

# SIEMENS



TIA PORTAL 10 JAAR

## TIA Portal versie 17 biedt maximale Industrial Security

Met TIA Portal versie 17 zet Siemens een grote stap op het gebied van Industrial Security. Wat is nieuw en hoe biedt dit nog meer bescherming tegen toegang door onbevoegden van buitenaf? Een overzicht.

Operationele Technologie (OT), waarvan TIA Portal een voorbeeld is, draaide in de praktijk jarenlang binnen een aparte omgeving, die los stond van de IT-omgeving van het bedrijf. Tegenwoordig worden IT- en OT-systemen steeds meer geïntegreerd in het overkoepelende bedrijfsnetwerk, dat verbonden is met het internet en waaraan strenge eisen worden gesteld. Drie nieuwe beveiligingsfeatures in TIA Portal versie 17 komen hieraan tegemoet.

### **Toegangsbeveiliging by default**

Bij de initiële configuratie van de PLC vraagt TIA Portal de gebruiker 'by default' een digitaal certificaat aan te maken en dit te beveiligen met een wachtwoord. Men wordt hier via een

wizard in drie stappen doorheen geleid. Alleen met de unieke combinatie van certificaat en wachtwoord krijgt men toegang tot de PLC. Hierna is de communicatie beveiligd via TLS 1.3. Dit om te voorkomen dat onbevoegden (hackers) de PLC kunnen benaderen. Om compatibiliteit met oudere systemen te behouden, bestaat de mogelijkheid om deze feature te deactiveren. Wij raden er sterk van af dit te doen! Ook de verbinding tussen PLC en HMI kan worden beveiligd, waardoor alle informatie versleuteld wordt verstuurd. Aftappen van informatie is dan niet meer mogelijk.

### **User Management and Access Control**

Met TIA Portal V17 is het User Management and Access Control (UMAC) verder uitgebreid. Bij het inloggen wordt aan de hand van de ingevoerde gebruikersnaam en het wachtwoord bepaald welke toegangsrechten tot projecten de gebruiker heeft. Zo zal een hoofdingenieur vaak onbeperkte toegang krijgen om wijzigingen in het project te kunnen doorvoeren. Een service engineer zal wellicht alleen wijzigingen kunnen doorvoeren in de HMI en of het standaard programma, maar bijvoorbeeld niet in het safety programma. Machinebouwers kunnen na de oplevering de gebruiker laten meekijken in het project, zonder dat deze cruciale wijzigingen kan doorvoeren.

Via centralized user management (UMC) kan men de gebruikersrechten vastleggen. Hierdoor hoeft men niet voor elk nieuw project in TIA Portal opnieuw rollen aan te maken. Als een medewerker het bedrijf verlaat of een nieuwe functie krijgt, kan zijn profiel met de bijbehorende gebruikersrechten worden verwijderd dan wel aangepast. Centralized user management is kosteloos tot maximaal 10 gebruikers en kan optioneel worden uitgebreid.

### **Certificaat voor OPC UA**

De PLC kan via het gestandaardiseerde OPC UA-protocol communiceren. Dit kan beveiligd worden op basis van een certificaat dat bij de initiële configuratie van de PLC wordt aangemaakt. Om veiligheidsredenen moet dit certificaat regelmatig worden vernieuwd. Dit was vroeger een taak voor de PLC-programmeur. Bovendien ging de PLC bij de vernieuwing van het certificaat in stop en lag de productie tijdelijk stil. Vanaf versie 17 kan men het certificaat via de Global Discovery Server (GDS) om de zoveel tijd automatisch vernieuwen, zonder dat de PLC in stop gaat. Na de oplevering van het project hoeft de machinebouwer niet meer te worden betrokken bij het vernieuwen van het certificaat. De Security Officer van de eindgebruiker kan dit eenvoudig zelf doen.

Vanzelfsprekend houden wij de beveiliging van TIA Portal continu up-to-date. Dit wordt standaard meegenomen in alle nieuwe releases en versies. Op 1 juli hebben we een webinar gehouden, waarin deze onderwerpen verder toegelicht zijn. U kunt dit webinar terugkijken via <https://new.siemens.com/nl/nl/products/automation/topic-areas/industry-actueel/workshops/tp202106.html>. Vooraf inschrijven is wel noodzakelijk.