

## Security Grundlagen für die Factory Automation (ST-SECFA1)

---

### Kurzbeschreibung

---

Das Training vermittelt einen Überblick zum Schutzkonzept Defense-in-Depth von Anlagen. Dabei sollen die Teilnehmer Gefahren für Anlagen aus der Fabrikautomatisierung kennenlernen, potentielle Schwachstellen analysieren und Risiken bewerten.

### Ziele

---

Im Kurs erwerben die Teilnehmer das Wissen, welche Gegenmaßnahmen für die verschiedenen Bereiche des Konzepts angewendet werden können.

### Zielgruppe

---

Projektleiter, Projektmitarbeiter  
Technologen  
Projektierer, Programmierer  
Inbetriebsetzer,  
Information Security Officers

### Inhalte

---

- Was sind die Unterschiede zwischen Office und Industrial Security?
- Wozu ist Industrial Security notwendig (Bedrohungen, Vorfälle)?
- Was umfasst das Sicherheitskonzept Defense in Depth?
- Ein Einstieg in die Benutzerverwaltung mit TIA Portal
- Controller-Sicherheit – Systemintegrität für SIMATIC Controller
- Ein Einstieg in Authentifizierungs- und Verschlüsselungsmechanismen
- Gesicherte Kommunikationsmechanismen der SIMATIC CPU S7-1500
- HMI-Sicherheit – HMIs und sm@rt Server Schutzmechanismen, Benutzerkonzept für HMI Runtime
- PC-Sicherheit – verschiedene Maßnahmen zur Härtung sowie zum Benutzer- und Patchmanagement von PC-Systemen, Schadsoftware erkennen
- Netzwerksicherheit – Härtung von Netzwerkkomponenten
- Das Zellschutzkonzept und die Realisierung von Fernwartungszugängen
- Mechanismen zum Zugriffsschutz auf Netzwerke
- Anlagensicherheit – physikalische und organisatorische Sicherheitsmaßnahmen und kontinuierliche Prozesse

### Teilnahmevoraussetzung

---

- Grundlegende Kenntnisse von Fabrikautomatisierung
- Grundlegende Netzwerkkennnisse (entsprechend Kenntnisse der WBT WT-IEOSI)

### Typ

---

Präsenztraining

### Dauer

---

2 Tage

### Sprache

---

de