Einfach, schnell und herstellerunabhängig

Alarmbildempfang mit FTP-Upload

Bei aller Vielfalt der Videogeräte verschiedener Hersteller gibt es doch einige Funktionen und Verfahren, die sich in der Praxis bewährt haben, die viele Hersteller übernommen haben und die somit geeignete Ansatzpunkte für den gemeinsamen Betrieb verschiedener Systeme liefern. Immer mehr Videogeräte bieten beispielsweise die Möglichkeit, Alarmbilder per FTP-Upload zu übertragen. Dieser Artikel erläutert die technischen Grundlagen und praktische Anwendung dieses Verfahrens.

Von Hardo Naumann, Hannover

Die meisten Hersteller legen ihren Videogeräten so genannte Remote- oder Client-Software bei, die auf einem PC installiert wird und mit der aus der Ferne auf Geräte dieses Herstellers zugegriffen werden kann. Solange nur wenige Geräte eines einzigen Herstellers zum Einsatz kommen, ist dies oft völlig ausreichend. Schwieriger wird es, wenn Videogeräte verschiedener Hersteller miteinander kombiniert werden sollen, denn die herstellerspezifische Software unterstützt in der Regel nur eigene Fabrikate, nicht aber Geräte anderer Hersteller.

Sofern Verbindungen nur von der Leitstelle zu den Bildquellen aufgebaut werden sollen, können die Mitarbeiter sich noch damit behelfen, zunächst die jeweils passende Client-Software zu starten und damit anschließend die gewünschte Verbindung aufzubauen. Wenn aber Ereignisse wie Bewegungen, Alarme und Störungen von den Videogeräten an die Leitstelle gemeldet werden sollen, müssen Verbindungen auch in umgekehrter Richtung, also von den Bildquellen zur Leitstelle aufgebaut werden. Es ist nicht vorhersehbar, welches Gerät welchen Herstellers das nächste Ereignis melden wird. Zum Empfang herstellerspezifischer Ereignisse muss aber die passende Client-Software laufen. Dies scheitert daran, dass viele dieser Client-Anwendungen die gleichen Ressourcen wie beispielsweise Speicher, Rechenleistung und TCP/IP-Ports benötigen und daher ein Parallelbetrieb vieler Anwendungen zu Ressourcen-Konflikten führt.

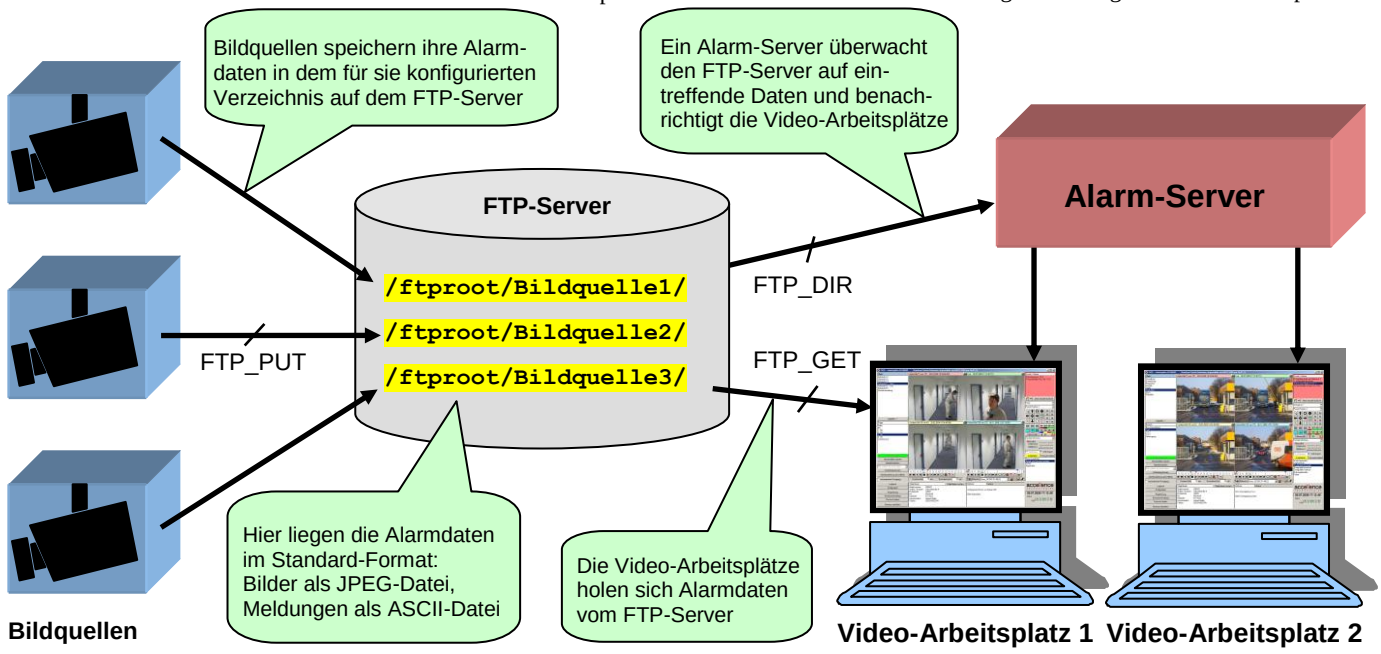
Die Lösung für dieses Problem besteht darin, zum Übertragen von Ereignisdaten Verfahren zu nutzen, die sich in anderen Bereichen bereits bewährt haben und die offen, herstellerunabhängig und ausreichend genau spezifiziert sind. Viele Hersteller haben solche Verfahren in ihren Videogeräten implementiert, beispielsweise

- FTP-Upload
- SMTP / MIME (Email)
- TCP/IP-Verbindungen
- SNMP-Traps
- WebService / SOAP

FTP steht als Abkürzung für File Transfer Protocol [1] und bezeichnet ein Verfahren, mit dem beliebige Dateien auf einem Server gespeichert und wieder abgerufen werden können. FTP wurde im Oktober 1985 spezifiziert [2] und hat sich seitdem in vielen Anwendungsfällen bewährt. Die Software, die benötigt wird, um einen PC als FTP-Server nutzen zu können, ist entweder bereits im Betriebssystem enthalten (etwa im Internet Information Service von Windows-Servern) oder kann kostenlos geladen werden, beispielweise unter http://filezilla-project.org. Auch dies trägt zur großen Verbreitung von FTP bei.

FTP-Server zur herstellerneutralen Übergabe von Alarmdaten

Die Grundidee: Ein FTP-Server wird als herstellerneutrale und standardisierte Übergabestelle für die typischen Alarmdaten von Videoüberwachungsgeräten, also Bilder und Meldungstexte, genutzt. Bilder werden dazu im JPEG-Format [3], Texte als ASCII-Datei [4] übertragen. Zum Alarmbildempfang wird in der Leitstelle ein FTP-Server eingerichtet, auf den im Alarmfall alle Videogeräte ihre Alarmbilder und Meldungen übertragen können. Es empfiehlt



Ein FTP-Server als einfache herstellerneutrale und standardisierte Übergabestelle für Alarmbilder und Meldungen

sich, für jede Alarmquelle ein eigenes Unterverzeichnis auf dem FTP-Server einzurichten und dafür jeweils eigene Zugangsdaten (Benutzername, Passwort) zu konfigurieren. Damit wird sichergestellt, dass nur berechtigte Sender ihre Alarmdaten dort speichern können und dass sich verschiedene Alarmquellen nicht gegenseitig beeinflussen.

Aus Gründen der Datensicherheit wäre es am besten, wenn kein Zugriff von außen erfolgen müsste, sondern alle Verbindungen in einem geschlossenen Netz erfolgen. Wenn doch einmal Verbindungen physikalisch über öffentliche Netze geführt werden müssen, beispielsweise um größere Entfernungen zu überbrücken, können sie durch so genannte VPN-Tunnel [5] vor unbefugten Zugriffen geschützt werden; VPN steht als Abkürzung für ein virtuelles privates Netzwerk, das zwar physikalisch über öffentliche Leitungen realisiert wird, aber mittels geeigneter Verschlüsselungsverfahren logisch vom öffentlichen Netz völlig getrennt ist.

Wenn eine Leitstelle auch Aufschaltungen aus dem öffentlichen Netz empfangen will, müssen Anfragen an die vom FTP-Server genutzten TCP/IP-Ports vom Router zu dem PC weitergeleitet werden, auf dem die FTP-Server-Software läuft (so genanntes Port-Forwarding); an der Firewall müssen diese Ports freigegeben werden. Da solche Zugänge bei Konfigurationsfehlern ein erhebliches Sicherheitsrisiko darstellen, darf die Konfiguration von Router, Firewalls und FTP-Server nur durch ausreichend qualifiziertes und vertrauenswürdiges Fachpersonal erfolgen. Grundlegende Regeln für eine sichere IT-Infrastruktur findet man in den IT-Grundschutz-Katalogen des Bundesamtes für Sicherheit in der Informationstechnik (BSI, [6]). Aus Sicherheitsgründen sollte ein öffentlicher FTP-Server beispielsweise stets in einer demilitarisierten Zone (DMZ, [7]) betrieben werden.

Bildquellen konfigurieren

Alle Bildquellen (Netzwerkkameras, digitale Videorecorder und Video-Interfaces), die Alarmdaten an den FTP-Server senden sollen, müssen dafür geeignet konfiguriert werden. Dazu sind mindestens folgende Einstellungen nötig:

- Ein **Name** für die FTP-Verbindung, den man meist frei wählen kann und anhand dessen der FTP-Upload in der Event-Konfiguration der Bildquelle mit verschiedenen Ereignissen (beispielsweise Bewegungserkennung, Kamerakontakt, Störungsmeldungen) verknüpft werden kann.
- Die **IP-Adresse**, unter der der FTP-Server erreicht werden kann. Sofern die Bildquelle das Domain Name System (DNS, [8]) unterstützt, kann hier auch ein DNS-Name eingetragen werden.
- **Benutzername** und **Passwort** für die Anmeldung beim FTP-Server. Bei geeigneter Konfiguration des FTP-Servers ist mit den Anmeldedaten bereits das passende Unterverzeichnis des FTP-Servers voreingestellt, in das diese Bildquelle ihre Daten schreiben kann.
- Falls dies nicht der Fall sein sollte, muss zusätzlich der **FTP-Dateipfad** eingegeben werden, unter dem die Alarmdaten abgelegt werden sollen, damit die Leitstelle sie korrekt zuordnen kann.

Bei Eingabe des FTP-Dateipfads ist zu beachten, dass dieser anderen Formatregeln unterliegt als beispielsweise ein Dateipfad unter Windows. Die genauen Formatregeln sind abhängig vom eingesetzten FTP-Server. Grundsätzliche Regeln:

- Keine Umlaute oder Leerzeichen verwenden
- Auf korrekte Groß- und Kleinschreibung achten
- Zur Trennung der Verzeichnisebenen den normalen Schrägstrich / an Stelle des so genannten Backslashs \ einsetzen

Außerdem bezieht sich der FTP-Dateipfad immer relativ auf den Pfad, der im FTP-Server für die verwendeten Anmeldedaten konfiguriert wurde, beispielsweise das Wurzelverzeichnis des FTP-Servers, das oft „ftproot“ genannt wird. Das FTP-Verzeichnis

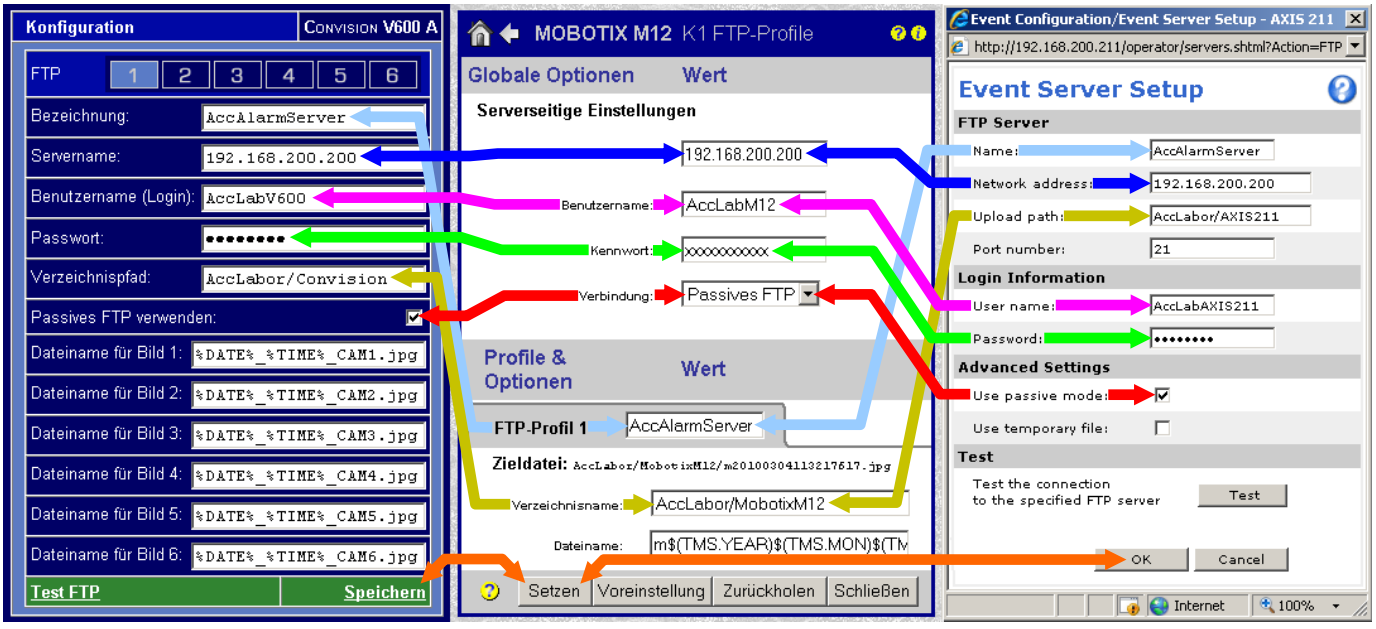
```
/AccLabor/MobotixM12/
```

kann somit beispielsweise dem Windows-Verzeichnis

```
C:\ftproot\AccLabor\MobotixM12\
```

entsprechen. Darauf ist zu achten, wenn auf einem Server unter Windows eine Datei wiedergefunden werden soll, die mittels FTP gespeichert wurde.

Bei manchen Bildquellen kann zwischen **Active-** und **Passive-Mode** umgeschaltet werden. Beim Passive-Mode baut die Bildquelle sowohl die Steuerungs- als auch die Datenverbindung zum FTP-Server auf. Das hat den Vorteil, dass die Bildquelle hinter einer Firewall betrieben werden kann, die keine eingehenden Verbindungen zulässt und damit besonders einfach und sicher zu konfigurieren ist; nur auf Leitstellenseite,



Die FTP-Konfiguration verschiedener Bildquellen sieht auf den ersten Blick sehr unterschiedlich aus. Die Pfeile zeigen aber, wo die entsprechenden Einstellungen wiederzufinden sind. Zur besseren Übersicht wurden die Dialogfenster teilweise gekürzt.

wo der FTP-Server in einer DMZ betrieben wird, müssen die benötigten Ports freigeschaltet sein: Port 21 für die Steuerverbindung und ein im FTP-Server konfigurierbarer Portbereich für die Datenverbindung.

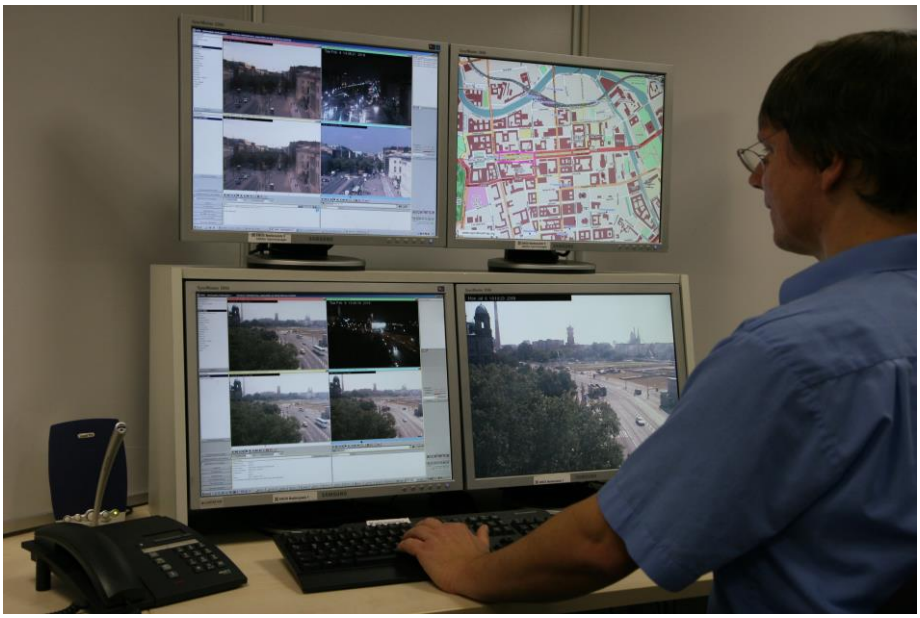
Diese Lösung ist auch unter dem Aspekt **Datenschutz** interessant: Eine Einwahl der Leitstelle in die Bildquelle ist grundsätzlich nicht möglich, da durch die Firewall gesperrt. Nur genau dann, wenn im zu schützenden Objekt ein dort vor Ort definiertes und in der Bildquelle konfiguriertes Ereignis eintritt (beispielsweise Druck auf einen Überfalltaster), werden Bilder von der Bildquelle zur Leitstelle übertragen.

Die Datenübertragung zum FTP-Server sollte auf jeden Fall im **Binärmodus** erfolgen. Im Textmodus, der auf manchen Servern voreingestellt ist, werden eventuell zusätzliche Steuerzeichen eingefügt, durch die Videodaten gestört werden. Die Bildquelle sollte daher zu Beginn jeder FTP-Sitzung das Kommando BINARY senden.

Üblicherweise wird **TCP/IP-Port** 21 benutzt, um eine Verbindung zum FTP-Dienst herzustellen. Diese Einstellung braucht – falls vorhanden – in der Regel nicht geändert zu werden.

Bei manchen Bildquellen können – teils unter Verwendung von variablen Namensbestandteilen – auch **Dateinamen** vorgegeben werden, unter denen die Alarmdaten auf dem FTP-Server gespeichert werden. Von Vorteil ist es, wenn der Dateiname Datum und Uhrzeit und gegebenenfalls auch die Kameranummer enthält, damit die Bilder bei einer späteren Auswertung korrekt zugeordnet werden können.

Zum Abschluss der Konfiguration sollte die Datenübertragung zum FTP-Server geprüft werden: Viele Bildquellen bieten im Konfigurationsdialog eine Schaltfläche zum **Test der Verbindung** zum FTP-Server. Mit einem Klick darauf, durch Bewegung vor der Kamera oder Betätigen des Kamerakontaktes sollte ein Testalarm ausgelöst werden. In der Logbuch-Anzeige des FTP-Servers kann dann verfolgt werden, ob die Daten ankommen. Das Logbuch weist auch auf eventuelle Konfigurationsfehler hin, beispielsweise wenn der Anruf einer Bildquelle wegen ungültiger Anmeldedaten oder Auswahl eines nicht vorhandenen Dateipfades zurückgewiesen wurde. Es sollte geprüft werden, ob die Daten ausreichend schnell, fehlerfrei und vollständig auf dem FTP-Server ankommen.



Video-Arbeitsplatz der Firma Accellence mit FTP-Alarmbildempfang

Zuverlässigkeit erhöhen

Wie jedes System so kann auch ein FTP-Server wegen technischer Störungen oder Fehlbedienung ausfallen. Wenn hohe Anforderungen an die Zuverlässigkeit des Systems bestehen, müssen daher zusätzliche Vorkehrungen getroffen werden. Eine gute Möglichkeit dazu bietet ein Test-Alarm-Generator: Er sendet von dort, wo auch die Bildquellen aufgestellt sind, in regelmäßigen Abständen (beispielsweise jede Minute) einen Testalarm, der von den Video-arbeitsplätzen „still“ angenommen wird, also ohne den Anwender zu stören. Lediglich eine kleine grüne Statusanzeige weist darauf hin, dass die Alarm-empfangseinrichtung geprüft wurde und intakt ist. Wenn dieser Testalarm für mehr als zwei Minuten ausbleiben sollte, schlägt der Video-Arbeitsplatz Alarm. Da jeder Video-Arbeitsplatz für sich autark arbeitet und diese Überwachung unabhängig von den anderen Arbeitsplätzen erfolgt, ist eine n-fache Redundanz der Überwachung gegeben mit n als Anzahl der Video-Arbeitsplätze.

Mit den Testalarmen wird nicht nur der FTP-Server, sondern die gesamte Alarm-Empfangsstrecke überwacht. Es werden also auch Ausfälle der Übertragungstechnik, Fehler in der Firewall-Konfiguration und Störungen im Alarm-Server erkannt und gemeldet. Damit kann auf eventuelle Ausfälle schnell reagiert werden.

Eine weitere – allerdings wesentlich kostspieligere – Maßnahme zur Steigerung der Zuverlässigkeit des Alarmempfangs ist eine redundante Auslegung zentraler Komponenten bis hin zu einer kompletten zweiten Alarm-Empfangsstelle an einem anderen Standort. Damit ist die Leitstelle dann sogar für Großereignisse wie beispielsweise die Räumung ihres Gebäudes aufgrund einer Bombendrohung gewappnet. Voraussetzung dafür ist, dass die Bildquellen in der Lage sind, ihre Alarmdaten automatisch auch auf einem alternativen Übertragungsweg (beispielsweise UMTS) an einen anderen FTP-Server zu versenden.

Fazit

FTP-Upload ist ein einfaches und kostengünstiges Verfahren zur hersteller-übergreifenden Alarmbildübertragung, das bereits von vielen Herstellern unterstützt wird und sich in der Praxis bewährt hat. Zusammen mit der passenden Video-Management-Software steht eine universelle und flexible Gesamtlösung für den Empfang von Alarmbildern und Meldungen von Videosystemen verschiedenster Hersteller zur Verfügung.

→ https://www.ebues.de/KB/000010

Quellen / Literaturhinweise

[1] http://de.wikipedia.org/wiki/File_Transfer_Protocol
[2] http://tools.ietf.org/html/rfc959
[3] http://de.wikipedia.org/wiki/JFIF
[4] http://de.wikipedia.org/wiki/ASCII
[5] http://de.wikipedia.org/wiki/Virtual_Private_Network
[6] https://www.bsi.bund.de/cln_156/DE/Themen/ITGrundschutz/itgrundschutz_node.html
[7] http://de.wikipedia.org/wiki/Demilitarized_Zone
[8] http://de.wikipedia.org/wiki/Domain_Name_System