

# Remote Maintenance via internet?

## *Eenvoudig met Talk2M!*

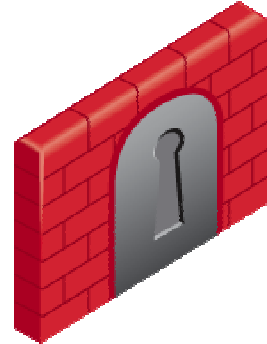
door René Langereis (Raster Products B.V.)

*Het op afstand benaderen van besturingen zoals PLC's en SCADA's is tegenwoordig met de huidige markt situatie van groot belang. Leveranciers van machines worden niet alleen maar geselecteerd op product of prijs, maar zeker ook op service. Er moet geproduceerd worden en stilstand kost geld. Reactietijden voor service zijn dus van zeer groot belang. Analoge inbelverbindingen worden in de industriële automatisering het meest toegepast om service op afstand te verlenen. Maar een "nieuw" medium doet zo zoetjes aan ook zijn intrede: Het Internet.*

### **Beren op de weg**

Hoewel we allemaal tegenwoordig bekend zijn met het internet, en hoewel we tegenwoordige allemaal stabiele internet verbindingen thuis hebben, is de industriële markt voorzichtig met het toepassen van het internet medium voor Remote Maintenance oplossingen. Een eigenschap van een internet verbinding is dat deze publiek aanwezig is en dus door iedereen die op het internet aanwezig is benaderd kan worden. Er moet dus op een of andere manier aan beveiliging worden gedacht.

Daarnaast krijgen we ineens te maken met de IT afdeling van een eindgebruiker. Deze afdeling heeft onder andere als taak het LAN netwerk up-and-running te houden en zoveel mogelijk gespuis buiten de deur te houden door middel van Firewall technologieën.



### **Beveiliging**

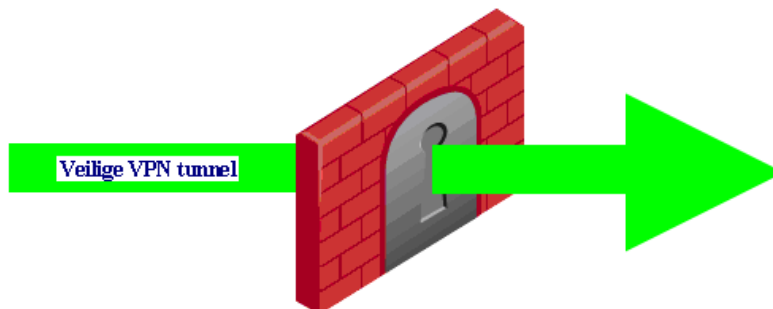
Bij vrijwel elke breedband verbinding die een eindgebruiker heeft wordt een firewall toegepast. Een firewall heeft als belangrijkste functie ongewenst verkeer buiten de deur te houden. Alleen, door de IT manager ingestelde, broodnodige poorten waarover bepaalde applicaties communiceren, worden naar binnen of naar buiten opengezet. Een van de bekendste poorten is poort 80 voor HTTP verkeer. Om een machine binnen het LAN netwerk van de eindgebruiker te kunnen benaderen moet er dus een poort naar binnen worden open gezet. Dit is tegenstrijdig met de doelstelling van de IT manager en stuit vaak op problemen.

Het gebruik maken van beveiligd dataverkeer is een compromis hierin.

Eén van de meest toegepaste vormen van het beveiligen van dataverkeer is Virtual Private Networking, kortweg VPN genoemd. Met VPN creëer je een stukje privé netwerk over een publiek toegankelijk netwerk heen. Alleen deelnemers met het juiste certificaat worden toegelaten tot de VPN. Daarnaast wordt VPN veelal in combinatie met encryptie toegepast. Hierbij wordt het dataverkeer door de tunnel ook nog eens versleuteld, waardoor het dataverkeer voor deelnemers van het netwerk die niet beschikken over deze sleutel "onleesbaar" is.

De meest toegepaste VPN technologie in kantoorapplicaties is IPsec (staat voor IP security). Dit is een op laag 3 van het OSI-model gebaseerd protocol en erg geschikt voor verbindingen die voor lange tijd tot stand worden gebracht. Omdat het een netwerklaag protocol is, krijgt de remote

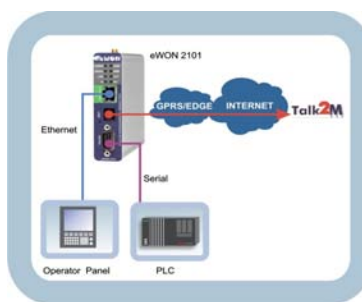
gebruiker toegang tot het achterliggende netwerk. Dit is een situatie die niet echt wenselijk is in de industrie.



Een ander steeds meer in opkomst zijnde VPN technologie is TLS/SSL. Dit is een technologie die werkt bovenop de TCP/IP stack (applicatie laag). Net als bij IPsec wordt ook bij TLS/SSL encryptie toegepast. TLS/SSL beveiligt echter alleen het verkeer tussen twee specifieke applicaties, waardoor slechts deze applicatie benaderbaar is en dus niet het hele netwerk. Eén van de meest bekendste toepassing van TLS/SSL technologie is het internet bankieren.

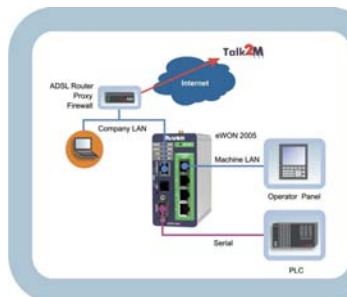
### Talk2M

Talk2M (Talk-to-Machines) is een internet service speciaal ontworpen om te voldoen aan de groeiende behoefte van breedband en draadloze toegang voor Remote Maintenance. De toegevoegde waarde van Talk2M is de totale integratie van IT beveiligingsstandaarden gebaseerd op TLS/SSL technologie die aan beide kanten van de verbinding geïmplementeerd kan worden zonder veranderingen aan te brengen in de IT infrastructuur. Dit omdat aan beide kanten naar buiten toe wordt gecommuniceerd. Deze doorbraak zorgt voor eenvoudige implementatie zonder aanpassingen aan de complexe IT netwerk structuur.



Als de Talk2M oplossing wordt gebruikt in combinatie met GPRS/EDGE verbindingen, dan heeft de remote zijde slechts een standaard SIM kaart nodig. Hiermee wordt een speciale APN of een duurdere speciale SIM kaart vermeden. Een verbinding via ADSL is recht toe recht aan.

De meest krachtige en innovatieve oplossing met Talk2M aan de Remote zijde is het gebruik van de bestaande Ethernet LAN netwerk met zijn internet verbinding. De remote besturing wordt overal ter wereld beschikbaar via het Internet. Hiervoor is geen extra telecom medium meer nodig.



## eWON

Samen met de brede eWON range industriële modem-routers, werpt Talk2M een nieuwe blik op Remote Maintenance en toegang over het internet. eWON is compatibel en integreerbaar met een brede range van seriële en Ethernet gebaseerde PLC's en SCADA's: Siemens®, Rockwell Automation®, Schneider Electric®, Omron®...



Met als doel kostenbesparing voor uw service afdeling, biedt de Talk2M's gebruikersinterface u een eWON adres boek en een single-click toegang tot uw besturingen!

Meer informatie over Talk2M kunt u vinden op de website van Raster.

## Over Raster

Raster Products is leverancier van high-end automatiseringsproducten op het gebied van industriële communicatie en visualisatie. Naast producten verzorgt Raster Products ook een groot aantal technologie trainingen. Tijdens de trainingen wordt theoretische maar met name ook praktische informatie gepresenteerd. De trainingen worden gehouden bij Raster of op een centrale plaats in de BeNeLux. Ook kunnen de trainingen In-House worden georganiseerd.

## Raster Products B.V.

Postbus 3  
6620 AA DREUMEL  
Tel: +31 (0)487-572719  
Fax: +31 (0)487-573394  
website: [www.raster.com](http://www.raster.com)