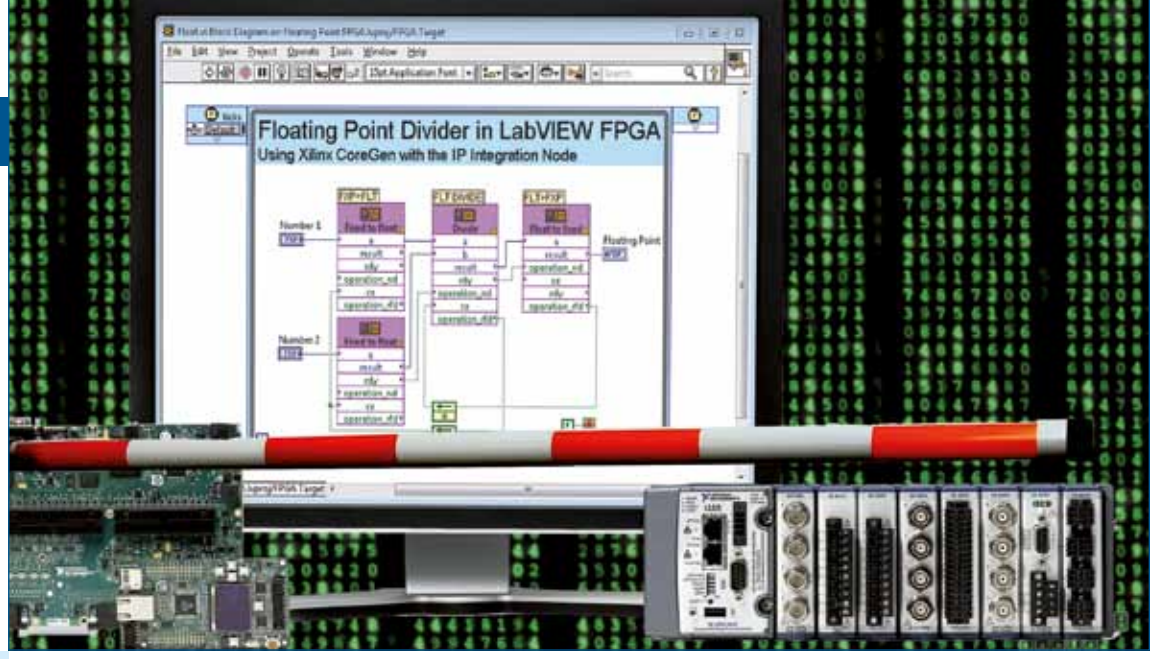
Geen toegang voor cybercriminelen

Tips om ellende buiten de deur te houden



Naast het garanderen van een goed werkend systeem is de beveiliging van gevoelige informatie een belangrijk veiligheidsaspect. Niet alleen de informatie zelf is daarbij van belang, maar ook de waardevolle algoritmen waarover de controllers beschikken. Het beschermen van deze, is met andere woorden eveneens cruciaal. Naast technische maatregelen is het ook belangrijk dat medewerkers doordrongen zijn van de nood en beveiliging inbouwen in hun dagelijkse routine.

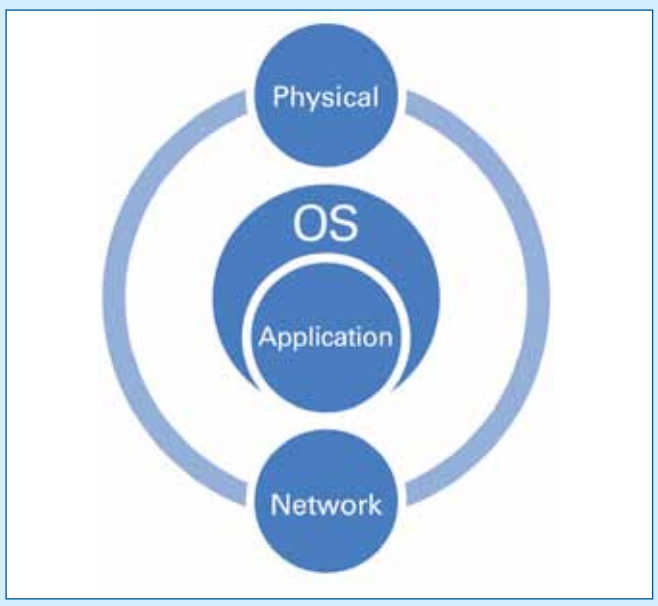
Beveiligingsniveaus

Moderne automatiseringssystemen bestaan vaak uit een mix van industriële controllers, industriële PC's (denk aan HMI) en via het netwerk aangesloten (kantoor)computers. Veiligheid hierbinnen kan op een aantal verschillende niveaus worden gedefinieerd: fysiek, netwerk, besturingssysteem en toepassing (zie figuur 1).

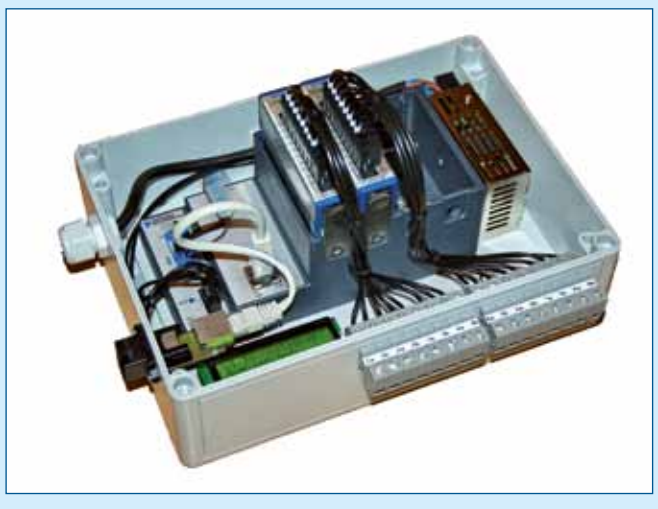
Het is belangrijk dat op elk niveau een vorm van beveiliging aanwezig is. Wordt veel tijd en geld geïnvesteerd in de beveiliging van één van de niveaus en wordt op een ander niveau bezuinigd, dan vindt vervolgens een indringer altijd wel een weg om het beveiligde niveau heen en neemt hij alsnog het beheer over.

Aanbevolen

De hier besproken procedures voor beveiliging zijn onderverdeeld in drie groepen: aanbevolen, optioneel en extreem. De aanbevolen procedures zijn een goede basis waarbij geen uitgebreide investeringen in tijd of kosten nodig zijn. De optionele maatregelen vereisen meer tijd en inspanning, maar worden voor veel applicaties wel als noodzakelijk ervaren. De extreme maatregelen vragen om aanzienlijke investeringen in tijd en kosten en zijn zeker niet voor alle toepassingen geschikt.



Figuur 1. De niveaus en de respectievelijke belangrijke beveiligingen voor een industrieel systeem.



Figuur 2. Om pieken in het stroomverbruik op te vangen, kunnen energieleveranciers noodstroomaggregaten op afstand starten via deze CompactRIO controllers. (Foto VI Technologies)

- **Netwerk Firewall:** De eerste maatregel is het gebruik van een softwarematige en een hardware matige firewall om de pc en de besturing te beschermen. Firewalls met een DMZ (demilitarized zone) hebben een LAN (veilig lokaal netwerk), een WAN (onveilig internet) en een DMZ (onveilig deel van het lokale netwerk), dit om te voorkomen dat internet in het LAN-deel terecht kan komen. Standaard behoort een softwarematige firewall op iedere computer thuis.
  Het beheren van het datatransport is een volgende stap. De aanbevolen methode hierbij is om de informatie tussen pc's te beveiligen door gebruik te maken van een SSL enabled Web Service en standaard poorten te wijzigen. Dit wordt gebruikt bij een systeem van VI Technologies opgebouwd met een CompactRIO controller (figuur 2). Dit is bedoeld om pieken in het stroomverbruik op te kunnen vangen door noodstroomaggregaten van bijvoorbeeld ziekenhuizen op afstand te starten. Om te zorgen voor een veilige communicatie, gebruikt men SSL web services en sturen de controllers elke 10 seconden een statusbericht en als antwoord ontvangen zij hun commando van een specifiek adres.
- **Updates, patches, anti virus en gebruikers.** Van belang is dat naast de firewall ook altijd de laatste beveiligingspatches door middel van updates beschikbaar zijn. Stel ook een standaard gebruikersaccount in waarmee de functionaliteiten worden begrensd. De toepassing van de default administratieve account biedt indringers de faciliteiten om meer schade op de pc aan te richten als zij weten in te breken.
  Wachtwoorden kunnen zowel op applicatieniveau als op broncode niveau worden ingesteld. Broncode kan immers gevoelige informatie of belangrijke algoritmen bevatten. Het verwijderen van de broncode of installatiebestanden op de pc en volledig vertrouwen op het EXE-bestand zorgt er eveneens voor dat een aanvaller veel meer werk heeft om de pc applicatie te stelen of te manipuleren.
- **Remote Access.** Dit wordt als methode gebruikt om op afstand op een veilige manier toegang tot de controller te krijgen Zorg er dan wel voor dat de instellingen en toestemmingen zorgvuldig zijn ingesteld om ongeautoriseerd beheer van de pc te voorkomen.
- **Bounds Checking.** Zinvol is een controle te implementeren om de hardware en de sensor downstream te beschermen tegen een binnendringende aanvaller. Daarnaast is het verstandig om een waakhond (watchdog) op de toepassing te zetten, zodat bij een foutmelding het systeem in een veilige modus kan worden geplaatst.

Optionele maatregelen

- **Uitzetten of encrypten van I/O.** Het gebruik van plug-and-play apparatuur (denk aan USB poorten in een soft-PLC) vormt een bedreiging. I/O zorgvuldig beheren of afschermen, voorkomt ongewenste aanvallen. Ook het fysiek beveiligen van de pc en de controller is aan te raden door er voor te zorgen dat de pc in een afgesloten omgeving staat.
- **Statussignaal.** Het gebruik van een statussignaal via een SSL enabled web service tussen de pc en de controller biedt de mogelijkheid om bij een foutmelding via het netwerk de gebruiker hierop te attenderen en de pc en de controller waken over elkaars veiligheid. Blijkt er een onjuist statussignaal aanwezig te zijn of er wordt niet tijdig gereageerd, wordt de veilige modus ingeschakeld.

Extreme maatregelen

Extreme maatregelen zijn bedoeld voor gebruikers die een absoluut beveiligingsniveau nastreven.

- **Applicatie Whitelisting.** Dit concept bestaat uit twee componenten. De eerste is de instelling waarbij de checksum van alle executables, binaries en andere uit te voeren bestanden wordt berekend op het moment dat het systeem volledig in orde is. Nadat een tabel hiervan is opgesteld, kan de whitelisting applicatie alles in de gaten houden. Het tweede deel bestaat uit een applicatie die vooraf controleert of er niet is geknoeid. Komt de checksum niet overeen, dan wordt voorkomen dat de applicatie wordt uitgevoerd. De enige nadelen van whitelisting zijn de kosten en het onderhoud.
- **Hardware Checking.** Een extra maatregel is het signaleren of de behuizing van het systeem is geopend (geweest). Zo ja, wordt de controller in een veilige modus gestart en/of een bericht naar een operator gestuurd.

Samenvatting

Het is helaas niet mogelijk om in dit artikel alle beveiliginsfactoren mee te nemen. De ANSI/ISA-99/IEC 62443 standaard is dan ook een uitstekende informatiebron voor ieder die met automatisering van doen heeft. ●

Voor meer informatie zie www.etotaal.nl/achtergrond.
Artikel "Geen toegang voor cybercriminelen".

Erik van Hilten, Marketing Engineer bij National Instruments