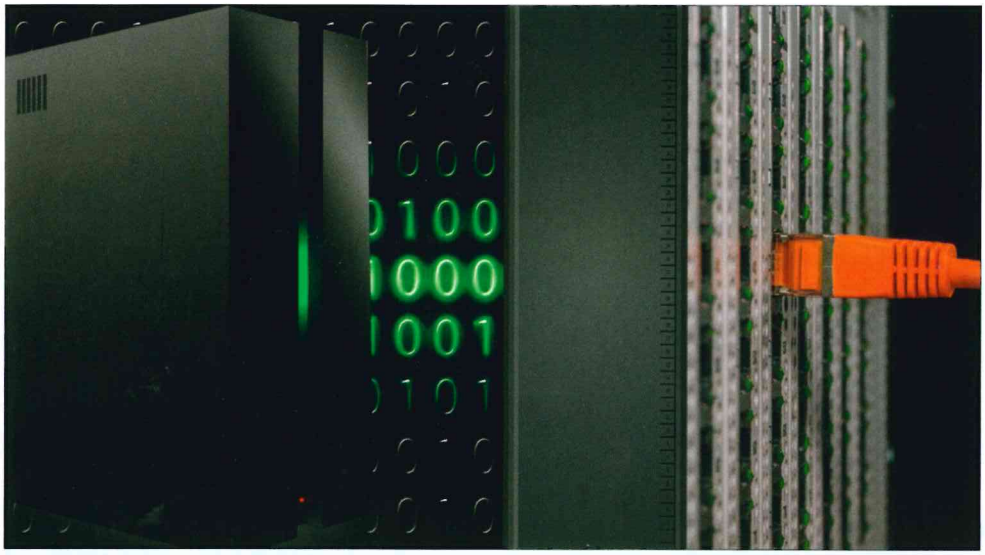
IP-basierte Übertragungstechnik und ihre Möglichkeiten

Alarmübertragung in der Cloud – Zukunftsvision oder Realität?

AUTOR: DIPL.-ING. STEPHAN HOLZEM



IP-basierte Kommunikation ist heute Standard (Quelle: ugoxuqu/ Pixabay, CCo)

Spätestens mit der laufenden All-IP-Umstellung der großen Netzbetreiber in Deutschland ist klar, dass die Alarmübertragung zukünftig ausschließlich über IP-Netze stattfinden wird. Folgerichtig haben sich die Richtlinien für die Übertragungstechnik geändert, um dem Wandel der Netze gerecht zu werden. Und die Entwicklung schreitet voran.

Es muss nicht weiter diskutiert werden, dass eine Übertragung per analoger oder ISDN-Protokolle keine zukunftsweisende Option mehr darstellt. Es hat sich sogar inzwischen herumgesprochen, dass selbst in den Funknetzen das Ende der leitungsvermittelten Übertragung eingeläutet ist. Die ersten Funknetzanbieter im benachbarten Ausland wie der Schweiz und auch in den Niederlanden haben den häufig für die Alarmübertragung über GSM genutzten CSD Datendienst abgekündigt, sodass auch hier zukünftig nur noch paketorientierte Dienste wie GPRS, UMTS oder gar LTE für die Übertragung genutzt werden sollten. Also wer in seinem Übertragungsgerät als Zieladressen noch Rufnummern programmiert, sei es für Funk- oder Festnetz, ist nicht mehr zukunftsweisend unterwegs. Eine zukunftsweisende Adressierung geht nur noch über IP-Adressen.

Die Normen folgen dem Wandel der Netze

Bereits seit dem Jahr 2012 gibt es inzwischen die „neue" Kernnorm für die Übertragungstechnik EN 50136-1, welche unabhängig von der Anwendung Leistungsmerkmale und Anforderungen für ein Übertragungssystem festlegt. Neu ist gegenüber früheren Richtlinien, dass keine konkreten Wege oder Lösungen beschrieben werden, sondern ausschließlich geforderte Leistungsmerkmale wie Übertragungsdauer, Zeiträume bis zur Ausfallerkennung eines Weges, Maßnahmen zur Informationssicherheit und Redundanzvorgaben. Diese Parameter werden durch die entsprechenden zugelassenen Übertragungsgeräte und Empfänger kontinuierlich überwacht und durch ein Monitoring-Center aufgezeichnet (welches im Allgemeinen in Deutschland Bestandteil der Alarm-Empfangsstelle (AES) ist). Abweichungen vom Sollzustand werden erkannt, sodass entsprechende Maßnahmen eingeleitet werden können. Die Aufzeichnungen werden regelmäßig von der die Leitstelle betreuenden Zertifizierungsstelle geprüft.

Und was kommt jetzt?

An diesen neuen Umgang mit der IP-Übertragungstechnik und den neuen Blickwinkel der Richtlinienwelt haben wir uns gerade gewöhnt. VdS hat aktuell seine Richtlinienwerke an diesen neuen Standard angelehnt und konkretisiert. Die neu erschienene VdS 2311 verweist für die VdS-Klasse A im Wesentlichen auf die Übertragungsklasse Single Path 4 nach EN 50136-1; Klasse-C-Anlagen sollen Systeme nach Dual Path 4 nutzen.

In der europäischen Working Group 5 des Technischen Komitees der CENELEC, welches für die Weiterentwicklung der EN 50136 verantwortlich ist, gehen die Gedanken

schon weiter: Es wird bereits an einem Anhang EN 50136-1/A1 gearbeitet, welcher zwar noch nicht final in Europa abgestimmt wurde, jedoch deutlich klarmacht, in welche Richtung die Alarmübertragung sich weiterentwickelt.

Aus ARC und MRT wird MARC

Ein MARC (Monitoring Alarm Receiving Center) ist neu die Zusammenführung aus Monitoring- und Alarmempfangsstelle. Gegenüber den bisherigen Einzelbegriffen ARC (Alarm Receiving Center) und MCT (Monitoring Center Transceiver) wird nun deutlicher gemacht, dass hier nicht nur der Alarmempfang stattzufinden hat, sondern auch das Monitoring, also die Überwachung der aufgeschalteten Übertragungsgeräte.

Mit dem neuem Begriff „Secure Location" (Sichere Umgebung), geht es schnell in die Nähe von zukünftigen Cloud-Lösungen für den Alarmempfang. Eine „Secure Location" kann nach dem vorliegenden Norm-Entwurf entweder eine AES (MARC) oder ein Rechenzentrum nach einem Rechenzentrumstandard wie z. B. TIER 3 oder EN 50600 sein.

An diesem Standort dürfen sich dann zukünftig unter bestimmten Voraussetzungen die Alarmempfänger befinden, ohne dass es Anforderungen an eine personelle Besetzung oder gar an die „Dicke der Wände" gäbe. Bisher war das undenkbar. In der AES gibt es dem Entwurf folgend dann nur noch ein „IRCT" – das Interface zum RCT, dem Alarmempfänger.

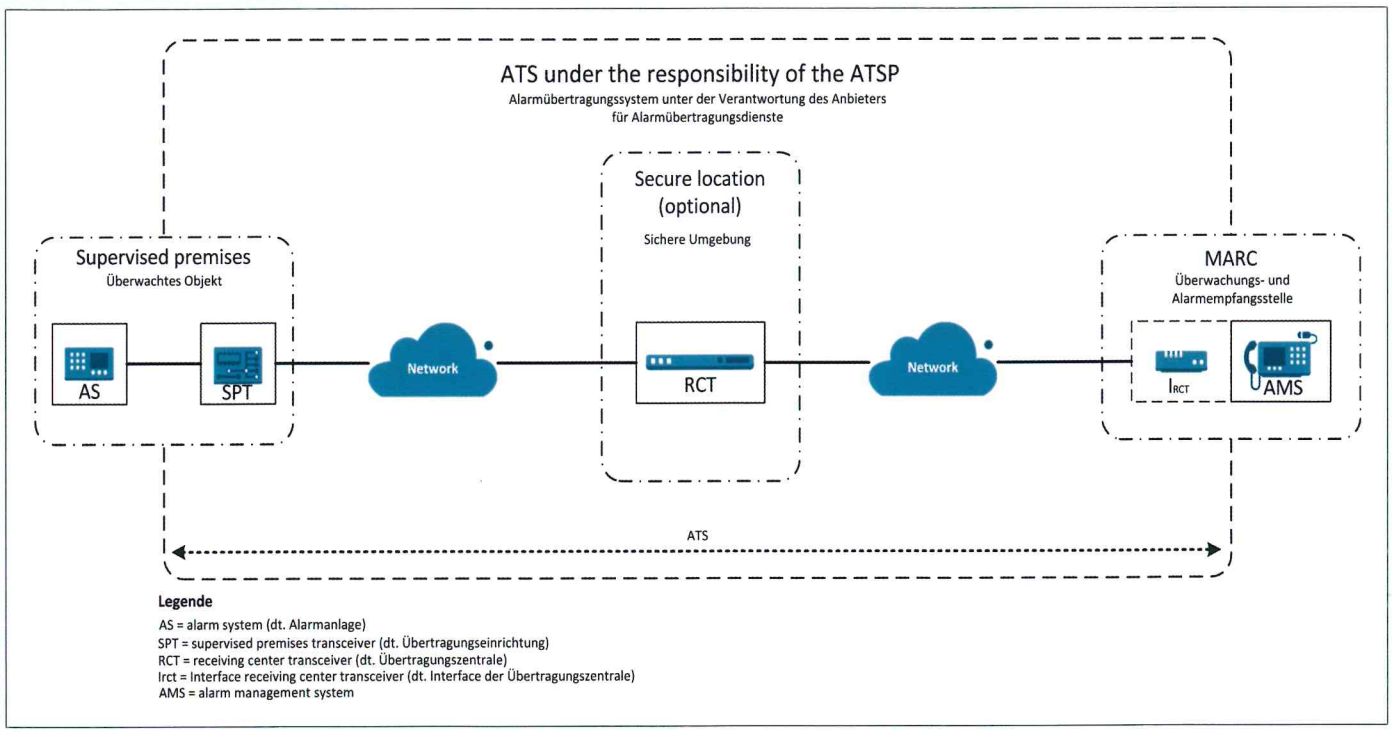
Die Cloud – Basis für die Alarmübertragung? (Quelle: wynpnt/ Pixabay, CCo)

Dieser Umsetzungsgedanke scheint möglich und ist nachvollziehbar, da die nach EN 50136 definierten Leistungsparameter auch zukünftig wie bisher in der AES (herkömmlicher Definition nach EN 50518) gemessen und überwacht werden müssen.

Die Zusammenhänge werden klarer, wenn man die Definition des Begriffes ATSP beleuchtet (dieser ist nicht grundsätzlich neu, wird aber deutlich konkretisiert). ATSP heißt konkret „Alarm Transmission Service Provider" und ist damit der „Anbieter von Alarmübertragungsdiensten". Dieser ist nach Definition verantwortlich für Planung, Betrieb und Nachweis der Leistungsmerkmale der Übertragungswege. Der ATSP kann ein unabhängiges Unternehmen, eine Unterorganisation der Leitstelle, der Errichter oder ein Netzwerkserviceprovider sein.

ATSP nach Norm immer erforderlich

Nach Norm ist der ATSP zukünftig in den höheren Übertragungsklassen immer erforderlich. Der ATSP kann Teilverantwortungen durch Verträge an Kunden, Alarmempfangsstellen und Netzprovider weitergeben. Er behält nach Definition aber im-



Beispiel für ein „Hosted Alarm Transmission System" (Quelle: EN 50136-1 prA1 for comment)

In einem Sicherheitsnetz mit geschlossener Benutzergruppe läuft der Datenverkehr unabhängig von der Internet-Kommunikation und ist damit weniger anfällig für Angriffe (Quelle: typographyimages/ Pixabay, CC0)

mer die Gesamtverantwortung für die gesamte Übertragungsstrecke. Über diese Definition werden der Betrieb und die Verantwortung der Komponenten in der „Cloud" verbindlich definiert und sichergestellt. Ein ATSP ist für Cloud-Lösungen (Hosted ATS) immer erforderlich. Für klassische Anwendungen, bei denen sich der Alarmempfänger in der AES befindet, besteht die Anforderung ab der Anwendungsklasse Single Path 4 bzw. Dual Path 2.

Aus der alten BE (Bedieneinrichtung) wird langsam das AMS – Alarmmanagementsystem mit den Aufgaben der Verwaltung des Speicherns, Organisierens und der Verwaltung von Kundensystemen. Dass an diese Systeme keine Hardwarevoraussetzungen mehr gestellt werden, muss nicht weiter betont werden.

Hosted ATS

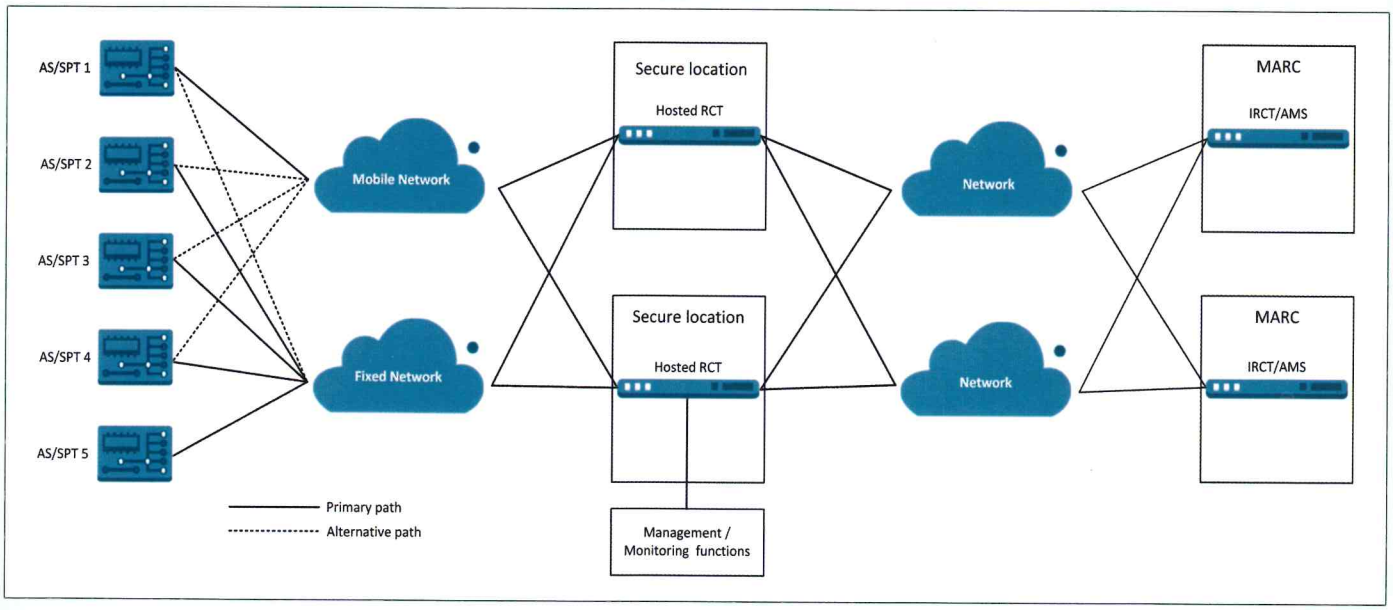
Zusammengefasst beschreibt sich die neue Cloud-Lösung „Hosted ATS" wie folgt:

- ❑ Der Alarmempfänger (RCT) in einem Rechenzentrum „Secure Location" kann über ein entferntes Interface (IRCT) über ein sicheres Netzwerk mit dem AMS im MARC verbunden sein.
- ❑ Die Secure Location muss mindestens dem „TIER 3"-Standard entsprechen.
- ❑ Die Performance der Schnittstelle zwischen Rechenzentrum und MARC muss mindestens der Performance der höchsten Kategorie der aufgeschalteten Geräte entsprechen.
- ❑ Das Monitoring der gesamten Strecke der Alarmübertragung ist Aufgabe des ATSP (Anbieter für Alarmübertragungsdienste).
- ❑ Das Interface zwischen Alarmempfänger (RCT) und AMS (IRCT) liegt in der Verantwortung des ATSP.
- ❑ Für die Klassen D1 bis D4 ist eine gedoppelte Schnittstelle zwischen RCT und AMS erforderlich.

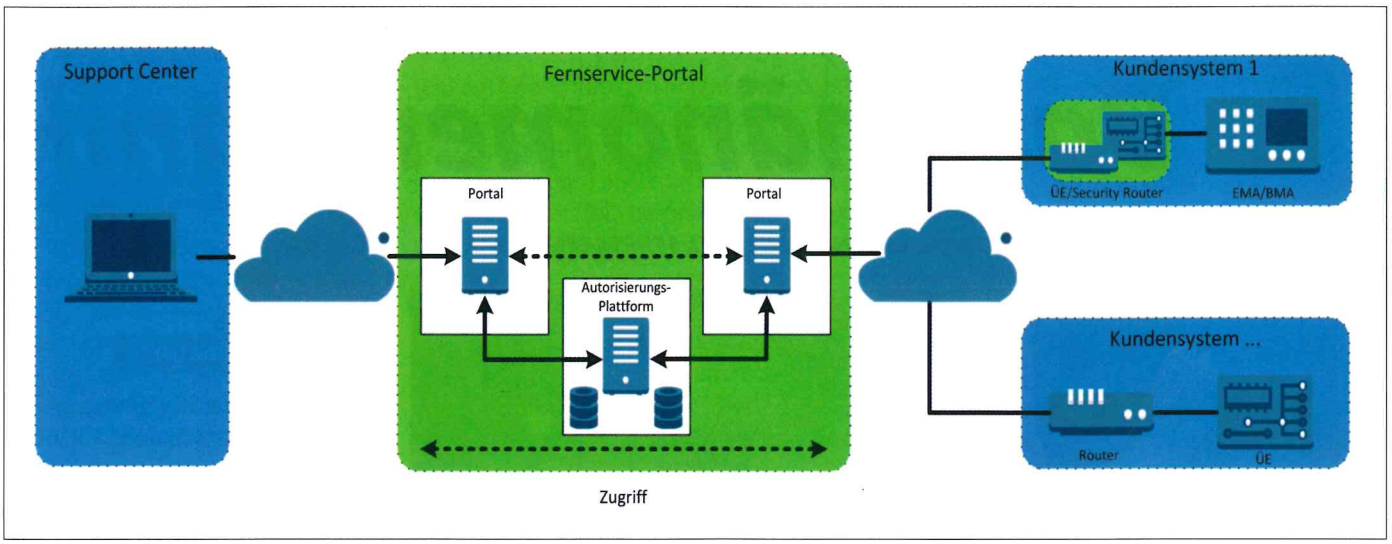
Wir dürfen gespannt sein, wie Europa final zu diesem Richtlinienentwurf abstimmen wird und wie sich nationale Richtliniengeber wie VdS in den nächsten Jahren zu den neuen Gedanken stellen werden. Es wird in jedem Falle deutlich, dass die Virtualisierung von Systemen auch vor den Komponenten der Sicherheitstechnik keinen Halt machen wird.

Muss die „Cloud" auf öffentlichen Netzen basieren?

Grundsätzlich eignen sich nach europäischen Normen und nationalen Richtlinien alle IP-basierten Netzformen zur Alarmübertragung – sofern man die Vorgaben der Normen und Richtlinien richtig anwendet und entsprechend zugelassene Systemkomponenten einsetzt. Zu diesen möglichen Netzformen gehören:



Beispiel eines Systemaufbaus für ein Übertragungssystem mit „Hosted RCT" (Quelle: EN 50136-1 prA1 for comment)



Struktur „Remote Services" in schematischer Darstellung (Quelle: TAS Sicherheits- und Kommunikationstechnik)

- ❑ Ein öffentliches Netz – Internet
- ❑ Ein vom Internet abgetrenntes Netz – Intranet z. B. einer Bank oder eines Filialunternehmens
- ❑ VPN-Netze von Filialunternehmen auf Basis des Internets
- ❑ Sogenannte „Sicherheitsnetze" mit geschlossener Benutzergruppe

In den letzten Jahren entstehen in Deutschland im Bereich der professionellen Alarmaufschaltung vermehrt sogenannte „Sicherheitsnetze". Diese Sicherheitsnetze beschreiben Netze mit „geschlossener Benutzergruppe". Das heißt, die Datenkommunikation läuft unabhängig vom öffentlichen Internetdatenverkehr.

Sicherheitsnetze: Vorteile bei Verfügbarkeit und Schutz gegen Angriffe

Die Nutzung von Sicherheitsnetzen gegenüber öffentlichen Netzen bietet generell einige Vorteile. Diese beziehen sich im Wesentlichen auf die höhere Verfügbarkeit des Übertragungssystems. Bei der Übertragung in einer „geschlossene Benutzergruppe" werden vom Netzanbieter eigene Netz-Zugangskennungen bereitgestellt. Der Datenverkehr ist nur zwischen den Teilnehmern im „Sicherheitsnetz" möglich.

Der gesamte Datenverkehr ist nicht öffentlich sichtbar und damit prinzipiell weniger anfällig für Angriffe jeglicher Art. Sicherheitsnetze werden angeboten für Fest- und Funknetze. Kombinationen von Netzen (z. B. Verwendung des vorhandenen öffentlichen IP-Anschlusses eines Privathauses für den ersten Übertragungsweg und Nutzung eines Funknetzes mit geschlossener Benutzergruppe für den zweiten Übertragungsweg) sind denkbar und in Abstimmung mit der AES möglich.

In Sicherheitsnetzen sind keine „Denial of Service"-Angriffe aus dem öffentlichen Internet möglich. Der Betreiber kann sogar Bandbreiten und Verfügbarkeitszusagen für seine Netze anbieten. Vertraglich können Service Level Agreements und Entstörzeiten für bestimmte Leitungsabschnitte definiert werden. Letztendlich kann die Verantwortung für das Netz klar zugewiesen werden. Dies vereinfacht die Erfüllung der Aufgaben des ATSP (Anbieter für Alarmübertragungsdienste) deutlich.

Welche Möglichkeiten bieten die „neuen Netze" in Bezug auf Remote Services?

Die Anbindung von Einbruch- oder Brandmeldesystemen über ein Übertragungsgerät an eine IP-basierte Netzstruktur eröffnet neue Möglichkeiten in Bezug auf Fernservicedienstleistungen – dabei ist es zunächst unerheblich, ob ein Sicherheitsnetz oder eine internetbasierende Cloudlösung verwendet wird. **Aus technischer wie auch** aus organisatorischer Sicht ist dies jedoch eine neue Herausforderung. Idealerweise soll ein Fernservice auf die dem Übertragungsgerät nachgeschalteten Systeme (meist Brandmelde- oder Einbruchmeldeanlagen) erbracht werden.

Dabei sollte Beachtung finden, dass die genannten Systeme ständig und unabhängig von der Netztopologie oder Firewallkonfiguration des Kunden zu erreichen sind. Dazu können über die Übertragungstechnik bereits heute VPN-Tunnel zu Fernserviceplattformen aufgebaut werden. Techniker oder Systeme, die einen Zugriff auf die Kundensysteme benötigen, stellen ebenfalls eine gesicherte Verbindung auf eine entsprechende Plattform her. Eine zentrale Berechtigungsverwaltung regelt den Zugriff zwischen Techniker und Kundensystem. Spezielle Sicherheitsrouter mit integrierter Alarmübertragungseinrichtung lassen die Anforderungen von Übertragungssystem und VPN-Router zusammenwachsen und ermöglichen die wirtschaftliche Realisierung einer effektiven Gesamtlösung.

Auch dieser Bereich „Remote Services für Alarm Systems" findet derzeit in der nationalen und internationalen Normung große Beachtung. Die ersten Normungsvorhaben befinden sich bereits in der Umsetzung.

Der Autor dieses Beitrags, ***Dipl.-Ing. Stephan Holzem***, ist Geschäftsführer der TAS Telefonbau A. Schwabe GmbH & Co. KG.

Kontakt: SHolzem@tas.de