

7. Türkommunikation im Netzwerk

Inhalt

1	Begriffsbestimmung	1
2	Anforderungen	1
3	Leistungsumfang	2
4	Sicherheit an der Tür	4
5	Video.....	5

1 Begriffsbestimmung

Türkommunikation ist für uns eine wichtige Unterabteilung unseres Arbeitsgebiets Netzwerk-Audio. An der Tür steht man besonderen Aufgaben gegenüber, die zwar der normalen Netzwerktelefonie ähneln, aber doch eine eigene Qualität aufweisen.

Unsere Betrachtungen beschäftigen sich nicht mit der notwendigen Gehäusetechnik und Produktmechanik. Das sind schon eigene Wissenschaften, die sich außerhalb unseres Einflussbereiches befinden. Wir konzentrieren uns auf die elektronischen und programmtechnischen Lösungen der Problematik.

Wir haben in der Vergangenheit bereits Erfahrungen mit der Türkommunikation gesammelt. Teilweise ging es da noch um analoge und ISDN-Technik, seit einigen Jahren beschäftigen wir uns aber nur noch mit Netzwerklösungen.

Zur Türkommunikation gehört bei uns nicht nur die „einfache“ Haustür, auch Zutrittskontrollen, Pförtnersteuerungen und Anlagen mit bis zu mehreren hundert Teilnehmern, sowie Integration in bestehende Telefonanlagen, Fernkontrolle über Internet und/oder Mobilfunk befinden sich in unserem Fokus.

2 Anforderungen

Für die Kompatibilität zu Fremdgeräten (wenn das verlangt wird), ist es notwendig gängige Standards zu unterstützen. Im Bereich der Netzwerkkommunikation ist hier in erster Linie die Sprache von SIP, was alle unsere Geräte von hause aus unterstützen. Auch IAX2, H.323 und die bei uns übliche neuronale Kommunikation werden unterstützt.

Gerade im Zusammenhang mit der Türkommunikation ist die Neuronalität von großem Vorteil, denn es wird auf die Existenz von Zentralen völlig verzichtet. Streaming, Durchsagen und priorisierte Gruppenkommunikation werden auf diese Weise ermöglicht.

Die Telefonie ist ein oft gewünschtes Leistungsmerkmal einer Türsprechstelle. Der Gedanke dabei ist, dass man per Telefon mit allen Leistungsmerkmalen (Voicebox, Weiterleitung usw.) versorgt ist und die Türsprechstelle integriert. Das ist auch grundsätzlich möglich, egal ob man hier mit VoIP (SIP, IAX2, H.323, neuronal) arbeitet oder über Gateway mit den anderen Techniken (analog, ISDN, GSM, LTE, G5). Man darf aber die Nachteile nicht übersehen. Die übliche Telefonsignalisierung (Ruf- und Besetztzeichen) zeigen der Person vor der Tür schnell und eindeutig, ob jemand im Haus ist oder

nicht. Eine Telefonie-Integration muss also über den Standard hinaus auch verschleiern können, auf welchem Weg die Verbindung aufgebaut wird.

Türkommunikation per IP meint üblicherweise, dass eine Verkabelung per Ethernet vorgesehen ist. Die gesamte Technik gründet sich auf einer zumeist schon bestehenden LAN-Infrastruktur. In manchen Umgebungen ist eine Verlegung von Netzkabeln nicht sinnvoll. Z.B. auch wegen größerer Entfernungen oder weil man alte Kabel verwenden will, wird Ethernet als nicht hilfreich empfunden.

Als Alternative zum Ethernet-Standard bieten wir auch andere Wege an, die gemischt integriert werden können. Da wäre zunächst WLAN, das auch in den meisten Umgebungen bereits vorhanden ist. Man muss sich dabei nur sicher sein, dass die Betriebssicherheit zu jeder Zeit gewährleistet ist.

Als klassische Alternative empfehlen wir ISDN UPO, das auf gewöhnlichen zweiadrigen Telefonkabeln Reichweiten von 4km erreicht und auch die Stromversorgung sicherstellt. Der eigentliche Nachteil dieser Technik besteht darin, dass man so nur eine (maximal zwei) Sprechstelle pro Kabelpaar anbinden kann. Eine Netzwerkverlängerung und Videoübertragung sind damit nicht möglich.

Ein völlig neues Verfahren bietet der Standard 802.3cg. Hier wird über ein verdrehtes Drahtpaar eine Geschwindigkeit von 10Mbps auf bis zu 1.000m erreicht. Auch diese Technik wird von uns unterstützt. Die Bauteile dafür sind aber voraussichtlich erst gegen Ende 2018 verfügbar.

Zum Thema Sicherheit an der Tür gibt es weiter unten ein separates Kapitel.

Bei der Entwicklung von Komponenten zur Türkommunikation beachten wir auch alle physischen Anforderungen unserer Kunden. Baugröße, Temperaturbereich, technische Prüfungen, Gehäuseanpassungen und der Systemgedanke sind beispielsweise Dauerthemen unserer Arbeit.

3 Leistungsumfang

Den Leistungsumfang eines Systems definiert grundsätzlich unser Kunde, also der Partner, der den Markt und seine Anforderungen bestens kennt. Trotzdem können wir hier einige Beispiele anführen, um zu zeigen, auf welche Erfahrungen zurückgegriffen werden kann.

Eine Türsprechstelle ist in unserem neuronalen Konzept keine zentrale Einheit. Das bedeutet, dass innerhalb eines Systems beliebig viele Türsprechstellen (z.B. Eingänge) geben darf. Im Innenbereich können einfache Wohnungsstationen, ebenfalls in beliebiger Menge, betrieben werden. Anstatt einer Wohnungsstation kann auch ein Gateway (auch mehrere) zu einer bereits bestehenden Technik genutzt werden. Das wären z.B. analoge oder ISDN-Telefonanlagen, aber auch Datenzugänge zu PCs, Tablets oder Mobiltelefonen. Ein Zugang zu einer SIP-Telefonanlage benötigt kein Gateway. Die Türsprechstelle kann eine entsprechende Anmeldung am Server selbst vornehmen.

Die Besonderheit, dass unser System keinen Server benötigt, nennen wir Neuronalität. Alle Komponenten kommunizieren direkt untereinander und realisieren das System mit verteilter Intelligenz. Die gibt uns auch die Möglichkeit umfangreicher Gruppenbildungen z.B. für Durchsagen in verschiedenste Teilnehmergruppen, auch mit Priorisierungen.

Jedes Gerät hat für sich einen eigenen Webserver, über dessen Webseiten die Konfiguration mit einem beliebigen Browser vorgenommen werden kann. So kann jeder Teilnehmer nur sein Gerät konfigurieren, nicht das der anderen. Darüber hinaus gibt es auch die Möglichkeit das System im Ganzen zu konfigurieren, indem man Parameterfiles im Netz verteilt. Das ist etwas anspruchsvoller,

dafür aber deutlich schneller und gibt dem Installateur die Möglichkeit, das gesamte System zentral zu administrieren. Der Betrieb bleibt weiterhin neuronal.

Immer mehr wird von der Kundenseite her, die Integration in mobile Techniken verlangt. Ein ohnehin netzwerkgestütztes Kommunikationssystem bietet hier den Zugriff von hause aus. Die Signalisierung und die Sprache (auch Video) wird mit gängigen Methoden übertragen. Ein Zugang über LAN (natürlich auch über WLAN) ist deshalb ziemlich einfach zu realisieren (auch direkt im Gerät ohne separaten Access Point). Sicherheitsaspekte sollten dabei beachtet werden, denn die Betriebssysteme der mobilen Geräte und PCs sind unsichere Kandidaten, im Gegensatz zum eLLan:RTOS in unserem System. Mehr über dieses Betriebssystem gibt es im nächsten Newsletter zu lesen.

SIP als gängiger Standard wird zwar oft gefordert, kann aber allein nicht alle Anforderungen erfüllen. Gerade bei der Türkommunikation wird Echtzeitbetrieb gefordert. Jede Reaktion (Klingeln, Öffnen usw.) wird ohne Verzögerung erwartet. Dies ist eine besondere Spezialität unseres Betriebssystems, auch auf kleinen und günstigen Microcontrollerbaugruppen.

DTMF (Tonsignalisierung) stellt eine allgemein verfügbare Methode der Steuerung während einer bestehenden Verbindung dar. Das Drücken einer Zifferntaste kann eine Tür öffnen, Licht schalten, Weiterleiten usw. Für die Decodierung des Tons benötigt man entweder eine spezielle Hardware oder eine DSP-Funktionalität (in unserem System enthalten). DTMF integriert Fremdgeräte (z.B. jedes beliebige Telefon) für einfache Steuerungen. Innerhalb des Systems gibt's es bessere und vor allem sicherere Verfahren.

Um ein Türkommunikationssystem an andere Gerätschaften anzubinden, benötigt man Gateways. Netzwerkitern kann das per Software erledigt werden (SIP, IAX2, H.323), wenn aber die Physik verlassen werden muss, braucht es einen intelligenten Adapter. Solche Gateways haben wir bereits erfolgreich entwickelt, z.B. für analoge Telefonie (auch mit Modem) und ISDN mit verschiedenen Interfaces (S0, Uk0, Up0, S2M, jeweils TE und NT).

Selbstverständlich, aber oft übersehen, ist eine ganz wichtige Funktion: das Freisprechen. Um Rückkopplungen zu unterdrücken wird oft Wechselsprechen eingesetzt. Das ist die mit Abstand sicherste Methode, denn hier wird entweder gesprochen oder gehört. Ähnlich sicher ist der Betrieb mit Hörern (Telefonen). Hier ist der negative akustische Effekt dadurch ausgeschlossen, dass die Rückwirkung durch die geringe Lautstärke verhindert wird.

Ein echter Freisprecher ermöglicht Sprechen und Hören gleichzeitig. Dazu muss der Schall aus dem Lautsprecher, der ins Mikrofon gelangt, herausgerechnet werden. Das ist sehr komplex, weil der Schall auf seinem Weg Änderungen unterliegt (Hall, Gehäuse- und Lautsprechereigenschaften). Auch dieses Problem wird durch DSP-Algorithmen gelöst.

Auch für die Unterdrückung von Hintergrundgeräuschen gibt es gerechnete Lösungen, die aber auch Anforderungen an die mechanische Ausführung der Türsprechstelle stellen.

Ein Türkommunikationssystem besteht in erster Linie aus den Tür- und Wohnungssprechstellen. Heutzutage ist das aber längst nicht mehr alles. Die Möglichkeit von Steuerungen kennt man ebenfalls seit langem, schon allein durch den Türöffner. In modernen Umgebungen integriert man aber auch noch andere Schaltvorgänge. Licht ist hier das gängigste Beispiel. Da das eLLan:RTOS aber mehr als nur ein Türkommunikationssystem ist, können z.B. auch optische und akustische Signalgeräte oder IP-Verstärker eingebunden werden, die Beschallung und Durchsagen, gesteuert aus einer Hand bieten.

Und auch der umgekehrte Weg digitaler Signalisierung ist von Interesse. Die Integration von Sensoren kann im System Reaktionen auslösen. Bewegungen, Tür geöffnet/geschlossen, Helligkeit, Erschütterungen und Neigung können passende Aktivitäten oder auch Alarme auslösen. Zentrales Management mit Überwachungen an mehreren Stationen ist möglich. Dieser Leistungsumfang verlässt dann schon das Feld der typischen Anforderungen an ein Türkommunikationssystem, aber da sich ein solches ja in 99% aller Fälle in jedem Gebäude befindet, ist eine entsprechende Erweiterung deutlich sinnvoller, als die Installation zusätzlicher Systeme.

4 Sicherheit an der Tür

Mit Einführung der Netzwerktechnik an der Tür ist der Aspekt der Sicherheit weiter in den Vordergrund gerückt. Immerhin endet das Netzwerk direkt an der Tür und ist von außen mit wenig Gewalt leicht erreichbar. Man muss sich also etwas einfallen lassen, um den unberechtigten Zugriff von außen zu verhindern. Das Betriebssystem ellan:RTOS bietet alle notwendigen Sicherheitsmechanismen und vieles darüber hinaus. Das System selbst kann so abgesichert werden, dass ein externer Zugriff ohne die entsprechenden Zugangsdaten schlicht unmöglich ist.

Aber ein abgesichertes Türkommunikationssystem allein genügt noch nicht. Es bleibt das Risiko des allgemeinen Netzwerkzugriffs über die Türkommunikation hinaus. Auch hier haben wir das notwendige zu bieten. Unser Sicherheitskoppler Elink751 blockiert externe Zugriffe sehr radikal durch physische Trennung vom Netz. Dazu wird der Datenverkehr und die Stromversorgung zur Türsprechstelle überwacht. Es ist ja bekannt, welche Art von Daten von dort kommen können. Passiert irgendetwas ungewöhnliches, trennt der Sicherheitskoppler die Verbindung und alarmiert entsprechend.

Elink751 eignet sich nicht nur für die Türkommunikation, sondern kann auch andere Einheiten, die sich im öffentlichen Zugriff befinden, schützen. Verschiedenste Bauformen sind möglich, als Einzelgerät wie auch für die Rackmontage in Gruppen. Elink751 wird im Laufe des Jahres 2018 in Produktion gehen.

Der Kern aller Sicherheitslösungen liegt in der Authentifizierung und Verschlüsselung. Dazu muss man wissen, dass sehr viele verschiedene Algorithmen dafür eingesetzt werden. Diese unterscheiden sich auch in ihrer Qualität. Man sieht nicht so leicht, wie gut ein verwendetes Verschlüsselungsverfahren ist. Geräte wie PCs, Tablets oder Mobiltelefone müssen aus Kompatibilitätsgründen alle Verfahren unterstützen. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) aber legt fest, dass die schlechten Verfahren nicht unterstützt werden dürfen (aus naheliegenden Gründen).

Unser Betriebssystem beherrscht alle populären Verfahren, wir setzen aber tatsächlich nur die vom BSI empfohlenen ein. Wir haben trotz dieser „Einschränkung“ keine Probleme mit der Kompatibilität, denn tatsächlich müssen die Geräte unseres Systems ja nur untereinander kompatibel sein. Das versetzt uns zusätzlich auch noch in die Lage, eigene Verfahren einzuführen, die noch sicherer sind, allein aus der Tatsache heraus, dass sie unbekannt sind.

Und dann gibt es auch noch das Problem mit dem Softwareschutz in der Hardware. Hier geht es darum, die Daten zu schützen, die sich z.B. in einer Türstation befinden, die ja recht einfach gestohlen werden kann. Dazu gilt es auch noch zu beachten, dass ein potentieller Dieb auch über die notwendige Expertise verfügen kann, die man für die Administration der Türkommunikationsanlage braucht. Deshalb kennen unsere Systeme die Möglichkeit, ihre Daten unsichtbar zu machen. Die

Geräte funktionieren noch, aber Konfigurieren ist nur noch möglich, wenn man das Gerät vorher komplett löscht, was kein Problem ist, wenn man die alten Daten noch hat. Der Dieb hat jedenfalls keinen Zugriff auf die Daten.

Faszinierend an einem netzwerkorientierten System, das externe Geräte über WLAN oder auch Mobilfunk anbindet, sind neben der Umleitung auf dieses Device auch die Eingriffsmöglichkeiten ins System. Auch WLAN funktioniert sehr wohl vor der Tür. Da ist die erste Anwendung, die einem Kunden einfällt: Das Öffnen der Tür mit dem Handy. Das geht natürlich problemlos, ist aber sicherheitstechnisch sehr anspruchsvoll.

Man kann sogar die Tür öffnen, wenn sich das mobile Device ins Netz einbucht, ohne dass man dafür eine besondere Aktivität braucht. Das lässt sich ebenso auch mit Bluetooth realisieren. Es bleibt aber das Risiko mit dem berühmten gestohlenen Handy. Eine Bestätigung in einfachster Form bleibt empfehlenswert (Fingerabdruck, Codeeingabe). Wichtig ist, dass die Authentifizierung direkt mit dem Gerät in der Tür stattfindet und nicht abhängig von einer Verbindung zu einem zusätzlichen Server abhängt. Außerdem ist es wichtig, dass zum Öffnen der Tür nicht immer der gleiche (wenn auch verschlüsselte) Code verwendet wird. Er könnte abgehört und mitgeschnitten werden. Jede Aktivität muss mit einem neu ausgehandelten Schlüssel einhergehen, sonst sieht es schlecht aus mit der Sicherheit.

5 Video

Für die Übertragung von Videosignalen gilt im Prinzip dasselbe wie für Audio. Die benötigte höhere Bandbreite stellt in modernen Netzen kein Problem mehr dar. Interessant sind die Möglichkeiten für den Anschluss. Unser System kann von hause aus mit Ethernet-Kameras umgehen, entweder über ein zusätzliches Ethernet-Port oder über das Netzwerk mittels Steuerpaketen und Umleitung.

Außerdem verfügen unsere Systeme größtenteils über USB-Anschlüsse und können die Signale preiswerter USB-Kameras über das Netzwerk leiten. Das Videosignal wird dabei nicht beeinflusst, sondern lediglich an einen geeigneten Empfänger weitergeleitet.

Andererseits verfügen unsere Systeme auch meistens über einen Anschluss für passende Displays, so dass Video auch direkt wiedergegeben werden kann, ohne dafür hochperformante Systeme notwendig zu machen. Dabei gibt es allerdings Einschränkungen bei den verwendbaren Codecs. Ein geeignetes Display kann neben der Videowiedergabe auch für die Anzeige aller anderen Informationen, Bilder oder Menüs verwendet werden.

Der Einsatz von alten analogen Kamerasystemen ist unter erhöhtem Aufwand ebenfalls möglich, aber bei Neuentwicklungen eher nicht empfehlenswert.

PC-Systeme sind im Prinzip in der Lage jeden Videocodec wiederzugeben. In der Anwendung ist es deshalb nicht wichtig, mit welchem gearbeitet wird, es sei dann man will Breitwandspielfilme übertragen. In einem preiswürdigen System ist es wichtiger, die erwartete Qualität mit geringstmöglicher Hardware zu realisieren und dabei alle Sicherheitsaspekte zu berücksichtigen.

Das im Bild übertragene Audio ist bei uns HDAudio (G.722) oder G.711 aus Kompatibilitätsgründen. Beide nutzen die gleiche Datenbandbreite. Noch höhere Audioqualitäten sind ohne weiteres möglich (HDAudio eignet sich schon für Musik), machen aber nur Sinn in hochqualitativen Beschallungsanwendungen.