Industrial Control Systems Security

Lerneinheit 1: Einführung

Prof. Dr. Christoph Karg

Studiengang Informatik
Hochschule Aalen

Wintersemester 2013/2014

3.10.2013

Einleitung

Diese Lerneinheit ist eine Einführung zu Sicherheitsaspekten von Industrial Control Systems (ICS)

Es werden folgende Fragestellungen behandelt:

- Welche Arten von ICS unterscheidet man?
- Wie ist der prinzipielle Aufbau eines ICS?
- Aus welchen technischen Komponenten besteht ein ICS?
- Welche Anforderungen müssen ICS erfüllen?
- Worin unterscheiden sich ICS von herkömmlichen IT-Systemen?

Diese Lerneinheit basiert auf dem NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security

Beziehung zwischen ICS und IT-Systemen

- ICS wurden ursprünglich parallel zu herkömmlichen IT-Systemen entwickelt
  - Proprietäre Protokolle
  - Spezialanfertigung von Hardware und Software
- Ab den 1980er Jahren zunehmende Adaption von gängigen IT-Komponenten
  - Kostenersparnis durch Einsatz von Commercial Off The Shelf (COTS) Komponenten
  - Anforderung zur Vernetzung mit betriebswirtschaftlichen Anwendungen
  - Fernwartung mittels IT-Systemen
- Konsequenz: Gefährdungen von IT-Systemen auch auf ICS anwendbar

Eigenschaften von ICS

- ICS haben einen direkten Einfluss auf die „reale“ Welt
- Störfälle stellen ein Risiko für die Gesundheit von Menschen und die Umwelt dar
- Der Ausfall von ICS führt zu einem großen finanziellen Schaden
- ICS stellen eine große Anforderung an Betriebssicherheit (Safety) und Zuverlässigkeit (Reliability)
- Die Sicherheitsanforderungen von ICS stehen oft im Gegensatz zu den entsprechenden Anforderungen von herkömmlichen IT-Systemen

Mögliche Sicherheitsvorfälle

- Blockierter oder verzögerter Informationsfluss
  $\rightsquigarrow$ Ausfall des ICS
- Unautorisierte Änderung von Parametern des ICS
  $\rightsquigarrow$ Gezielte Manipulation des ICS
- Gezieltes Einspeisen von Fehlinformationen
  $\rightsquigarrow$ Social Engineering des Wartungspersonals
- Software-Manipulation durch Malware
  $\rightsquigarrow$ Generierung von Störfällen bis hin zum Ausfall des ICS

Gängige Sicherheitsvorkehrungen I

- Beschränkung des Netzwerkzugriffs auf ICS
  - ▷ Netzwerktopologie mit mehreren Zonen (Zwiebelmodell)
  - ▷ Demilitarized Zone (DMZ)
  - ▷ Einsatz von Firewalls
- Beschränkung des physikalischen Zugriffs auf ICS Hardware
  - ▷ Bauliche Maßnahmen
  - ▷ Zugangskontrolle
- Schutz von Software-Schwachstellen
  - ▷ Regelmäßiges Einspielen von Patches
  - ▷ Deaktivierung von nicht benötigten Funktionalitäten
  - ▷ Rollenbasiertes Berechtigungskonzept

Gängige Sicherheitsvorkehrungen II

- Aufrechterhaltung des Betriebs bei Störfällen
  - Schaffung von Redundanz bei Hardware-Komponenten
  - Vermeidung von hohem Netzwerkverkehr bei Ausfall von Systemkomponenten
  - Verhinderung von Kaskadeneffekten
- Erstellen von Notfallplänen
  - Aufrechterhaltung des Betriebs bei Störfallen
  - Wichtiges Kriterium: Zeitspanne zwischen Auftreten eines Störfalls und Wiederherstellung des Betriebs

Komponenten einer Sicherheitsstrategie I

- Entwicklung von Sicherheitsrichtlinien und -mechanismen speziell für ICS
- Erarbeitung von geeignetem Schulungsmaterial
- Berücksichtigung von Sicherheit während des kompletten Lebenszyklus eines ICS
- Entwicklung einer mehrschichtigen Netzwerktopologie für ICS
- Logische Trennung von Unternehmens- und ICS-Netzwerken
- Einsatz einer DMZ für den Zugriff auf das ICS-Netzwerk

Komponenten einer Sicherheitsstrategie II

- Schaffung von Redundanz bei Hardware-Komponenten und Netzwerkkomponenten
- Deaktivierung von nicht benötigten Softwarekomponenten (inklusive Netzwerk-Ports)
- Patch-Management
- Einschränkung des physikalischen Zugriffs auf ICS-Komponenten
- Entwicklung eines rollenbasierten Benutzerkonzeptes
- Beschränkung der Benutzerberechtigungen auf die zur Erledigung der Aufgaben notwendige Berechtigungen

Komponenten einer Sicherheitsstrategie III

- Trennung von Zugriffsmechanismen für ICS- und Unternehmensnetzwerk
- Authentizitätsprüfung mit modernen Technologien (z.B. Smartcards)
- Einsatz von Überwachungsmechanismen wie z.B. Virenscannern, Intrusion Detection Systemen und Integritätschecks von Dateisystemen
- Einsatz von Verschlüsselungsmechanismen an den notwendigen Stellen
- Protokollierung und Beobachtung von Auditvorgängen

Supervisory Control And Data Acquision (SCADA)

Eigenschaften

- Verteiltes System
- Schmalbandige Netzwerkanbindung
- Steuerung und Überwachung von geografisch weit verteilten Anlagen
- Zentrale Datensammlung und Steuerung sind für den Betrieb essentiell

Beispiele

- Wasserversorgung
- Gas- und Ölpipelines
- Stromnetz
- Bahnnetzwerk

Distributed Control Systems (DCS)

Eigenschaften

- Steuerung von Produktionsanlagen
- Breitbandige Netzwerkanbindung
- Mehrschichtige Architektur
- Anbindung an Warenwirtschaftssysteme

Beispiele

- Erdölraffinerien
- Automobilproduktion
- Chemische Industrie

Programmable Logic Controllers (PLC)

Eigenschaften

- Steuerung von kleineren Anlagen und Prüfständen
- Breitbandige Netzwerkanbindung
- Einsatz in allen industriellen Prozessen
- Einsatz als Komponente in SCADA Systemen oder DCS

Beispiele

- Steuerung von Fertigungslinien
- Signal- und Schrankensteuerung bei der Eisenbahn

Arten von Produktionsprozessen

Unterscheidung:

- Kontinuierlicher Produktionsprozess
- Diskontinuierlicher Produktionsprozess
- Mischformen

Beachte: Die Steuerung beider Prozessarten basiert auf derselben Art von ICS

Kontinuierlicher Produktionsprozess

Eigenschaften

- Produkte werden fortlaufend hergestellt
- Betrieb der Anlage rund um die Uhr
- Hohe Kosten beim Stillstand der Fertigung

Beispiele

- Papierherstellung
- Verhüttung von Metallen
- Energiewirtschaft
- Raffinerien

Diskontinuierlicher Produktionsprozess

Eigenschaften

- Die Produktion unterteilt sich in mehrere diskrete Fertigungsschritte
- Eine Produktionslinie kann zur Herstellung verschiedener Produkte eingesetzt werden
- Herstellung von Chargen

Beispiele:

- Automobilindustrie
- Lebensmittelindustrie
- Herstellung von elektronischen Komponenten

Aufbau eines ICS

Control Loop

- Steuerung des Fertigungsprozesses
- Komponenten: Sensoren, Aktoren, Steuerungseinheit

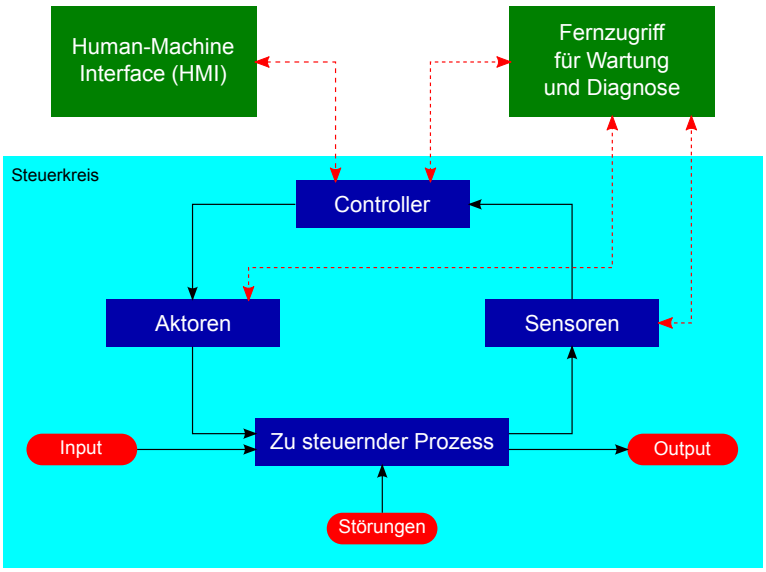
Human-Machine Interface (HMI)

- Darstellung des Prozessstatus
- Überwachung des Prozesses und Manipulation der Parameter

Fernzugriff für Wartung und Diagnose

- Werkzeuge, um fehlerhaftes Verhalten zu untersuchen oder zu verhindern

Aufbau eines ICS – Grafik



Bausteine von ICS

- In ICS kommt eine Vielzahl von technischen Komponenten zum Einsatz
- Unterscheidung:
  - Bausteine zur Steuerung der Anlage
  - Netzwerk Komponenten

Steuerungskomponenten I

- Control Server
  - Steuerung der gesamten Anlage
  - Netzwerkzugriff auf die nachgeordneten Systeme
- SCADA Server/Master Terminal Unit (MTU)
  - Zentrale Steuerungseinheit bei SCADA Systemen
  - Informationsbeschaffung durch Zugriff auf nachgelagerte RTUs
- Remote Terminal Unit (RTU)
  - Einheit zum Sammeln von Daten und Steuern von Knoten in einem SCADA System
  - Oft Spezialanfertigung von Hardware und Software
  - Netzwerkanbindung über Kabel oder Mobilfunk

Steuerungskomponenten II

- Programmable Logic Controller (PLC)
  - Embedded System oder Industrie-Rechner mit kleiner Bauform
  - Flexibel einsetzbar
- Intelligent Electronic Devices (IED)
  - Smart Sensor/Aktor
  - Automatisierte Steuerung auf lokaler Ebene
- Human-Machine-Interface (HMI)
  - Interaktion des Personals mit dem ICS
  - Darstellung des aktuellen Systemzustands
  - Möglichkeit zur Parameteränderung und Steuerung der Anlage

Steuerungskomponenten III

- Data Historian
  - Datenbank zur Protokollierung von Vorgängen im ICS
  - Einsatzgebiete: Überwachung, Rekonstruktion von Vorfällen, Produktionsplanung
- Input/Output (I/O) Server
  - Komponente zum Abruf und zur Speicherung der von RTUs oder PLCs bereitgestellten Daten
  - Teil des Control Servers oder eigenständige Einheit

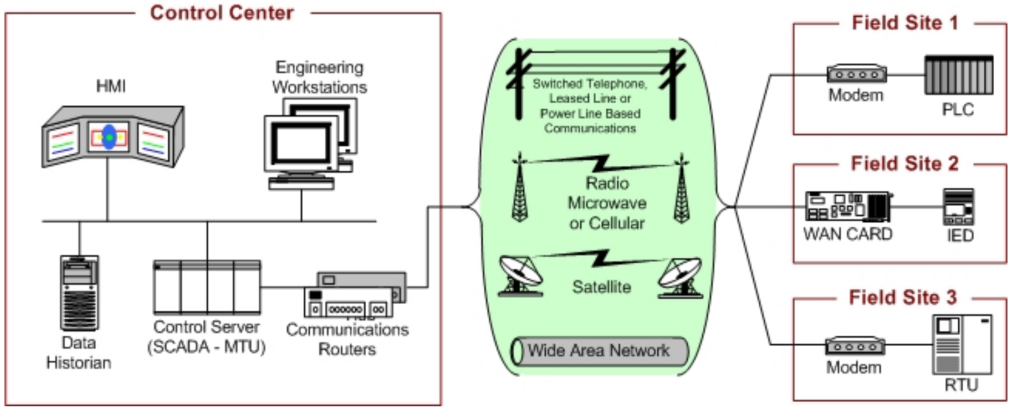
Netzwerkkomponenten I

- Fieldbus Network
  - Anbindung von Sensoren und Aktoren an einen PLC
  - Ringtopologie
- Control Network
  - Verbindung der Überwachungssysteme mit nachgeordneten Modulen
  - Einsatz verschiedener Technologien z.B. Ethernet, ADSL
- Router
  - Verbindung zwischen separaten Netzwerken
  - Schnittstelle für den Übergang zwischen Netzwerksegmenten unterschiedlicher Technologie

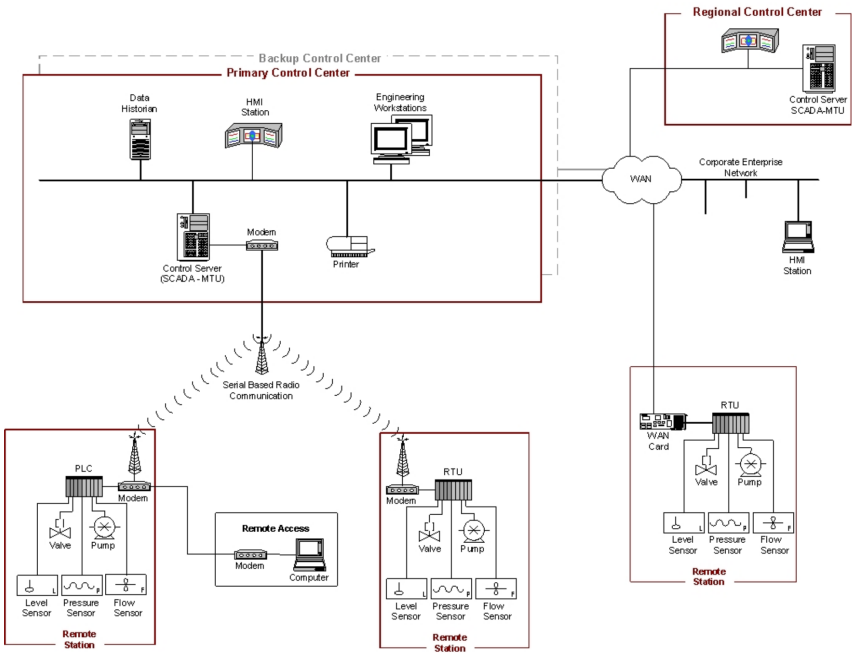
Netzwerkkomponenten II

- Modems
  - Anbindung von Systemen über Telefonleitungen
  - Weit verbreitet bei SCADA Systemen
- Remote Access Points
  - Fernzugriff auf Kontrollsysteme
  - Abfrage von Messdaten eines PLCs

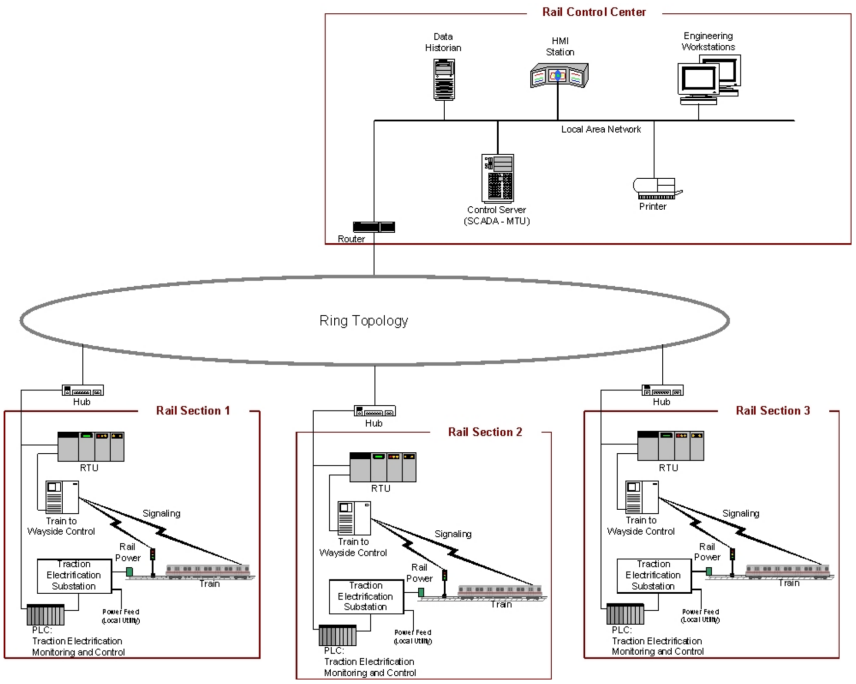
Beispiel: SCADA System 1



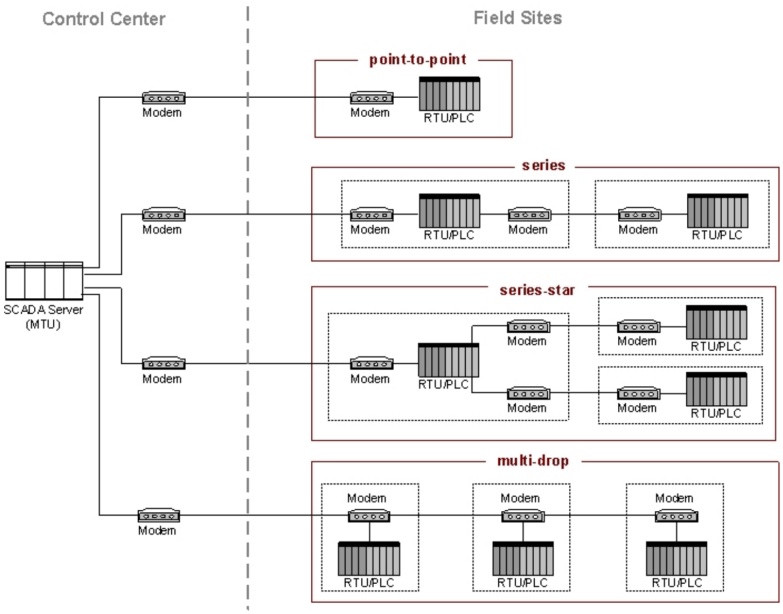
Beispiel: SCADA System 2



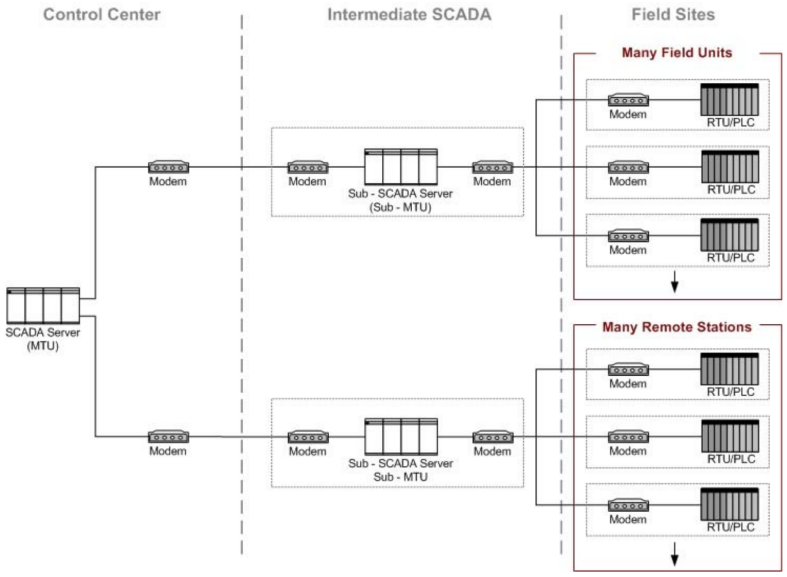
Beispiel: SCADA System 3



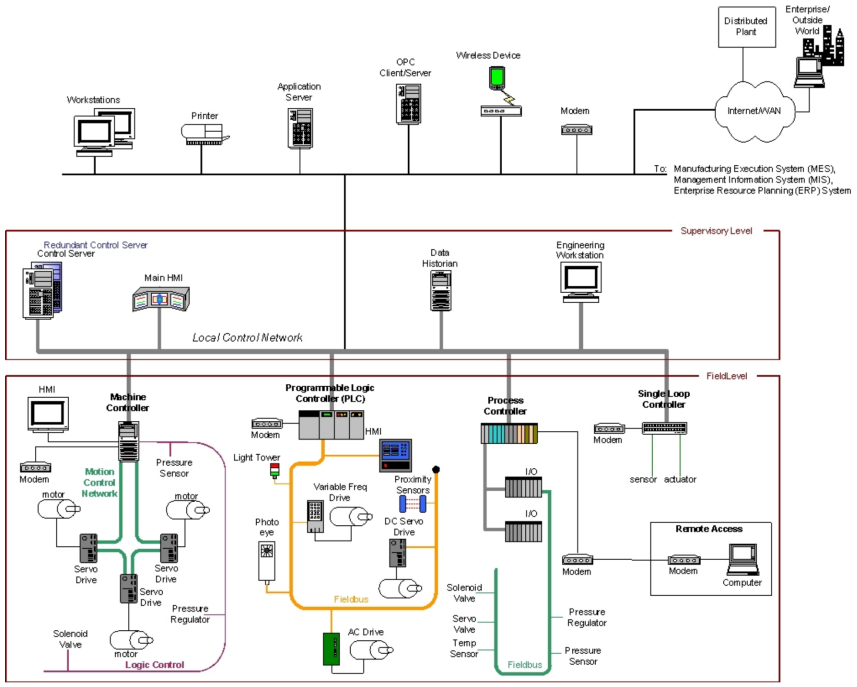
Beispiel: Topologie eines SCADA Systems 1



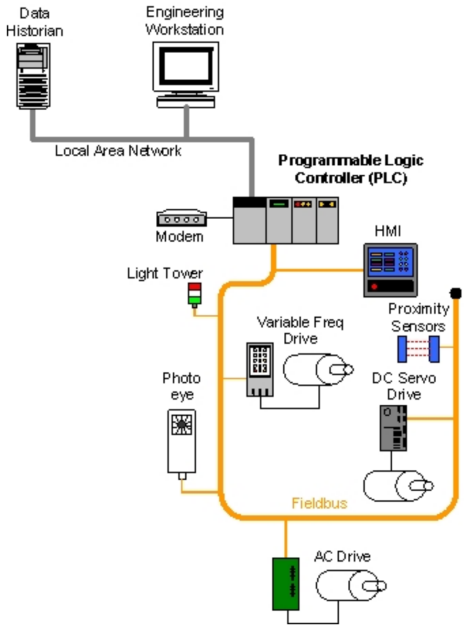
Beispiel: Topologie eines SCADA Systems 2



Beispiel: DCS



Beispiel: PLC



Vergleich: IT-Systeme vs. ICS

- Aufgrund der verschiedenen Einsatzszenarien gelten für ICS andere Anforderungen als für IT-Systeme
- Für IT-Systeme entwickelte Sicherheitsmechanismen lassen sich nicht einfach auf ICS übertragen
- Um Sicherheitsaspekte von ICS zu erörtern, ist die Kenntnis der Unterschiede von ICS im Vergleich zu IT-Systemen hilfreich

Systemleistung

IT-System:

- Keine Echtzeitanforderungen
- Hoher Datendurchsatz
- Delay und Jitter sind oft akzeptabel

Industrial Control System:

- Hohe Echtzeitanforderungen
- Reaktion auf Störungen ist zeitkritisch
- Moderater Datendurchsatz
- Hoher Delay und Jitter ist nicht akzeptabel

Verfügbarkeit

IT-System:

- Neustart des Systems ist akzeptabel
- Einschränkung der Verfügbarkeit über einen längeren Zeitraum ist tolerierbar
- Software Updates können im laufenden Betrieb eingespielt werden

Industrial Control System:

- Neustart des Systems gefährdet die Stabilität des Prozesses
- Systemausfälle sind nicht tolerierbar und müssen durch Redundanzen abgefangen werden
- Wartungsfenster müssen rechtzeitig geplant werden
- Vor Einspielen eines Updates muss die Software gründlich getestet werden

Risk Management

IT-System:

- Vertraulichkeit und Datenintegrität sind vorrangige Schutzziele
- Fehlertoleranz ist nicht entscheidend
- Risiken durch kurzfristige Downtime sind gering
- Risiko für den reibungslosen Ablauf von betriebswirtschaftlichen Prozessen

Industrial Control System:

- Sicherheit von Menschen und der Umwelt hat höchste Priorität
- Fehlertoleranz ist essentiell
- Risiken durch kurzfristige Downtime sind hoch
- Typische Risiken sind Umweltschäden, Gefährdungen von Menschen, Produktionsausfall oder Geldstrafen wegen Verletzung gesetzlicher Auflagen

Betriebssysteme

IT-System:

- IT-Systeme werden für den Einsatz von gängigen Betriebssystemen entworfen
- Gängige Betriebssysteme beinhalten standardisierte Sicherheitsmechanismen
- Updates werden automatisiert eingespielt

Industrial Control System:

- Betriebssysteme sind oft proprietäre auf die Hardware zugeschnittenen Spezialanfertigungen
- Oft fehlen Sicherheitsmechanismen oder sie sind unvollständig oder fehlerhaft implementiert
- Updates können nicht automatisiert eingespielt werden

Hardware Ausstattung

IT-System:

- Leistungsfähig
- Gute Ausstattung an Speicher und Festplatten
- Gute Konnektivität durch zahlreiche Schnittstellen

Industrial Control System:

- Auf den Produktionsprozess zugeschnittene Spezialanfertigungen
- Wenig Speicher und kleine Festplatten
- Keine „überflüssigen“ Schnittstellen
- Rechenleistung für kryptografische Zwecke oft nicht ausreichend

Kommunikation

IT-System:

- Einsatz standardisierter Protokolle und Mechanismen
- In der Regel kabelgebundene Netzwerke mit lokal angesiedelten Wireless LAN Knoten

Industrial Control System:

- Proprietäre Protokolle
- Großes Spektrum an Technologien (Satellit, Kabelmodem, Funk)
- Komplexe Netzwerkstrukturen

Change Management

IT-System:

- Automatisierte Bereitstellung von Software
- Regelmäßige automatisierte Updates
- Einsatz einer passenden Sicherheitsrichtlinie

Industrial Control System:

- Software muss vor dem Einsatz intensiv getestet werden
- Zum Einspielen der Software muss ein Wartungszeitfenster festgelegt werden
- Aufgrund von veralteten Betriebssystemen existieren oft keine Patches für Sicherheitslücken

Lebensdauer der Komponenten

IT-System:

- Größenordnung 3 bis 5 Jahre
- Defekte Systeme können leicht ersetzt werden

Industrial Control System:

- Größenordnung 15 bis 20 Jahre
- Ein defektes System muss durch ein baugleiches ersetzt werden

Wartbarkeit der Komponenten

IT-System:

- Die Komponenten eines IT-Systems sind leicht zugänglich
- Reparaturen können zeitnah durchgeführt werden
- Die durchgehende Standardisierung ermöglicht den Einsatz kompatibler Komponenten

Industrial Control System:

- Komponenten sind in der Regel schwer zugänglich
- Die Hardware besteht aus Spezialanfertigungen
- Zwecks Reparatur muss ein Wartungsfenster vereinbart werden

Zusammenfassung

- Industrial Control Systems steuern industrielle Anlagen verschiedenster Art
- Die an ICS gestellten Anforderungen unterscheiden sich an vielen Stellen zu den an herkömmliche IT-Systeme gestellten Anforderungen
- Die Konzeption und Implementierung von Sicherheitsmechanismen für ICS ist eine interdisziplinäre Aufgabe