Årskrönika 2011

Axplock från en trådlös bransch

Induos ABs årskrönika om trådlöst är ett urval artiklar, debattartiklar och andra inlägg som vi arbetat med under 2011. Varsågod att publicera innehållet men ange oss gärna som källa.

Dags för en digital agenda för industrin?

Det är av intresse för oss alla att den svenska industrin skall utvecklas och behålla sin ställning i framtiden. En konkurrenskraftig industri, motståndskraftig mot det ökade trycket från låglöneländer, förutsätter en industri med hög automationsgrad. Och i sin tur kräver hög automatisering en bra infrastruktur för kommunikation.

Tillgången till en bra kommunikationsinfrastruktur är och kommer att vara en viktig faktor i den framtida ekonomin. I Sverige och EU har det under året arbetats fram Digitala Agendor, planer för hur den infrastrukturen skall utvecklas fram till 2020. I Sveriges arbete har småföretagens och industrins utveckling nämnts som viktiga, ett av de långsiktiga målen sägs vara att automatisera fler av de tunga jobben inom den svenska industrin. Senast år 2020 skall 90 % av alla företag erbjudas 100 Mbit/s i bredbandshastighet, dessutom ”ska det gå att koppla upp sig när som helst och var som helst”.

Med en bra kommunikationsinfrastruktur kan produktionen automatiseras i högre grad. Som en effekt av ökad automation med krav på ökad produktivitet och miljöhänsyn kommer fjärrservice av maskiner att bli en allt viktigare faktor. Utvecklingen går ju som bekant framåt, därför är det troligt att fjärrservice kommer att innefatta allt mer avancerade realtidsmätningar och överföring av rörlig bild, tjänster som kräver nät med kapacitet och tillgänglighet. Idag sköts fjärr-

service i stor utsträckning via mobilt bredband, en viss del av trafiken flyttar säkert över till fast uppkoppling, men den del som fortsatt kommer förlita sig till mobilnäten kommer att ställa höga krav på tillgängligheten i näten och att dessa byggs med tilltagen kapacitet för mobilt bredband. I år har en stor omläggning av mobilnäten effektiviserat tillgången på frekvenser och under 2013 kommer fler frekvensband att tas i drift vilket ger ytterligare kapacitet. På EU-nivå sker på svenskt initiativ ett arbete inom med att se över om det går att frigöra ytterligare frekvensområden för att klara av framtida kapacitetsbehov, målet är ytterligare 1 200 MHz utrymme för datatrafik.

Inom en nära framtid kommer den administrativa sidans behov av informationsutbyte med den producerande att öka. Vattentäta skott mellan administrationssystem och produktionssystem kommer i förlängningen inte att vara möjliga. Men medan den administrativa sidan kan leva med kortare avbrott när en dator i bakgrunden analyserar om datapaketen som skickas är virus eller inte så kan vi inte tillåta att maskinen låter nödstoppet dröja en halv sekund extra medan antivirusprogrammet jobbar. Den dag de administrativa systemen och fabriken på allvar är en enhet så måste det som tillhör automationssystemen ha samma reaktionstider och säkerhet som idag. Utgångslägena att lösa kommunikationen i dessa system har varit olika, produktionen har haft en infallsvinkel och ad ministrationen en annan. I framtiden behöver vi en gemensam utgångspunkt. Kanske det är dags att för en egen Digital Agenda för industrin?

Denna artikel har även publicerats som debattartikel i tidningen Automation.

Frekvensbristen i EU snedvrider marknaden

I EU pågår ett arbete att fria upp fler frekvenser för mobilt bredband, initierat av bland annat den svenska EU-parlamentarikern Gunnar Hökmark. I Sverige har vi nyligen tagit del av den Digitala Agendan för Sverige. I bägge dessa initiativ finns en omfattande plan för att frigöra frekvenser för mobiloperatörer, däremot saknas det drivkrafter för att utöka de fria frekvensbanden som behövs för att bygga trådlösa nätverk utan licens.

Frekvensauktionerna för mobilt bredband drar in stora summor till stadskassan samtidigt som det är en betydande kostnad för operatören. Genom nya tekniker som just nu utvecklas kommer det att vara möjligt att använda vanliga trådlösa nätverk för att avlasta mobilt bredband. Dessa frekvenser är licensfria och mobilbranschen ser en möjlighet att lastbalansera de överhettade mobilnäten genom att använda trådlösa nätverk som infrastruktur. I köpcentrum, på hotell och restauranger med trådlösa nätverk kommer därmed kunder att kunna använda de trådlösa nätverken utan inloggning, det är själva grundtanken.

Denna lastbalansering är nödvändig, men vad kommer å andra sidan att hända när de fria frekvenserna blir allt mer nedlastade av mer trafik? Vilka frekvensband skall användas då?

”Trådlösa nätverk kommer avlasta mobilt bredband”

Redan i dag märker vi av att frekvensbandet 2,4 GHz är överlastat med wifi-nätverk, bluetooth och allehanda trådlösa anläggningar, i flerbostadshus är ofta problemen påtagliga med sämre överföringshastigheter som följd något som går stick i stäv med ambitionen i den Digitala Agendan.

Som frekvenspolitiken bedrivs för närvarande öppnas inte marknaden för mindre aktörer. Med tillräcklig tillgång på fria frekvenser kan även mindre operatörer erbjuda trådlöst bredband på begränsade geografiska ytor. I vissa delstater i USA står sådana mindre aktörer för 30-40% av bredbandsmarknaden, i Sverige ställer vi vår tilltro till att mobiloperatörerna bygger ut 4G täckningen. Om vi öppnar marknaden för mindre aktörer kommer trådlösa länkar på fria frekvensband kunna nå avlägsna abonnenter kostnadseffektivt. Trådlösa nätverk på fria frekvenser kan enkelt och effektivt täcka mindre byar och orter och erbjuda en bra kapacitet för Sveriges landsortsbor.

Genom ett målmedvetet arbete att hitta nya fria frekvensband för trådlösa nätverk kommer vi att uppnå en bättre balans i den trådlösa datatrafiken i framtiden. Detta behövs delvis också för att kunna nå målen i den Digitala Agendan för Sverige. Trådlösa nätverk behövs i våra hem, och de behövs för att vi som land skall uppnå en balanserad trådlösa datakommunikation.

Denna artikel har även publicerats som debattartikel på teknikdebatt.se

Trådlös standard för smarta hem behövs

Utvecklingen går mot smarta hem, med stegrande elpriser och en utbredd önskan att leva miljövänligt blir det allt intressantare att spara energi. I smarta hus kan vi reglera värmen så att byggnaden är varm då det behövs och under övrig tid kan vi spara energi. Det som saknas inom smarta hem är en enhetlig standard för kommunikation med termostater och givare.

Inom trådbaserade system sker harmonisering och branschanpassning till ett fåtal standarder, inom trådlöst har inte utvecklingen kommit lika långt, eller har den? Det normala sättet att bygga trådlösa smarta hus om man vill installera ett trådlöst system med sensorer, larmpunkter samt styrning av funktioner är att först installera en gateway och sedan hårdvara som kan kommunicera med denna gateway. Kanske skulle det vara lättare om vi hade en annan infallsvinkel för de flesta har redan en fungerande gateway hemma i form av ett vanligt trådlöst nätverk. De flesta har redan gjort den första räckviddskontrollen och optimerat antennplaceringen och täckningen för den plats där det trådlösa nätverket är monterat.

Vi kanske skulle kasta ut larmcentralen och ersätta den med en servermjukvara som kan hantera larmer, slå av och på belysningen och övervaka allt från temperatur till om

”Vi kan i praktiken surfa rätt in i luftvärmepumpen”

diskmaskinen läcker? Om vi väljer en trådlös kommunikation baserad på WLAN så får vi automatiskt en bra kryptering, en väletablerad standard, vi får ett IP baserat system och vi kan i praktiken surfa rätt in i luftvärmepumpen för att se att allt står rätt till.

Batteridrift av sensorer är efterfrågat och WLAN är traditionellt en batterislukande teknik. Men företag som RFM har utvecklat radiolösningar för sensorer som klarar drift på batterier i åtskilliga år utan att behöva byte. Allt beror naturligtvis på hur ofta noden i fråga behöver sända eller lyssna. Och om man tänker det omvända, hur många sensorer behöver egentligen batteridrift? Allt som är associerat med övervakning och styrning av el har ju en naturlig väg att strömförsörjas. Brandvarnare och liknande, ja där har ju användarna vanan att byta batteri med jämna intervaller.

Fördelarna med WLAN är att det är en väletablerad teknik, de flesta har infrastrukturen och det finns naturliga vägar att logga in i sitt nät och sina sensorer, både lokalt och utifrån. Tekniken bygger på IP, den är säker med kryptering och kretsarna är billiga. Dessutom är standarden öppen vilket främjar konkurrensen.

Trådlöst kan öka turismen

På våra turistorter finns idag inte fri wifi i så stor utsträckning men det finns uppenbara fördelar för kommuner och näringsidkare att investera i nätverk som täcker tillexempel en stadskärna.

Ett kostnadsfritt trådlöst nätverk ger utländska besökare möjlighet att surfa fritt utan att tänka på datakostnaden. Det stimulerar också möjligheten att få folk att checka in via sociala medier som Facebook och Foursquare vilket ökar kännedomen och spridningen om turistmålens namn och de aktiviteter som möter besökaren.

Den region som är ytterligare kreativ förser besökaren med en app för att hitta i närområdet, se intressanta besöksmål och ta del av historia. I förlängningen finns kan företagare annonsera i appen och kunder kan hitta restauranger, caféer eller butiker. Tack vare det fria trådlösa nätverket kan turismens och handelns omsättning i regionen ökas.

Just nu pågår också ett arbete för att använda trådlösa nätverk för avlastning av mobilnäten vilket skall ge snabbare uppkoppling av mobilt bredband. Genom att styra över trafik till trådlösa nätverk lastbalanseras mobilnäten och tillgängligheten ökar, vinst för alla med andra ord. Att bygga öppna trådlösa nät kan vara till gagn för många regioner, för handen på hjärtat, en stor del av oss vill kunna komma ut på internet på semestern.

Denna artikel har även publicerats som debattartikel på teknikdebatt.se

”Trådlösa nätverk kan vara en konkurrensfördel för en hel region”

Ett av hetaste teknikområdena: sensorer

Analysföretaget Gartner identifierar att Internet of Things, IoT, är en av de 10 hetaste teknikområdena under 2012. Vid ett symposium i Orlando, Florida, den 18 oktober i år definierade man sensorer som ett intressant delområde inom IoT som kommer ha stor inverkan på de flesta organisationer de kommande åren: ”Sensors that detect and communicate changes are being embedded, not just in mobile devices, but in an increasing number of places and objects.” Att dessa sensorer skall anslutas till Internet, eller det utökade Internet, The Internet of Things, är underförstått.

Kommunikation med sensorer

En viktig marknad i Sverige, som verkligen skulle kunna dra nytta av Internet of Things är fastighetsautomation. Man kan spara uppvärmningskostnader och miljö genom att effektivare övervaka och styra uppvärmning av lokaler och reglera fläktanläggningar. Att dra kabel till funktsensorer eller termostater i uthyrda lokaler eller bostäder är kostsamt och kräver ingrepp i lokalerna, vilket oavsett verksamhet i allmänhet är störande.

Som ett resultat växer efterfrågan på trådlösa givare för industri, handel, lokaler och även bostäder. Det som är det stora problemet är att de flesta givare bygger på standarder som Zigbee, Bluetooth och andra tillverkarspecifika standarder. Eftersom få har utbyggd infrastruktur för dessa standarder krävs en eller flera kostnadskrävande gateways

för att hantera trafiken. Detta är en hämmande faktor och här behöver det utkristalliseras en vettig trådlös standard, gärna en som kan användas till annat än att bara koppla ihop sensorer.

Trådlösa nätverk lösningen

Eftersom många hem och lokaler redan har trådlöst nätverk, wifi/ wlan, för att koppla samman allt från datorer och smart phones til musikanläggningar och TV apparater, vore det logiskt att ta tillvara på den infrastrukturen som redan finns för att öka spridningen av trådlösa sensorer. Med wlan får man låg kostnad för Gateway, man får en teknik som är tillgänglig, som baseras på IP kommunikation, med bra säkerhet och med höga tillverkningsvolymer vilket är attraktivt för att hålla ned givarnas kostnad. Fram till för något år sedan var wifi-lösningar energislukare och rent av olämpliga för denna typ av applikationer. Idag finns lösningar som med hjälp av två vanliga AA batterier leverera temperaturvärden två gånger per minut i två år innan batterierna måste bytas.

Att bygga trådlösa sensornät baserat på wlan är framtiden, det ger en infrastruktur som kan användas för fler ändamål än bara att överföra mätvärden. Det håller dessutom kostnaderna nere för nätet vilket möjliggör att fler investerar i tekniken vilket på sikt även ger miljövinster.

Denna artikel har även publicerats som debattartikel på teknikdebatt.se

Mobilen behöver avlastning

Att lastbalansera mobilnäten genom att använda wifi-nätverk och hotspots är en intressant utveckling och är högaktuellt just nu. Den nya standarden 802.11u som finns på ritbordet skall kunna hantera handover mellan wifi-nätverk utan inloggning. Dessutom testas möjligheten att utnyttja wifi-hotspots för avlastning av datatrafiken i 3G och 4G näten. Dessa så kallade Hotspots 2.0 kommer med all sannolikhet börja skeppas ut under första halvåret 2012.

Att ta fram en teknik för wifi-roaming är ett initiativ från bland annat Wi-Fi Alliance. De visar att vi redan är en bra bit på väg genom att i juni 2011 skriva en avsiktsförklaring att tillsammans med Wireless Broadband Alliance utveckla Hotspot 2.0 och tillsammans arbeta med standarder för wifi-roaming. Tester av tekniken görs redan nu och under första halvan av nästa år anser man att det skall gå att börja implementera tekniken i skarp drift.

Att göra wifi mobilt

Idag bygger wifi-näten på mobila klienter som kommunicerar med en fast basstation utan möjlighet att roama mellan basstationerna, flera initiativ har dock påvisat att det är möjligt att lösa roamingfrågan. För detta ändamål har man börjat skissa på standarden 802.11u där en viktig fråga är hur operatörerna skall kunna autentisera roamingen. 802.11u lovar alltså en mobilliknande wifi-upplevelse med grundtanken ”varför skall det inte kunna vara lika lätt att ansluta till ett wifinät som till mobilnätet?”.

Hotspot 2.0

Wireless Broadband Associations Next Generation Hotspot (NGH) program bygger på 802.11u och kallas även Hotspot 2.0. Där definieras kraven för såväl accesspunkter och hotspots som för 3G/4G operatörerna. Tekniken är avancerad och ställer så klart stora krav på såväl operatörer som tjänsteleverantörer att hantera sömlös roaming av trafiken mellan mobilnät och wifi-nät och för den delen även roaming av trafik mellan wifi-nät. Lyckas man är det ett intressant steg på vägen för att avlasta de trafikerade mobilnäten.

Undersökningsföretaget In-Stat har kartlagt antalet hotspots och den framtida utvecklingen. Man anser att antalet wifi-hotspots förväntas tredubblas till 2015 med 120 miljarder anslutningar. Genom denna massiva utveckling kan infrastrukturen för mobilnäten snabbt förstärkas och lastbalanseras genom att dra nytta av hotspots.

”Antalet hotspots kommer att uppgå till 120 miljarder om tre år”

Säkerhet i M2M och WSN nät

Säkerhet i trådlösa nät har varit i hetluften under hösten (2010). SVTs Uppdrag Granskning hade ett inslag under hösten om säkerhet i trådlösa hemmanätverk, ett inslag som lyfte fram en sanning vi redan kände till, WEP-kryptering är inte ett säkert sätt att kryptera data. SVD publicerade under december en artikel med titeln ”mer trådlöst julafton för kriminella” som framförde kritik mot ”okritiskt användande” av trådlöst.

Så vad gäller när man vill skydda sin information på bästa sätt och hur går man tillväga för att bygga ett optimalt trådlöst nät? I vår bloggserie om säkerheten i de trådlösa näten kommer vi att fokusera på säkerhet i industriella trådlösa nät för M2M kommunikation. Vårt fokus ligger på kommunikation såväl via GSM/3G som i lokala nät med olika trådlösa standarder. Vi kommer att fördjupa oss i två typer av nät nämligen nät för M2M-kommunikation (Machine to Machine) samt WSN (Wireless Sensor Networks), trådlösa sensornätverk.

Hur skapar vi säkra lokala nätverk?

För den som planerar system för M2M kommunikation finns flera aspekter att ta hänsyn till än bara krypteringen. Att skapa en tillförlitlig radiomiljö i industrin kräver idag en del kartläggning och fundering innan man skrider till verket. De tre viktigaste sakerna att ta hänsyn till är störningar i luften,

risken för angrepp från utomstående och skillnader mellan trådlösa standarder för trådlösa nät. Inom industrin är de trådlösa sensornätverken på frammarsch, samtidigt finns många redan uppbyggda lokala M2M nät som skall samexistera med dessa nya nät på verkstadsgolven.

Störningar påverkar säkerheten

Lokala M2M nätverk och trådlösa sensornätverk bygger på trådlös överföring via radio som kommunicerar lokalt med andra enheter. I dessa lokala radionät finns en risk för störningar. Då M2M kommunikation ofta är beroende av hög tillgänglighet i överföringen, kan därför en störning vara en säkerhetsrisk.

Detta är något som Mats Björkman, professor i datakommunikation vid Mälardalens högskola, utreder ordentligt. Han leder två forskningsprojekt som skall möjliggöra säker och pålitlig automationskommunikation över trådlösa nät. Projekt Gauss tjänar till att se hur kommunikationen påverkas i elektromagnetiskt störda miljöer. Projekt Tesla, det andra projektet, syftar till att ta fram beräkningsmodeller för förutsättningarna för kommunikation i olika industriella miljöer. Genom att modellera karaktäristiken för den kanal som används för trådlös överföring (primärt 2,4 GHz-området) hoppas man kunna förutsäga kommunikationsprestanda som tillexempel förväntad bandbredd, fördröjning och risken för att ett paket inte tar sig fram.

”M2M kommunikation är ofta beroende av hög tillgänglighet”

Frekvensplanering för verkstadsgolvet

Trådlösa nätverk finns i många olika utföranden och standarder, men merparten av näten använder 2,4 GHz bandet. Dessa standarder använder frekvensspektrat på litet olika sätt, antingen används en frekvens för sändning och mottagning, alternativt väljer och vrakar nätverket bland de tillgängliga kanalerna för att hitta en ledig kanal att sända på.

Om man vill använda fasta frekvenser måste man redan innan installation göra en adekvat frekvensplanering. Under hela systemets installationstid måste man sedan följa upp att det inte tillkommer andra sändare inom nätverkets område. Alternativet är att välja en standard som använder frekvenshoppning. ”Sensornätverk som använder sig av frekvenshoppning är ganska bra på att motstå störningar, såväl från andra nätverk som rena elektromagnetiska störningar” berättar Mats Björkman, professor i datakommunikation vid Mälardalens högskola.

Men vad händer om man fyller radiospektrat med frekvenshoppande utrustningar, blir det inte återigen risk för kollisioner? Kan man styra detta på något sätt? När det gäller frekvenshoppning så finns det inte mycket man kan göra. Hoppen delas in i sekvenser och olika standarder använder olika hoppsekvenser, men det är inte givet att man som användare kan styra

vilken hoppsekvens som används. Om två närliggande förbindelser använder samma hoppsekvens kan det innebära problem om sekvenserna hamnar i synk med varandra, d.v.s. att samma frekvens används av båda sändarna samtidigt. Viktigt är återigen, kartläggning och analys innan installation. Med sin forskning hoppas Mats att de trådlösa nätverkens prestanda i industrin skall öka. Mats rekommenderar idag till eftertanke om säkerhetskraven är höga ”Även i en väldigt störd miljö brukar det gå att förr eller senare få fram ett meddelande, men då får tillämpningen inte ha alltför korta svarstidskrav.”

Säkerheten moment 22

M2M har ett moment 22 förhållande till säkerhet. Systemen är ofta beroende av hög säkerhet samtidigt är tillgängligheten mycket viktig och verksamheten får inte bli stillastående eller fördröjd till följd av störningar eller av säkerhetssystem som fördröjer kommunikationen. Kraven på systemen skiljer sig från den administrativa sidan, där man kan acceptera störningar och komplexa säkerhetssystem som drar ned systemets prestanda. Vi kan acceptera att arbetspasset avbryts för att ladda hem en uppdatering, något som är helt otänkbart i ett produktionssystem. Resultatet är att den tekniska sidan ligger efter då säkerhet har definierats utifrån driftssäkerhet och tillgänglighet snarare än datasäkerhet. Om ett kommando inte besvaras kan det få konsekvenser. Processer kan heller inte stoppas för att ladda ned den senaste antivirusprogramvaran.

”Ett produktionssystem har helt andra krav på svarstider”

Kryptering av kommunikation

I höstas gjorde SVTs Uppdrag Granskning en test av trådlösa hemmanätverk där många WLAN använde en för svag kryptering, den osäkra WEP krypteringen. Med en korrekt vald kryptering blir näten säkrare och informationen blir svårare att lyssna av.

-I M2M kommunikation används kryptering för att förhindra att information kan läsas och/eller ändras av obehöriga. Genom val av beprövade krypton uppnås bra säkerhet. Med en bra implementation av kryptering, nyckelhantering och autentisering, så erhålls en bra säkerhet. För att uppnå ett fungerande nät krävs att man dessutom möter kraven på driftsäkerhet, tillförlitlighet och enkelt användande. Först då får man en godtagbar och användbar säkerhet som varken stör eller negativt påverkar den verksamhet som utnyttjar M2M, berättar Leif Åkesson på Informasic. Det gäller alltså att ha alla bitar i balans.

Vad gäller kryptering så har små sensornoder ibland inte tillräckligt med processorkraft eller energi för att handa tunga krypteringar, exempelvis sådana som bygger på system med publika nycklar. Det gör att små noder är hänvisade till symmetriska krypton med hemliga nycklar, vilket i sin tur gör att nyckelhantering kan bli ett problem: hur skall den lilla sensornoden få sin hemliga nyckel på ett säkert sätt?

I de lokala näten är det ofta fråga om tidskritisk överföring av information, att en överföring har en fördröjning är inte att tänka på. Jämför man M2M eller WSN nät med de nät som

används för administration så är tidsfördröjningar oftast inte ett problem i de administrativa systemen. Utformningen av M2M och WSN systemen å andra sidan blir en balansgång mellan vilken säkerhet som kan implementeras och vilken tid en överföring får ta.

Standarder har olika säkerhetsnivå

Lokala trådlösa M2M nät kan utformas runt någon av de förekommande standarderna som 802.11 a/b/g/n (WLAN), Bluetooth, Zigbee och WirelessHART. WirelessHART är den standard som anses säkrast av dessa, den har en 128 bitars AES kryptering som inte går att stänga av. Det bygger på ”end-to-end” sessioner som säkerställer att överförd information bara kan dekrypteras av rätt mottagare. WirelessHART har en frekvenshoppande radioteknik med 16 kanaler, den har dessutom MESH teknik, vid störningar tar signalen en annan väg. WirelessHART skall kunna fungera klanderfritt, till och med så nära en WLAN basstation som 1 meter.

Mats Björkman, professor i datakommunikation vid Mälardalens högskola, har en del erfarenheter av WirelessHART i praktiken ”Vi har gjort en del tester som visar att WirelessHART är ganska bra på att få fram trafik. WirelessHART byter frekvens mellan paket (ett långsamt alternativ till frekvenshoppning), så om en frekvens är väldigt störd så kommer omsändningen att gå via en annan kanal. Genom parallella överföringar via alternativa vägar ökar också robustheten. Däremot är WirelessHART designat för datainsamling från sensorer, och dagens standard ger inte

”Val av beprövade krypton ger bra säkerhetsnivå”

alls bra resultat om man både vill samla in data från sensorer och styra aktuatorer genom samma nät. De fina tidsegenskaperna gäller bara data på väg åt åt ena hållet i nätet.”

GSM och 3G

En viktig aspekt av kommunikation via GSM och 3G nätet är att all kommunikation går okrypterat i operatörens nät, vid M2M kommunikation rekommenderar vi därför att överföringen krypteras, något som även Multicom Security ser som en viktig aspekt.

”En bra början är att inte lämna M2M terminaler öppna för åtkomst från Internet, de skall ligga bakom en brandvägg. De flesta M2M-utrustningar har dock ingen inbyggd brandvägg, då får trafiken styras över en central brandvägg hos kunden eller hos en serviceprovider. Ett exempel på en sådan lösning är Multicom Security med vår tjänst Mobiflex” säger Johnny Olsen på Multicom.

Johnnys tips för säker M2M kommunikation via GSM och 3G är att se till att terminalerna inte är direkt nåbara från Internet. Att styra trafiken genom en brandvägg ger bättre säkerhet. Andra lösningar kan vara att kryptera trafiken, även om den vanligaste lösningen är genom att skicka trafiken genom en så kallad VPN-tunnel. Då skapas en säker förbindelse mellan två anslutna enheter. De flesta moderna M2M kommunikationsprodukter för GSM/GPRS och 3G har stöd för detta i hårdvaran, inga anpassningar av den egna lösningen krävs.

Om stöd för kryptering i M2M-kommunikationen saknas går det också att i efterhand komplettera enheterna i nätet med en krypteringsmodul. Därmed skapas en krypterad och skyddad förbindelse hela vägen från sändare till mottagare, på samma sätt som med en VPN tunnel. Ingen utomstående kan då längre avlyssna eller manipulera kommunikationen. Alla enheter autentiseras, dvs sändare och mottagare vet alltid att det är rätt enhet man kommunicerar med. Skulle någon försöka byta ut en enhet och ersätta den med en annan, kommer kommunikationen inte längre att fungera.

I framtiden kommer trenden att gå mot ett ökat säkerhetstänkande menar Johnny Olsen på Multicom Security. ”Trenden går mot differentierade lösningar som tar hänsyn till hotbild och antal enheter. Bättre skydd ända ute i M2M-utrustningarna med inbyggda brandväggar och stöd för autentisering och kryptering samt generiska lösningar med många enheter där man eftersträvar en centralt kontrollerad säkerhetslösning för enkel administration och konfiguration av utrustning i fält.”

”M2M terminaler skall ligga bakom en brandvägg”