

Basics of Industrial Security in the factory automation (ST-SECFA1)

Korte beschrijving

Deze training geeft een overzicht van het 'defense-in-depth' concept om installaties te beveiligen, met als doel de deelnemers vertrouwd te maken met de gevaren voor installaties in de maakindustrie, mogelijke kwetsbaarheden te analyseren en risico's in te schatten.

Doelen

In deze opleiding leren de deelnemers welke maatregelen genomen kunnen worden om de verschillende soorten bedreigingen het hoofd te bieden.

Doelgroep

- Projectleiders, projectmedewerkers
- Hardware-ingenieurs, programmeurs
- Inbedrijfname
- Information security officers

Inhoud

- Verschillen tussen security in bureau- en industriële omgeving
- Waarom is industrial security noodzakelijk (bedreigingen, incidenten)?
- Wat omvat het beveiligingsconcept 'defense in depth'?
- Inleiding in het gebruikersbeheer van TIA Portal
- Controller security - systeemintegriteit voor de SIMATIC PLC's
- Inleiding in authenticatie- en encryptiemechanismen
- Beveiligde communicatiemogelijkheden van de SIMATIC CPU S7-1500
- HMI security – beveiligingsmechanismen voor HMI's and sm@rt Server, gebruikersbeheer voor HMI runtime
- PC security – verschillende maatregelen voor zowel hardening, als gebruikersbeheer en patch management van PC-systemen, detectie van malware
- Network security – Hardening van netwerkcomponenten
- Het cell protection concept en de implementatie van remote service
- Mechanismes voor toegangsbeveiliging voor netwerken
- Plant security – fysieke en organisatorische beveiligingsmaatregelen en continue processen

Vereiste voorwaarden

Basiskennis van automatisering in de maakindustrie
Basiskennis netwerken (in overeenstemming met de web-based training WT-IEOSI)

Opmerking

Cursusdocumentatie: Engels
Trainer: Nederlandstalig

Soort

Face-to-face-training

Duur

2 dagen

Taal

nl