung keine Anfragen von den ZK-Terminals und kann somit den Mitarbeitern keinen Zutritt gewähren. Und der Errichter? Hat er ein mangelfreies Zutrittskontrollsystem installiert, das den Wünschen des Kunden entspricht und den Mitarbeitern jederzeit den berechtigten Zutritt zum Werksgelände gewährt?

## Zentralsystem als neuer Weg?

Neben der klassischen Einbindung einzelner Anlagen oder Anlagenkomponenten gibt es An-

bieter, die einen völlig anderen Weg beschreiten. Bei ihnen gibt es keine EMZ, BMZ usw. mehr, sondern alle Anlagenkomponenten werden direkt in ein Netzwerk eingebunden. Das bedeutet, dass z. B. Bewegungsmelder, ZK-Terminals, Kameras usw. über entsprechende Schnittstellen mit dem Netzwerk verbunden sind. Die Auswertung der eingehenden Signale erfolgt durch eine allumfassende Software, die neben den Bereichen GLT und Facilitymanagement so nebenbei auch für die Sicherheitstechnik zuständig ist.

**Keine autarken Teilbereiche.** Je komplexer eine Software ist, umso schwieriger wird es, über einen längeren Zeitraum eine fehlerfreie Funktion zu gewährleisten. Im Gegensatz zum Standardnetzwerk, bei dem in einzelnen Segmenten verschiedener Programme gearbeitet wird und im Störfall ggf. einzelne sicherheitstechnische Anlagen nicht mehr funktionieren, bedeutet eine Software, die alles gleichzeitig handelt, dass ein Ausfall alles lahmlegen kann. Es gibt keine Zentralen mehr, die zumindest in Teilbereichen autark weiter funktionieren.

**Notstromversorgung.** Bei allen Varianten der direkten Einbindung von Meldungsgebern in das Netzwerk, insbesondere bei der hier beschriebenen, gibt es einen gravierenden Mangel. Jedes einzelne Gerät muss ausreichenden mit Notstrom versorgt werden. POE ist da nur bedingt ein Mittel. Alle teuren Netzwerkkomponenten mit POE müssten ihrerseits an einer Notstromversorgung betrieben werden, was an sich schon zu einem aufgeblähten Netzwerk führt. Der Einsatz von Batterie/Akku, wie bei Funk-EMA und -BMA, ist nicht für alle Anwendungen geeignet. Zudem sind die Kosten deutlich höher, als bei der konventionellen Notstromversorgung in einer eigenständigen Zentrale. Sowohl POE als auch Batterie/Akku-Einsatz scheitern auch daran, dass einzelne sicherheitstechnische Komponenten einen hohen Stromverbrauch haben (selbst für die neuen Variante von POE). Alleine aufgrund der Problematik mit der Notstromversorgung sind

derartige Anlagen niemals sicherheitstechnische Anlagen im Sinne der VDE 0833.

## Öffnung autarker Strukturen

Auch wenn bisher das Hauptaugenmerk auf Netzwerken, wie LAN, WAN, WLAN usw. lag, so sind die Betrachtungen in gleicher Weise auf Verknüpfungen mit Bus-Systemen, wie z. B. dem EIB anzuwenden. Ferner sind alle Überlegungen aus dem Bereich großer Industrieanlagen in gleicher Weise auch auf kleine Objekte anwendbar.

Die Einbindung von Sicherheitstechnik in Netzwerke bedeutet die Öffnung ansonsten in sich geschlossener und autarker Sicherheitsstrukturen. Es kann zu Vereinfachungen in der Handhabung durch den Kunden oder zu etwas mehr Flexibilität im Systemaufbau kommen. Jedoch kann unter Umständen das Schutzziel, welches für das Objekt definiert wurde, nicht mehr erreicht werden. Jetzt ist vorrangig nicht das Objekt, sondern das Netzwerk mit den daran angeschlossenen sicherheitstechnischen Systemen zu schützen, damit diese wiederum ihre Schutzfunktion, bezogen auf das Objekt, fehlerfrei ausüben können. Dies muss nicht nur dem planenden und ausführenden Unternehmen klar sein, sondern der Kunde muss von Anfang an auf die Risiken von Netzwerkanbindungen hingewiesen werden. Ansonsten ist bereits die Beratung unzureichend.

## Beratung und Haftung

Wer haftet, wenn ein Sicherheitssystem aufgrund von Netzwerkproblemen nicht einwandfrei funktionieren konnte und dadurch Menschen (oder Sachwerte) zu Schaden gekommen sind? Zusätzlich zu allen Schutzmaßnahmen, die allgemein zu treffen sind, damit ein sicherheitstechnisches System nicht manipuliert werden kann (z. B. Sabotageschutz), sind bei jeder Form der Einbindung dieser Anlagen in Netzwerke zusätzliche Maßnahmen zu treffen, um

Störungen, Unterbrechungen oder Ausfälle nach menschlichem Ermessen und entsprechend dem Stand der Technik möglichst zu verhindern bzw. auf ein als noch akzeptables Restrisiko zu vertretendes Minimum zu reduzieren.

Bereits in der Beratungs-/Planungsphase ist ein erheblicher Mehraufwand erforderlich. Fehler bei den späteren Anlagen beschränken sich nicht nur auf Fehlbedienung durch den Kunden, sondern ergeben sich aus der gesamten Firmenstruktur beim Kunden. Von ihm müssen alle relevanten Informationen eingeholt werden, wie z. B.

- Wie ist der Aufbau des Firmen-netzwerkes?
- Wer arbeitet an diesem Netzwerk?
- Wer hat Zugriff auf das Netzwerk?
- Welche externen Unternehmen haben Zugriff auf das Netzwerk?
- Wie ist das Netzwerk strukturiert?
- Wie hoch ist die bisherige Belastung des Netzwerkes?
- Welche Komponenten sind im Netzwerk integriert usw.?

Nur wenn alle Eventualitäten späterer Probleme und Ausfälle, soweit anhand der zur Verfügung stehenden Informationen möglich, berücksichtigt werden, besteht bei einem Schadensfall die Möglichkeit, das anschließende Verfahren zumindest halbwegs unbeschadet zu überstehen. Das verdeutlicht auch, wie wichtig es ist, die notwendigen Informationen nicht nur einzuholen,

sondern auch schriftlich festzuhalten. Damit kann ggf. belegt werden, dass der Kunde wichtige Informationen zurückgehalten hat. Aber auch das ist kein Freibrief, denn dem Errichter wird man unter Umständen vorhalten, dass es aufgrund seiner Berufsausbildung und des zu unterstellenden Sachverstandes bestimmter Informationen durch den Kunden nicht bedurft hätte. Unwissenheit schützt nun mal nicht vor Strafe.

## Fazit

Wenn Sicherheitstechnik über ein Netzwerk miteinander verbunden werden sollte, dann möglichst nur über ein eigenständiges und vom Unternehmensnetzwerk abgekoppeltes Netzwerk, zu dem nur Sicherheitsverantwortliche und Sicherheitsdienstleister Zugang haben dürfen.

## Literatur

- [1] Kraheck, A.: Einbruchmelde- und Elektrotechnik. Elektropraktiker Berlin 62(2008)5, S. 433–435.
- [2] Kraheck, A.: Brandmelde- und Elektrotechnik. Elektropraktiker Berlin 62(2008)6, S. 530–531.
- [3] Kraheck, A.: Video-Überwachungstechnik. Elektropraktiker Berlin 62(2008)8, S. 698–699.
- [4] Kraheck, A.: Zutrittskontrolle. Elektropraktiker Berlin 62(2008)10, S. 896–898.
- [5] Kraheck, A.: Alarmmanagementsysteme. Elektropraktiker Berlin 62(2008)11, S. 990–993.
- [6] Kraheck, A.: Überwachungsplätze. Elektropraktiker Berlin 62(2008)12, S. 1091–1093.

www.valentin.de

## Photovoltaik & Solarthermie

### Softwarelösungen für Profis von Valentin EnergieSoftware

Kostenlose DEMOS und TUTORIALS zum Herunterladen!

- Planungssoftware
- Firmensoftware
- Onlineberechnung

Madrid-Spanien  
12.-14. Mai 2009  
Halle: 7 Stand: E 35

Dr. Valentin EnergieSoftware GmbH  
Stralauer Platz 34, D-10243 Berlin  
Tel: +49 (0)30/ 588 439-0, Fax: -11  
info@valentin.de