
# Informationssicherheit

## Absicherung von Prozesssteuerungs- und Automatisierungssystemen

Durch die zunehmende Nutzung von modernen IT-Technologien in Automatisierungs- und Prozesssteuerungsumgebungen sind diese nun auch vermehrt konventionellen IT-Sicherheitsbedrohungen ausgesetzt. Da die genannten Systeme in der Regel zentrale Produktions- oder Versorgungsprozesse überwachen und steuern, können IT-Sicherheitsprobleme hier schnell weitreichende Folgen haben – von kostspieligen Produktionsausfällen in der herstellenden Industrie bis zu nachhaltig wirkenden Versorgungsengpässen und Störungen der öffentlichen Sicherheit bei kritischen Infrastrukturen.

Unabhängig von Industriebranche oder Anwendungsumfeld werden in heutigen Steuerungsumgebungen nahezu überall Softwaresysteme und Technologien der klassischen IT eingesetzt, wie z.B. Industrial Ethernet, TCP/IP und Betriebsysteme wie Linux, Unix oder Microsoft Windows. Aufgrund hoher Verfügbarkeitsanforderungen und der notwendigen, umfangreichen Tests ist es hier aber nur selten möglich, die zahlreichen Sicherheitslücken der Systeme zeitnah durch Security-Patches zu schließen. Ein zusätzliches Problem ist, dass Industrieprotokolle und Hardware-Komponenten wie SPSen oder Kommunikations-Gateways über keine eigenen Sicherheitsfunktionen verfügen, die wirksam vor unberechtigten Zugriffen oder anderen Angriffen schützen könnten. Während Prozessdatennetze bis vor wenigen Jahren komplett isoliert betrieben werden konnten, besteht heute in allen Branchen der Bedarf, zeitnah auf Daten aus der Automatisierungs- und Prozesswelt zuzugreifen oder Fernwartung zu ermöglichen. Deswegen entstehen immer mehr Schnittstellen zu Büronetzwerken, aber auch zu externen Systeme, z.B. von Dienstleistern oder Lieferanten.



Durch die Kombination dieser Probleme sind die Systeme mittlerweile durch vielfältige Sicherheitsbedrohungen gefährdet, wie z.B. Eindringen von Schadsoftware, Unachtsamkeit von Angestellten oder Zugriffe von Unbefugten. Die Absicherung von kritischen Steuerungs- und Automatisierungssystemen erfordert durchdachte und individuelle, auf die jeweilige Umgebung angepasste Konzepte und Strategien. Die GAI NetConsult verfügt hier über langjährige Erfahrung aus verschiedenen Industrie-Branchen und dem Versorgerumfeld und unterstützt Sie gerne in allen Projekt-Phasen.

Unser Leistungsangebot auf dem Gebiet der Absicherung von kritischen Automatisierungs-, Leit- und Steuerungssystemen deckt das gesamte Spektrum von Analyse, Test und Audit über Sicherheitskonzeption bis zur Sicherheitsorganisation ab.

### ☞ Analyse

- ☑ Erfassung der vorhandenen Systemarchitektur
- ☑ Durchführung von Schutzbedarfsfeststellungen
- ☑ Durchführung von Risikoanalysen
- ☑ Erstellung von Maßnahmenkatalogen für die Sicherheitsorganisation und -technik
- ☑ Entwurf von Sicherheitskonzepten

### ☞ Test und Audit

- ☑ Technische Sicherheitsüberprüfung von Systemen, Komponenten und Netzwerken
- ☑ Schwachstellensuche mit Scan- und Penetrationstests im Prozesssteuerungs- und Automatisierungsumfeld
- ☑ Sicherheitstests im Rahmen von Systemabnahme und Präqualifikation
- ☑ Organisatorische Audits auf Basis anerkannter Standards wie ISO/IEC 27001/27002 und IEC 62443

### ☞ Sicherheitskonzeption

- ☑ Technische Sicherheitsmaßnahmen
- ☑ Sichere Fernwartungs- und Datenkopplungslösungen
- ☑ Evaluierung, Auswahl und Einführung von Sicherheitsprodukten unter besonderer Berücksichtigung industrieller Anforderungen
- ☑ Beratung zu Sicherheitsfragen beim Systemdesign
- ☑ Definition von Sicherheitsvorgaben bei Systembeschaffungen und Ausschreibungen

### ☞ Sicherheitsorganisation

- ☑ Aufbau von Information Security Managementsystemen (ISMS) im Prozess- und Produktionsumfeld
- ☑ Konzepte zur Betriebsorganisation
- ☑ Erstellung von Sicherheitsrichtlinien und Standards unter Beachtung branchenspezifischer Besonderheiten
- ☑ Unterstützung beim Aufbau der IT-Notfallplanung

GAI NetConsult GmbH, Am Borsigturm 58, D-13507 Berlin, Tel: 030-417 898-0, Fax: 030-417 898-300
E-Mail: vertrieb@gai-netconsult.de Internet: http://www.gai-netconsult.de