Internet of things maakt extra maatregelen nodig

Machines beter beveiligd

door **Alfred Monterie**

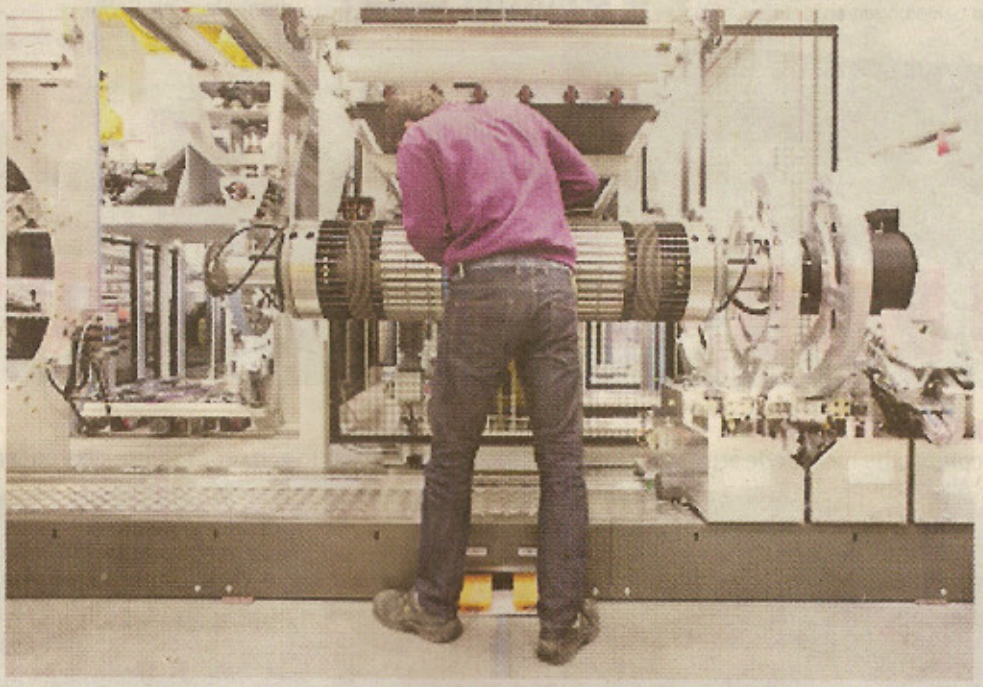
HENGELO • Het *internet of things* gaat de industriële wereld volledig op zijn kop zetten. Door machines in een netwerk te plaatsen kan hun efficiency worden vergroot.

Een apparaat is voortaan zelf in staat aan te geven wanneer onderhoud nodig is. GE maakt al locomotieven die dankzij sensoren weten hoeveel regen en wind ze hebben doorstaan. Die melden zich automatisch bij de werkplaats voor een oplapbeurt.

Ook zullen nieuwe diensten ontstaan. Machines worden niet meer tegen een vaste prijs verkocht maar afnemers gaan naar verbruik betalen. Leveranciers zien brood in het Nespresso-model waarbij niet aan het apparaat maar aan de koffiepads wordt verdiend.

Elk apparaat dat aan het netwerk is gekoppeld, krijgt software. Die moet voorkomen dat machines worden gemanipuleerd, bijvoorbeeld door geen originele grondstoffen te gebruiken of met de teller te knoeien. Die software is ook nodig voor de aansturing en de communicatie met andere apparaten en centrale databases.

Dat betekent meer kans op veiligheidsproblemen. Aanvallers kunnen namelijk op veel plaatsen inbreken als straks tientallen miljarden apparaten aan het internet zijn gekoppeld.



De bandenmachines van VMI zijn beveiligd tegen gesjoemel.

Nike voorkomt illegale kopieën

Nu al is de beveiliging van machines en bescherming tegen namaak een groot probleem. Concurrenten of afnemers zelf proberen vaak uit het Westen geleverde machines na te bouwen, iets wat in China veel gebeurt. Ook is er veel piraterij. Nike laat in India op shirtjes logo's borduren. Als daarvoor machines worden geleverd, duurt het maar een paar weken voordat een stroom namaakartikelen op gang komt.

Textielfabrieken komen snel in de verleiding naast de orders van Nike grijze productie te draaien. Merkfabrikanten die de vervaardiging uitbesteden, willen daarom de totale controle over hun machines hebben.

Softwareleverancier Wibu Systems, met vestiging in Hengelo, denkt de oplossing in huis te hebben. Directeur Marcel Hartgerink: „Aan elk apparaat met een usb-ingang wordt een dongel geplaatst met software. Die regelt wie wanneer toegang krijgt tot het systeem. Zonder deze sleutel kan er niets gebeuren. Dit beschermt de broncode. Hackers komen voor een gesloten deur. Ze kunnen niet van afstand ovens ontregelen door bijvoorbeeld de temperatuur gevaarlijk hoog te maken. Dit soort chantage is niet mogelijk. Ook het benadelen van licentiegevers door heimelijk extra productie te draaien wordt bemoeilijkt."

Een grote klant als VMI uit Epe kan zo voorkomen dat zijn geavanceerde bandenmachines worden nagebouwd. Deze installaties, die jaarlijks 250 miljoen banden vervaardigen, zijn hermetisch beveiligd. De aansturing gaat volledig automatisch. Alleen de eigen servicemedewerkers zijn in staat om online even taken uit te voeren. Zowel de machine als het recept van de band zit achter slot en grendel.

Een andere klant van Wibu is GenKey uit Eindhoven, die stemkastjes maakt. Tijdens de verkiezingen in Ghana moest elke kiezer zich met een vingerafdruk identificeren. Om fraude tegen te gaan had niemand toegang tot de software die de stemmen telt. „Alleen onze servicemensen konden erbij", aldus Hartgerink.