SAE IT-systems

Member of LACROIX Group

IT-Sicherheit
in der Fernwirktechnik

Warum Sicherheit jetzt wichtiger ist als früher

Koordinierte Cyberangriffe auf Stationstechnik sind heute nicht mehr nur konstruierte Schreckensszenarien, sondern bereits Teil unserer Realität. Für die Versorgungsnetzbetreiber birgt diese Gefahr enorme Risiken sowohl für die Versorgungsstabilität - und den möglicherweise damit verbundenen Schadenersatzansprüchen - als auch für die öffentliche Reputation: wichtige Gründe, sich lieber heute als morgen mit dem Thema IT-Sicherheit zu beschäftigen.

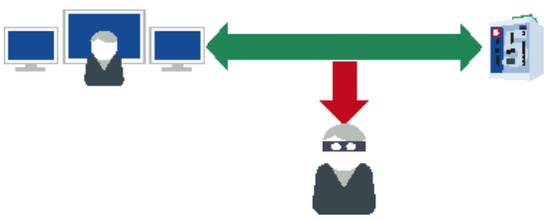
Doch was bedeutet das konkret? Ein optimal geschütztes System wahrt die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten und Informationen und verhindert ungewollte Eingriffe. Die Herausforderungen, denen sich IT-Experten dabei in den Weg stellen, wachsen kontinuierlich. Die Angreifer werden immer professioneller, gesetzliche Vorgaben immer spezifischer und last but not least, müssen verschiedene Interessengruppen berücksichtigt werden: Trotz der notwendigen Sicherheitssteigerung, darf beispielsweise die Praktikabilität der Systeme für das Bedien- und Wartungspersonal nicht in Vergessenheit geraten.

Im Idealzustand basiert eine Versorgungsanlage also auf einer Netzwerkinfrastruktur, die sowohl sichere Verbindungen mit starken Verschlüsselungen erlaubt, als auch hohe Funktionalität und Komfort für die Anwendungen des Tagesgeschäftes bietet. Eine zukunftssichere Infrastruktur benötigt zudem die Möglichkeit zur kontinuierlichen und detaillierten Überwachung, um Risiken identifizieren und Schutzmaßnahmen ableiten zu können. Die praxisorientierte Lösung dieser Herausforderung kann daher nur ein ganzheitliches Sicherheitskonzept sein, welches kontinuierliche Weiterentwicklungen und Aktualisierungen ermöglicht.

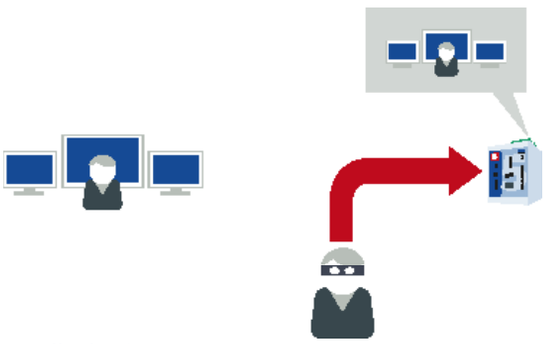
Grundbegriffe der IT-Sicherheit

Um ein grundlegendes Verständnis für die unterschiedlichen Bedrohungsszenarien im Hinbklick auf die IT-Sicherheit zu erhalten, sollten die wesentlichen Grundbegriffe erläutert werden. Vier Aspekte sind hierbei entscheidend:

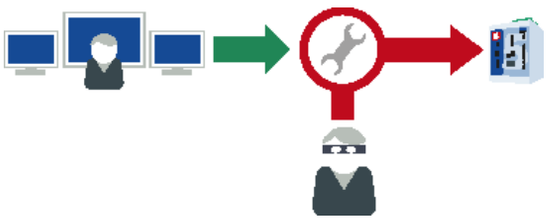
1. **Vertraulichkeit**
   Niemand der unbefugt ist, darf die Daten lesen
2. **Integrität**
   Unbefugte dürfen die Daten nicht verändern
3. **Authentizität**
   Die Daten stammen wirklich von der angenommenen Quelle
4. **Verfügbarkeit**
   Der Zugriff auf die Daten muss für Befugte gewährleistet sein



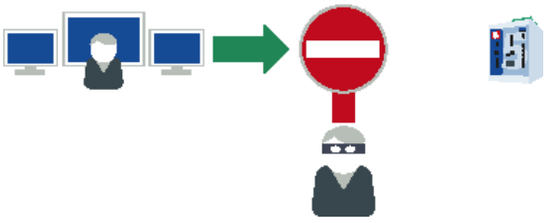
Angriff auf Vertraulichkeit



Angriff auf Authentizität



Angriff auf Integrietät



Angriff auf Verfügbarkeit

Leistungsstarke Hardware - series5e

Die Produktfamilie series5e stellt sich den komplexen Sicherheits- und Praxisanforderungen von heute und morgen gekonnt entgegen. Die kontinuierlich steigenden Anforderungen an IT-Sicherheitsmaßnahmen führen zu einem deutlich gewachsenen Leistungsbedarf der Komponenten. Jedes net-line Produkt der neuen series5e Technologie bietet dank des 32-Bit RISC Prozessors mit Gleitkommaeinheit (Floating Point Unit) und des 1 GB Speichers noch mehr Performance: Mit 1.200 MIPS läuft die Hardware mit dreifacher Leistung im Vergleich zur Vorgängergeneration series5+. Die gesteigerte Performance wirkt sich insbesondere in der Netzwerkkommunikation via IEC 61850 und in der Prozesspunktbehandlung nach IEC 60870-5-10x Standards positiv aus und ermöglicht darüber hinaus die Nutzung modernster Verschlüsselungsalgorithmen. Das Gesamtsystem wurde auf einen modernen Linux-Kernel aufgesetzt, der insbesondere mit Hinblick auf IT-Sicherheit mehr Flexibilität und eine bessere Wartbarkeit der Firmware erlaubt.

Auf Herz und Nieren

Um die Wirksamkeit unserer kontinuierlichen Weiterentwicklungen im Bereich der IT-Sicherheit zu verifizieren, lassen wir unsere Fernwirksysteme in regelmäßigen Abständen auch von externen Spezialisten prüfen. Zuletzt wurde eine Prüfung auf Einhaltung der Anforderungen des BDEW Whitepapers durch die GAI NetConsult GmbH durchgeführt. Das Ergebnis:

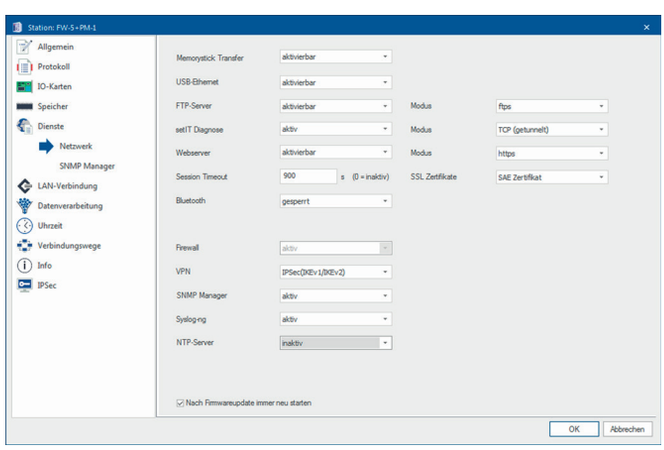
„Aus Sicht der IT-Sicherheit bestehen für die geprüften Geräte in der untersuchten Konfiguration keine Bedenken für den produktiven Einsatz in Netzen mit erhöhtem Sicherheitsbedarf.“

FW-5-GATE-4G mit series5e Technologie

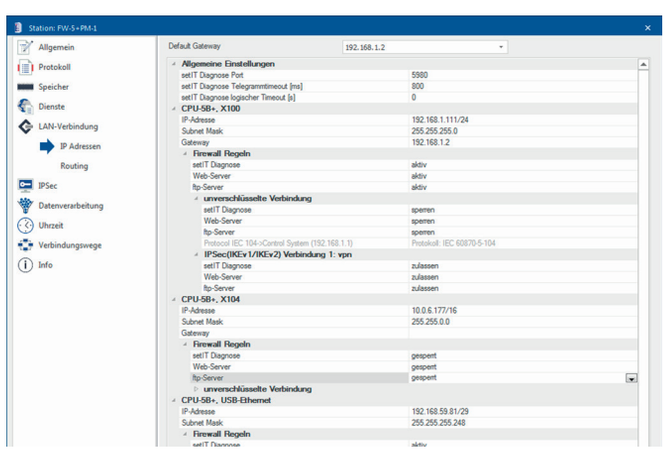
Ein Herz für Praktiker - Parametriersoftware setIT

In die Bedienoberfläche unserer Parametriersoftware setIT wurden erweiterte Sicherheitsfunktionen nahtlos eingearbeitet:

- In den Defaulteinstellungen neuer Stationen sind jetzt standardmäßig die sicheren Protokolle FTPs/HTTPs voreingestellt
- Benutzerverwaltung mit individueller Rechtezuweisung (Role Based Access Control)
- Zugriffe auf Servicefunktionen in der Station können über einen Systembefehl aus der Leitstelle temporär aktiviert werden
- Die Stationskonfiguration kann mit einem projektspezifisches Systempasswort verschlüsselt werden
- VPN-Verschlüsselung über IPsec mit IKEv2
- Das neue Datenbankformat .sdbx ermöglicht die Verschlüsselung der gesamten Projektdatenbank
- Einfache Definition von erweiterten Firewallregeln: Dienste sind granular aktivierbar und auf verschiedene Netzwerkschnittstellen begrenzbar
- Anzahl der möglichen Prozesspunkte für FW-5000, FW-50 und BCU-50 auf 20.000 erhöht (series5e)
- Zentrale Erfassung von sicherheitsrelevanten Betriebsereignissen mit SYSLOG
- Back-up-Funktion mit frei wählbarem Speicherort zur Sicherung der Konfigurationsdaten



Auswahl der Dienste und Funktionen in setIT



Firewall mit Verbindungseinstellungen über VPN in setIT

Umfassende Dienstleistungen aus dem Bereich der IT-Sicherheit

SAE bietet neben anforderungsorientierten Hard- und Softwareprodukten auch alle wichtigen Dienstleistungen von der Projektplanung bis zur Inbetriebnahme der Anlage an. Da die IT-Sicherheit eine ganzheitliche Betrachtung aller Komponenten, Prozesse und Rahmenbedingungen eines Systems bedarf, ist insbesondere unsere sicherheitsbezogene Beratung im Vorfeld eines Projektes eine effektive und effiziente Investition. Folgende Themenkomplexe werden hierbei typischerweise beleuchtet:

- Übergeordnete, konzeptionelle Beratung
  Fragen in diesem Zusammenhang:
  - Wie kann ein Netzwerk sinnvoll geplant und aufgebaut werden?
  - Wie harmonieren Maßnahmen im Netzwerk mit Maßnahmen, die außerhalb des Netzwerkes getroffen werden?
  - Wie wird eine Zugriffsbeschränkungen eingerichtet?
  - Wie sollten Netzwerke segmentiert werden?
  - Wie wird die Anbindung zur Leitstelle gesichert?
- Beratung zu konkreten Sicherheitsmechanismen unserer Technik
  Klärung spezifischer Fragen, zum Beispiel:
  - Wie bzw. wie stark kann die Verschlüsselung eingestellt werden?
  - Welche Übertragungsprozeduren oder Verschlüsselungsalgorithmen werden unterstützt?
  - Wie funktioniert die Firewall in den Geräten?
  - Wie kann die Vergabe sicherer Kennwörter gewährleistet werden?
- Wie kann ein vernünftiger Weg zwischen Usability und Sicherheit gefunden werden?

Besonders die letzte Frage stellt unsere Kunden vor große Herausforderungen und kann nur individuell beantwortet werden. Früher lag das Hauptaugenmerk auf der Funktion, Sicherheitsfragen waren eher sekundär. Heute muss Funktion, Handhabung und Sicherheit in einem vernünftigen Verhältnis zueinander stehen – unter Berücksichtigung der gesetzlichen Vorgaben, der Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der aktuellen Gefährdungslage.

Welche Rolle spielt Fernwirktechnik in Bezug auf die Sicherheit Ihrer Netzwerkinfrastruktur

Fernwirk- und Stationsleittechnik sitzt in der Regel an zentralen Punkten des Kommunikationsnetzwerkes. Die Geräte besitzen verschiedene Schnittstellen zu anderen Diensten und Herstellern, zu unterschiedlichen Komponenten sowie zum physikalischen Prozess. Die Übertragung findet häufig auch zu verschiedenen Leistellen mehrerer Betreiber statt. Fernwirktechnik ist daher immer Teil eines Gesamtsystems.
Für die IT-Sicherheit gilt: *„Die Kette ist nur so stark wie ihr schwächstes Glied.“*
Hieraus lassen sich zwei zentrale Herausforderungen ableiten:

1. Es muss immer das gesamte Netz mit all seinen Komponenten, physikalischen Gegebenheiten und Prozessen im Betrieb betrachtet werden.
2. Jede einzelne Komponente (auch die Fernwirktechnik) muss dem gewünschten Sicherheitslevel genügen.

Mit diesen Anforderungen im Fokus entwickeln wir unsere Hardware, unsere Software sowie die dazugehörigen Dienstleistungen kontinuierlich weiter, um unseren Kunden sichere und praxistaugliche Lösungen bereitstellen zu können.

Informationssicherheit: ISMS & ISO 27001 Zertifizierung

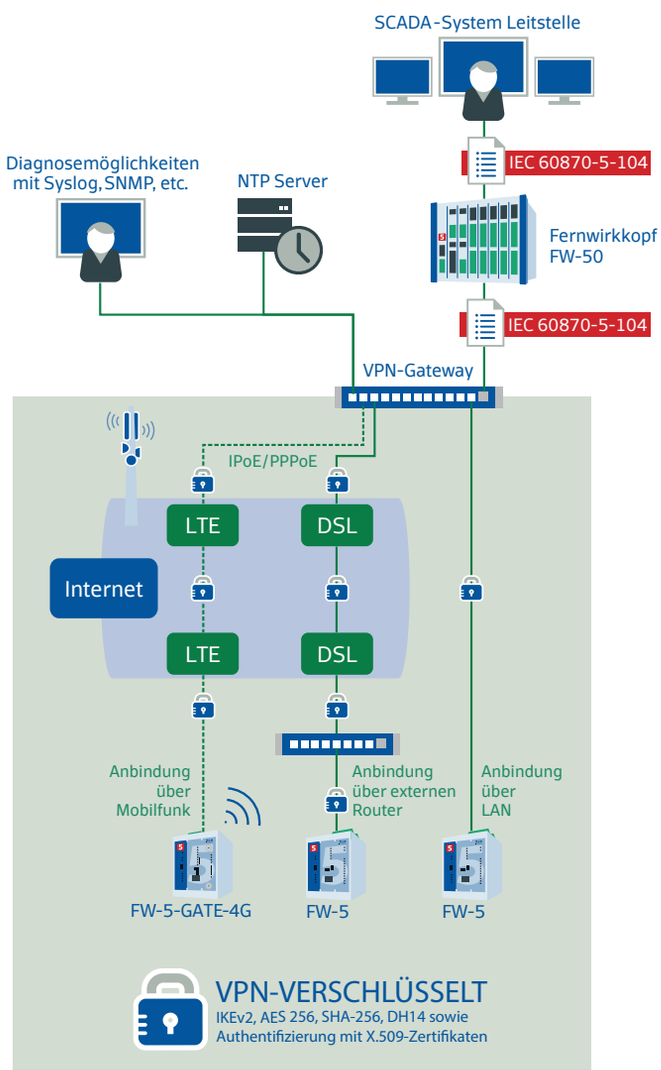
Als Lieferant für Betreiber kritischer Infrastrukturen sind wir uns unserer Verantwortung in Bezug auf die Informationssicherheit bewusst. Zur Anhebung des Sicherheitsniveaus in unseren Prozessen haben wir uns dazu entschieden, einen Informationssicherheitsbeauftragten zu bestellen, welcher in Zusammenarbeit mit externen Sicherheitsexperten die Anforderungen für eine Zertifizierung gemäß ISO 27001 umsetzt.
Unser Informationssicherheitsexperte Markus Dewerny arbeitet seit 2002 bei SAE IT-systems – vorher war er selbst Kunde. Als ehemaliger Projekteur kennt er nicht nur die Systeme und Technik, sondern auch die Anliegen und Probleme der Kunden aus erster Hand. Nach der Fortbildung zum IT-Security Coordinator (IHK) und Security Manager (EBS) übernahm er 2017 die Position des Informationssicherheitsbeauftragten bei SAE und hält den Dialog mit Kunden, Partnern und Lieferanten in Fragen der Informationssicherheit und des Datenschutzes. Weiterhin entwirft er unternehmensinterne Richtlinien, führt die Risikoanalysen im Bereich der Informationssicherheit durch und koordiniert die daraus resultieren Maßnahmen.

Systemautonomie und Transparenz

In einem von fremden Diensten abhängigen Netzwerk liegt die Netzwerksicherheit nicht vollständig in der eigenen Hand. Wer die Abhängigkeiten reduziert, erhöht nicht nur die Autonomie des Netzwerkes, sondern auch dessen Sicherheit. Eine clevere Lösung: die Verwendung eines hausinternen NTP-Servers zur Zeitsynchronisierung als Alternative zu einem Internetdienst. Außerdem sieht unser Anbindungskonzept die kontinuierliche und detaillierte Überwachung der Netzwerkinfrastruktur in Bezug auf Stabilitätsveränderungen, Zugriffe und Zugriffsversuche vor: Hierzu sendet die Fernwirktechnik relevante Daten an einen Syslog-Server, der die zentrale Erfassung von Betriebsereignissen vieler Stationen sowie die Auswertung dieser Meldungen ermöglicht. Je nach Art und Ausstattung des Syslog-Servers können Alarme generiert werden, die zum Beispiel eine hohe Anzahl an fehlerhaften Passworteingaben, ein Update außerhalb der Betriebszeiten oder sonstige ungewöhnliche Vorgänge melden. Über diese Beobachtungen können die Ursachen für aktuelle Stabilitätsschwankungen abgeleitet und potentielle Gefahren frühzeitig erkannt werden.

Anbindungsmöglichkeiten für die Fernwirktechnik

Unser Anbindungskonzept empfiehlt ein VPN-Gateway als verbindende Komponente. Es ermöglicht die zentrale Steuerung vieler Stationen über nur einen Fernwirkkopf. Unsere Fernwirkkomponenten erlauben verschiedene Anbindungstechniken, wie beispielweise die Nutzung eines beliebigen Internetanschlusses, eines externen Routers sowie die Anbindung über Mobilfunk oder LAN. Zudem empfehlen wir redundante Anbindungen zur Sicherung der Verbindung. Wir konzipieren Lösungen für Versorgungsnetzbetreiber mit unterschiedlichen Anforderungen – daher lassen sich auch hardwareseitig verschiedene Produkte in das Sicherheitskonzept integrieren: beispielsweise die hier dargestellten Feldgerätetypen net-line FW-5, net-line FW-50 sowie das net-line FW-5-GATE-4G. Dank der series5e Technologie wurden diese Produkte auf eine neue, zukunftssichere Plattform gestellt.



Anbindungskonzept - Flexible und sichere Einbindung von Fernwirktechnik

VPN, Verschlüsselung und Firewall

Eine sichere Verbindung benötigt ein sicheres VPN-Verschlüsselungsprotokoll sowie einen Mechanismus zum Schlüsselaustausch. IPsec kann in der Parametriersoftware setIT sowohl auf Protokollversion 1 (IKEv1) als auch auf der in RFC4306 beschriebenen Protokollversion 2 (IKEv2) aktiviert werden. Doch nicht nur die Stationen vor Ort sollten vor externen Zugriffen jeglicher Art geschützt werden, sondern auch die Konfigurationsdatenbank selbst. Das neue Datenbankformat .sdbx ermöglicht die Verschlüsselung der gesamten Projektdatei mit dem sicheren AES-256 Algorithmus – diese Verschlüsselung wird auch in der Richtlinie TR-02102 (kryptographische Verfahren) vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen. setIT erlaubt zudem die Festlegung von erweiterten Firewallregeln: Bestimmte Dienste sind sowohl aktivierbar als auch auf verschiedene Schnittstellen begrenzbar. Es können auch gezielt Einstellungen vorgenommen werden, die mehr Flexibilität ermöglichen. Zusammenfassend erlaubt unser Konzept vielfältige und abgesicherte Anbindungsmöglichkeiten per VPN und ein hohes Maß an Funktionalität. Die Sicherheit unserer Kunden und der Versorgungsnetze hat uns dazu angespornt, unser Angebotsportfolio um eine sicherheitsbezogene Beratung bezogen auf die Integration unserer Produkte zu ergänzen und dieses sicherheitsoptimierte Anbindungskonzept zu entwickeln.

IT-systems

Member of LACROIX Group

SAE IT-systems GmbH & Co. KG
Im Gewerbegebiet Pesch 14
50767 Köln (Cologne, Germany)
Tel.: +49(0)221/59 808-0
Fax: +49(0)221/59 808-60
info@sae-it.de
www.sae-it.com