SAUTER
Für Lebensräume mit Zukunft.

33. GLT Anwendertagung FM
Lüneburg · 25. – 27.09.2019

Sicherheit in der GA

… aus Sicht der Hersteller

Dr. Andreas Wetzel, Leiter Gebäudeautomation, SAUTER Deutschland

Aktuelles Bedrohungsbeispiel aus den Medien (Feb. 2019)

SAUTER
Für Lebensräume mit Zukunft.

Auszug faz.net vom 17.02.2019

- Nicht direkt Gebäudeautomation im Focus, hier der Bereich „kritische Infrastruktur" KRITIS
- Gebäudeautomation auch bei Flughäfen, Bahnhöfen, Banken, Krankenhäusern, Universitäten …
- Es kann jeden „treffen"…

Die Lage der IT Sicherheit in Deutschland 2018

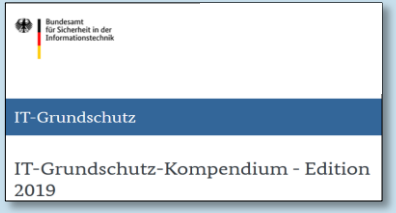
SAUTER
Für Lebensräume mit Zukunft.

…
Die **Gefährdungslage ist weiterhin hoch**. Im Vergleich zum vorangegangen Berichtszeitraum hat sie sich weiter verschärft und ist zudem vielschichtiger geworden. Es gibt nach wie vor eine hohe Dynamik der Angreifer bei der **Weiterentwicklung von Schad-programmen und Angriffswegen**. Darüber hinaus gibt es z. B. mit den entdeckten Schwachstellen in Hardware eine neue Qualität der Bedrohung, wie bei den Sicherheitslücken Spectre/Meltdown und Spectre NG, die ohne einen Austausch der Hardware nicht vollständig geschlossen werden können.
100%ige Sicherheit gibt es nicht.
…

(Auszug)

BSI: IT Grundschutz

- Allgemeiner und aktueller Überblick über IT-Anforderungen und Bedrohungen
- Bisher: 94 veröffentlichte Bausteine (Stand 01.03.2019)



Bausteine des IT Grundschutz:

ISMS: Sicherheitsmanagement
ORP: Organisation und Personal
CON: Konzeption und Vorgehensweisen
OPS: Betrieb
DER: Detektion und Reaktion
APP: Anwendungen
SYS: IT-Systeme
IND: **Industrielle IT**
NET: Netze und Kommunikation
INF: Infrastruktur

IND.1 Betriebs- und Steuerungstechnik
IND.2.1 Allgemeine ICS-Komponente
IND.2.2 **Speicherprogrammierbare Steuerung (SPS)**
IND.2.3 Sensoren und Aktoren
IND.2.4 Maschine
IND.2.7 Safety Instrumented Systems

BSI: IT Grundschutz: IND.2.2 Speicherprogrammierbare Steuerung (SPS)

SAUTER
Für Lebensräume mit Zukunft.

1.1 Einleitung

Eine speicherprogrammierbare Steuerung (SPS, engl. Programmable Logic Controller, PLC) ist eine ICS-Komponente. Sie **übernimmt Steuerungs- und Regelaufgaben** in der Betriebstechnik (engl. Operational Technology, OT). Die Grenzen zwischen verschiedenen Geräteklassen und Bauformen sind heute fließend: So kann z.B. auch ein Fernwirkgerät (engl. Remote Terminal Unit, RTU) die Funktionen einer SPS übernehmen oder ein Programmable Automation Controller (PAC) kann versuchen, die Vorteile einer SPS und eines Industrie-PCs zu vereinen. Jedoch ist die SPS immer noch **das klassische Automatisierungsgerät**, sodass in diesem Baustein diese Begriffe synonym verwendet werden.

Eine SPS verfügt über digitale **Ein- und Ausgänge**, ein Echtzeitbetriebssystem (Firmware) sowie weitere Schnittstellen für Ethernet oder **Feldbusse**. Die **Verbindung zu Sensoren und Aktoren** erfolgt über die analogen oder digitalen Ein- bzw. Ausgänge oder über einen Feldbus. Die Kommunikation mit **Prozessleitsystemen** findet meist über die Ethernet-Schnittstelle und **IP-basierte Netze** statt.

(Auszug)

Bedrohungen für IT-Systeme

SAUTER
Für Lebensräume mit Zukunft.

Für IT-Systeme existieren eine Vielzahl möglicher Bedrohungen, die im Rahmen der **Risiko- und Schwachstellenanalyse** identifiziert, erfasst und bewertet werden.

Mögliche Bedrohungen sind:

- Diebstahl von Benutzerkennungen
- Unbefugter Zugriff auf Systeme
- Unbefugter Zugriff auf Daten
- Diebstahl oder Manipulation von Daten
- Manipulation von Systemen
- Störung der Verfügbarkeit von Systemen
- Angriffe durch Malware
- Angriffe durch Denial of Service Attacken
- …

… auch in der Gebäudeautomation, da hier vielfach diese IT Techniken verwendet werden

Schadprogramme / Maleware
(exemplarisch)

SAUTER
Für Lebensräume mit Zukunft.

- Viren und Würmer

Befall von Software mit Schadcode die eigene Aktionen ausführen und sich selbst kopieren/verbreiten

- Ransomware

Schadprogramm, welches den Zugriff auf Daten und Systeme einschränkt. Freigabe bei Lösegeld (engl. Ransom)

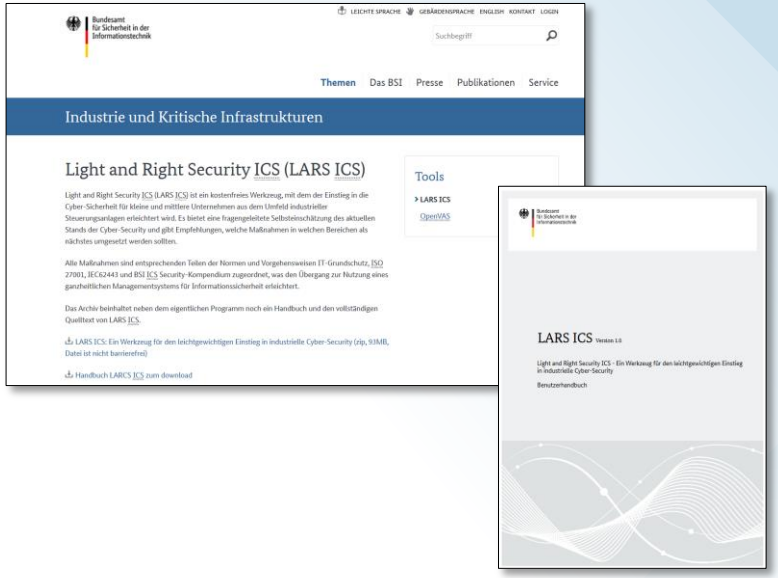
- Trojaner

Als nützliche Software getarntes Schadprogramm. z.B. für Bots zum „Fernsteuern“ für DoS Attacken.

- Spyware

Schadprogramme mit dem Ziel des Ausspionierens und der Weitergabe von Nutzerdaten

Risiko- und Schwachstellenanalyse



https://www.bsi.bund.de/DE/Themen/ICS/Tools/LarsICS/LarsICS.html

Erforderlich ist eine projektspezifische Bewertung der IT-Sicherheit der Gebäudeautomation.

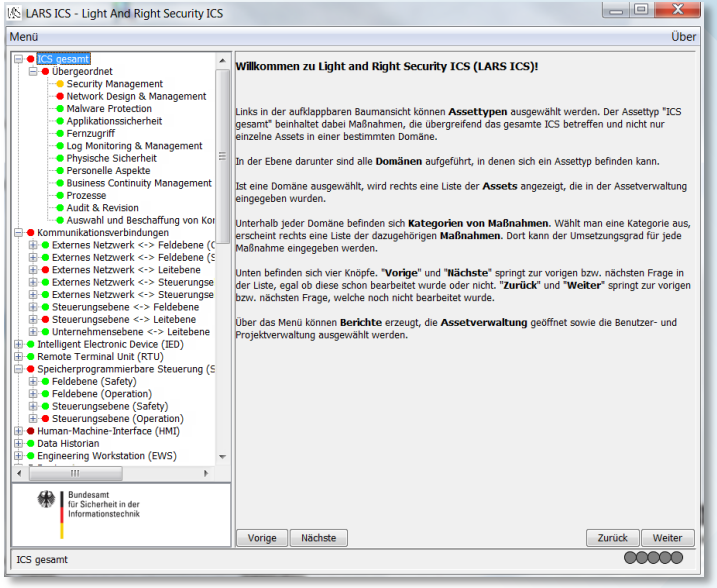
Mögliches Hilfsmittel gemäß VDMA EB 24774:

BSI „**LARS**“ Tool

(LARS: Light and Right Security ICS)

LARS ICS: Überblick

SAUTER
Für Lebensräume mit Zukunft.



- Vollständiger Überblick über gebäudespezifische IT Funktionalität
- Erforderliche Bereiche werden bzgl. Secutity 5-stufig farblich bewertet
- Geführte Bearbeitung durch die einzelnen Themen (voriges/nächstes)
- Integrierte Berichtsfunktionalität
- (LARS nicht speziell für GA konzipiert, daher einige Unterpunkte, die für GA nicht erforderlich wären. Dennoch:)
- Gute Möglichkeit zur Aufnahme der IT Sicherheit in der Gebäudeautomation
- Identifikation möglicher Schwachstellen

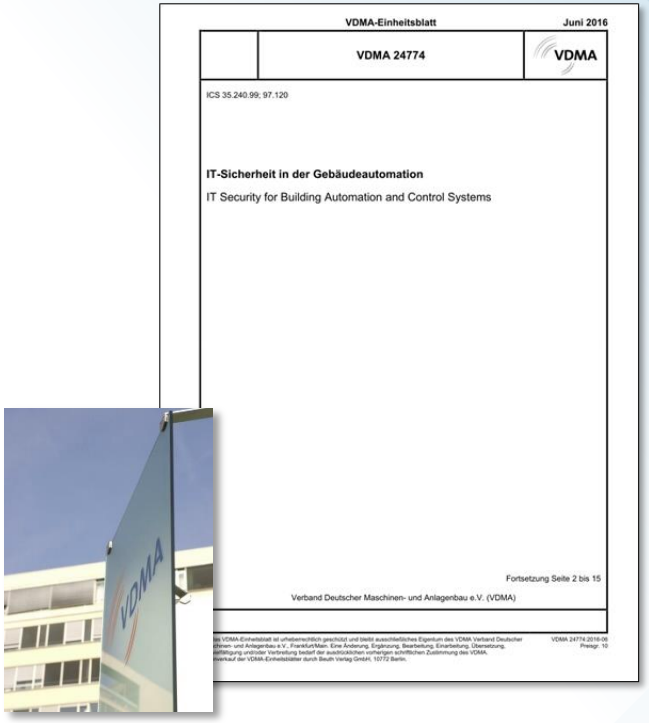
SAUTER
Für Lebensräume mit Zukunft.

- Zusätzliche Planung der IT Sicherheit über den Gebäudelebenszyklus
  - Bei der Ausschreibung (Definition der IT Sicherheit & Produktanforderungen)
  - Bei der Produkt-/Herstellerauswahl
  - Bei der Inbetriebnahme (projektspezifische Einstellungen)
  - Beim Betrieb (Backups, Authentifizierung)
  - Bei der Wartung (Updates/Upgrades/ Patches)

- IT- Sicherheit benötigt
  - Ressourcen / Zeit
  - Investition / Geld
  - KnowHow / Arbeitsanweisungen
  - Zugangs- / Zugriffseinschränkungen

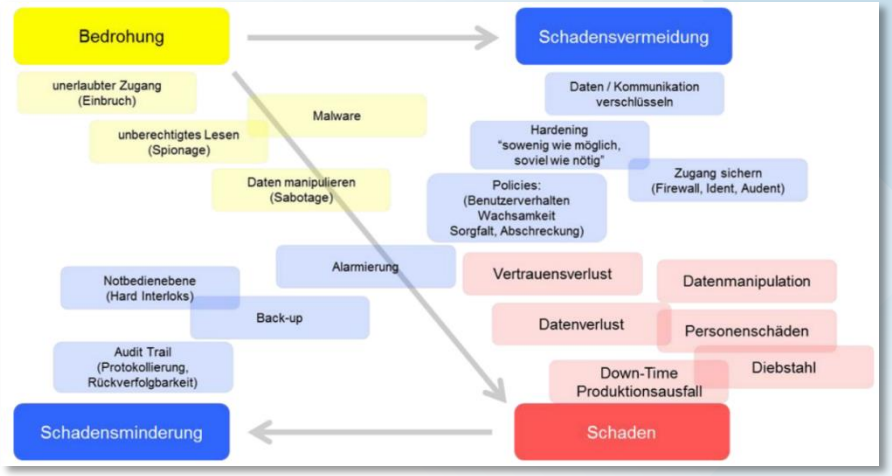
- Es kann jeden „treffen“…

VDMA Einheitsblatt 24774



- Das VDMA EB 24774 von 2016 definiert IT Sicherheitsanforderungen in der Gebäudeautomation.
- Zusammenarbeit mit VDMA Bereich Industrial Security und dem BSI
- Im VDMA arbeitet die Arbeitsgruppe „IT Sicherheit in der Gebäudeautomation“ weiter, um das Einheitsblatt auf einem aktuellen Stand zu halten
- Treffen in 2017 und 2018
- Überarbeitete Version des VDMA Einheitsblatt 24774 für 2019 erwartet
- Integration von erforderlichen IT-Sicherheitsanforderungen in das VDMA EB 24186-4 (Leistungsprogramm für die Wartung von technischen Anlagen und Ausrüstung in Gebäuden)

VDMA Einheitsblatt 24774



Auszug Vorwort:

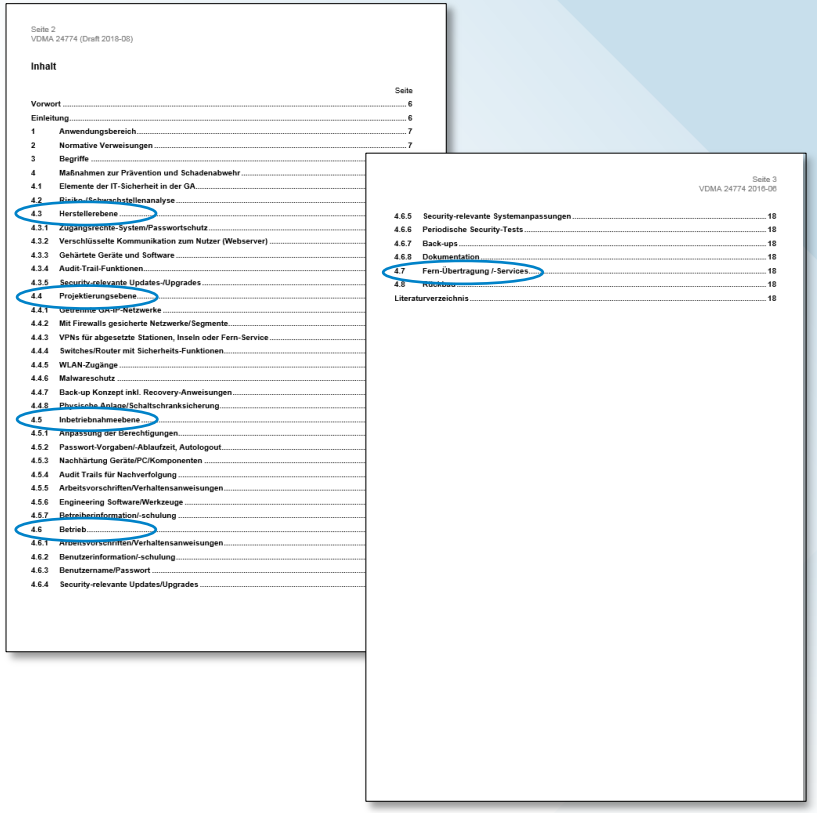
„Das VDMA-Einheitsblatt soll Planer, Errichter und Betreiber dabei unterstützen Maßnahmen für IT-Sicherheit von neuen oder schon errichteten GA-Systemen umzusetzen. Dies betrifft den gesamten Lebenszyklus, inklusive Wartung, Service und Rückbau.

Das VDMA-Einheitsblatt soll dabei helfen die **Bedrohung durch Cyberangriffe zu erkennen, zu vermeiden oder deren Auswirkung zu minimieren**. …“

Bedrohung ↔ Gegenmaßnahmen
reagieren ↔ agieren

VDMA Einheitsblatt 24774

SAUTER
Für Lebensräume mit Zukunft.



Seite 2
VDMA 24774 (Draft 2018-08)

Inhalt

Seite 3
VDMA 24774 2016-06

Verantwortlichkeiten für IT Sicherheit in der GA:

- Hersteller
- Projektierung
- Inbetriebnahme
- Betrieb
- Fernservice

Ziel:

Projektspezifisches IT Sicherheitskonzept für die GA

SAUTER
Für Lebensräume mit Zukunft.

Die Anforderungen der **IT Sicherheit** in der Gebäudeautomation sind relevant für **kommunikationsfähige Geräte**, die an ein Netzwerk angeschlossen sind:

- Automationsstationen
- Raumcontroller
- Gateways
- Intelligente bzw. kommunikative Sensoren
- Touch Panel (mit GA Kommunikationsschnittstelle) …

sowie die **Software** für die Management-Ebene:

- MBE Software
- Energieanalyse- und Energiemanagementsoftware
- Sowie deren Hardware und Softwareinfrastruktur (Betriebssysteme, SQL-DB, Anti-Virenprogramme, …)

weniger betroffen sind Engineering-Softwaretools
(zeitlich beschränkt und selbst eingesetzt durch GA-Hersteller und Anlagenbauer)

VDMA Einheitsblatt 24774: **Herstellerebene**

SAUTER
Für Lebensräume mit Zukunft.

Aktuelle Hardwareplattformen und embedded Betriebssysteme

- Funktionalität durch Hersteller (Lebensdauer der Produktfamilien bei Herstellern und Einsatz der Produkte in den GA Projekten)

Gehärtete Geräte und Software

- Funktionalität durch Hersteller
- (interne QS, Abschalten nicht benötigter Funktionen und Dienste, Dokumentation verwendeter Funktionen und Dienste)

Verschlüsselte Kommunikation

- Funktionalität durch Hersteller
- z.B. https, SFTP, KNX secure, BACnet/SC

Security-relevante Updates-/ Upgrades

- Funktionalität durch Hersteller
- Nutzen bei Betrieb (ggf. über Wartungsverträge SW / DL)

SAUTER
Für Lebensräume mit Zukunft.

Zugangsrechte / Passwortschutz

- Funktionalität durch Hersteller (AS, MBE, Projektierung: konfigurierbar, Mindestanforderungen)
- Einrichten bei Inbetriebnahme
- Nutzen bei Betrieb

Getrennte Netzwerke

- Physikalisch: Funktionalität durch Hersteller
- Logisch: Einrichten bei Inbetriebnahme

Aufzeichnen der Benutzeraktivitäten

- Funktionalität Audittrail durch Hersteller (AS und MBE)
- Nutzen bei Betrieb

Lokale Vorrangbedienebene

- Funktionalität durch Hersteller (Manueller Betrieb im Schadensfall)
- Einrichten bei Inbetriebnahme
- Nutzen bei Betrieb

SAUTER
Für Lebensräume mit Zukunft.

Backup-/Restore Funktionalität

- Funktionalität durch Hersteller
  (Backup gesamter AS und MBE Projektierung.
  MBE DB via IT Tools)
- Inbetriebnahme Backup-Strategie
  (Einrichten und Ablegen)
- Nutzen bei Betrieb
  (Aktualisieren)

Integrierte Firewall

- Funktionalität durch Hersteller in AS
- Einrichten bei AS Inbetriebnahme
- Einrichten in PC Umgebung bei Inbetriebnahme

SAUTER
Für Lebensräume mit Zukunft.

GENERAL	IEC 62443-1-1 (Ed. 2) Terminology, concepts and models	IEC/TR 62443-1-2 Master glossary of terms and abbreviations	IEC/TS 62443-1-3 System security compliance metrics	IEC/TR 62443-1-4 IACS security lifecycle and use-case
POLICIES & PROCEDURES	IEC 62443-2-1 (Ed. 2) Requirements for an IACS security management system	IEC/TR 62443-2-2 Implementation guidance for an IACS security management system	IEC/TR 62443-2-3 Patch management in the IACS environment	IEC/ 62443-2-4 Installation and maintenance requirements for IACS suppliers
SYSTEM	IEC/TR 62443-3-1 Security technologies for IACS	IEC 62443-3-2 Security levels for zones and conduits	IEC 62443-3-3 System security requirements and security levels	
COMPONENT	IEC 62443-4-1 Product development requirements	IEC 62443-4-2 Technical security requirements for IACS components		

IEC 62443:

komplette Normreihe mit

- Entwicklungsanforderungen im Teil 4-1
- Hardwareanforderungen im Teil -3-3 und -4-2
- Inbetriebnahme im Teil -2-1 / -2-4 und -3-3
- Betrieb im Teil -2-1 und -2-4
- Wartung im Teil -2-3 und -2-4

SAUTER
Für Lebensräume mit Zukunft.

IEC 62443-3

» Der Standard IEC 62443-3 definiert «Systemsicherheitsanforderungen und Sicherheitsstufen» für IACS (Industrial Automation and Control Systems).
» Die definierten Sicherheitsstufen richten sich nach der Kompetenz, der Motivation und den verfügbaren Mitteln eines potentiellen Angreifers:

Stufe 4
» Schutz vor vorsätzlichen Verstössen mit ausgeklügelten Mitteln mit erweiterten Ressourcen, IACS-spezifischen Fähigkeiten und hoher Motivation.

Stufe 3
» Schutz vor vorsätzlichen Verstössen mit ausgeklügelten Mitteln mit moderaten Ressourcen, IACS-spezifischen Fähigkeiten und moderater Motivation.

Stufe 2
» Schutz vor vorsätzlicher Verletzung mit einfachen Mitteln mit geringen Ressourcen, generischen Fähigkeiten und geringer Motivation.

Stufe 1
» Schutz vor unbeabsichtigten oder zufälligen Verstössen

SL 4

SL 3

SL 2

SL 1

SL 0: 72 (Grund-) Anforderungen
SL 4: bis zu 123 Anforderungen

IEC 62443-3-3 Relevante Basisanforderungen

Nr.	Kürzel	Kategorie
FR 1	IAC	Identifizierung und Authentifizierung
FR 2	UC	Nutzungskontrolle
FR 3	SI	Systemintegrität
FR 4	DC	Vertraulichkeit der Daten
FR 5	RDF	Eingeschränkter Datenfluss
FR 6	TRE	Rechtzeitige Reaktion auf Ereignisse
FR 7	RA	Verfügbarkeit der Ressourcen

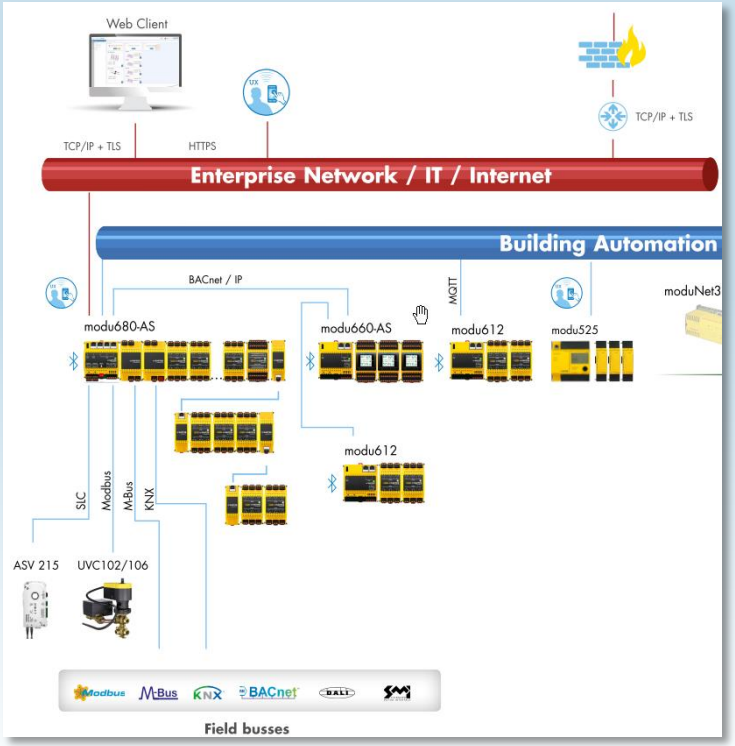
FR 5 – Restricted data flow (RDF)	
SR 5.1 Network segmentation **"The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks."**	Depending on the size of your network, it may be necessary to do network segmentation. For this, the appropriate components for network management shall be used. modu680-AS provides two different network interfaces, thus allowing a firs network segmentation. The Building automation Network and the BACnet Protocol is supported over the LAN ports, while it is not over the WAN port.

FR 5 – Restricted data flow (RDF)	SL-1	SL-2	SL-3	SL-4
SR 5.1 Network segmentation	☑	☑	☑	☑
SR 5.1 RE 1 Physical network segmentation		☑	☑	☑
SR 5.1 RE 2 Independence from non-control system networks			☑	☑

FR: Foundational Requirements = Grundlegende Anforderungen

Netzwerktrennung in der GA

SAUTER
Für Lebensräume mit Zukunft.

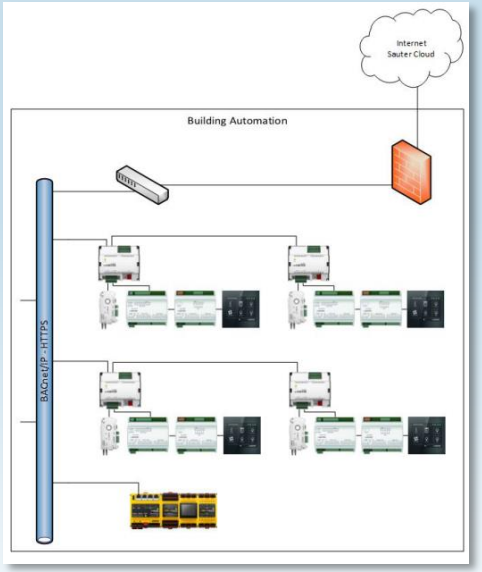


- Physikalische Trennung von GA Netzwerk (BACnet/IP) und IT-Netzwerk / Internet
- Verschlüsselte Kommunikation über IT-Netzwerk zu GA-Komponenten (z.B. MQTT) und Bedienung MBE/AS (via. HTTPS)
- Einschränken des Zugangs (z.B. Schaltschränken, Server-Racks) zu unverschlüsseltem GA Netzwerk
- Reduzierung der GA Netzwerkteilnehmer (Feldbusse über AS an GA, Switche in AS integriert, AS mit hoher Packungsdichte, RC raumübergreifend)
- (Alternativ: logische Trennung via VLAN, dann aber GA-Kommunikation und Bedienung nicht eindeutig trennbar)

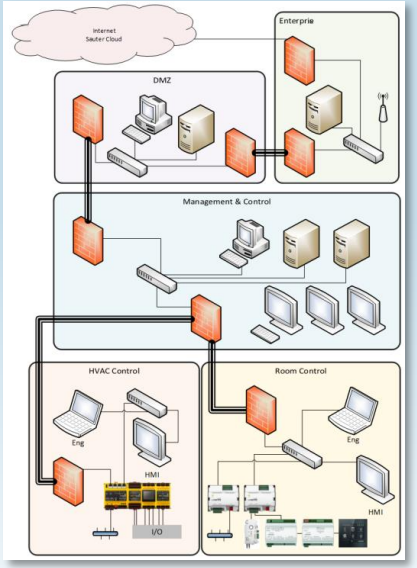
Segmentierung der GA

SAUTER
Für Lebensräume mit Zukunft.

herkömmliche GA

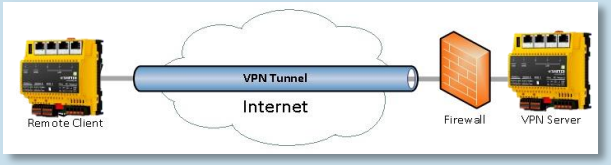


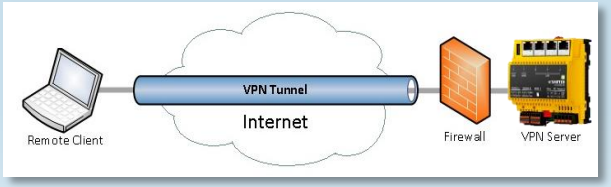
segmentierte GA

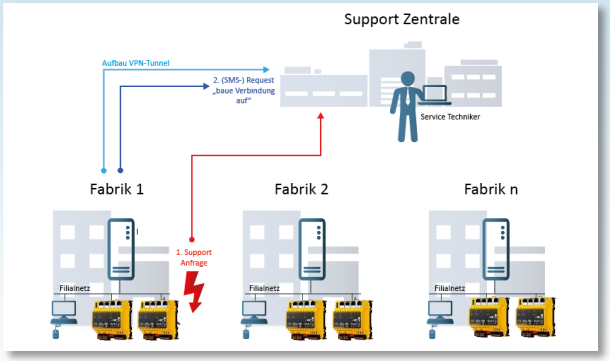


- Planen, einrichten und abgrenzen von IT-Bereichen mit unterschiedlichen Aufgaben und Schutzbedürfnissen
- Zusätzliche Hard-, Software- und Dienstleistungsaufwand
- Mehr IT Knowhow bei Planung und Betrieb der segmentierten Infrastruktur
- Höhere IT Sicherheit

VPN in der GA







- Gesicherte Kommunikation von außerhalb zur GA
- Nutzung etablierter IT Technologien, wie z.B. VPN Verbindungen
- Für:
  - Abgesetzte Inseln / AS- Stationen
  - Fernbedienung
  - Fernservice / Fernwartung

SAUTER
Für Lebensräume mit Zukunft.

Schützen Sie Ihre Gebäudeautomation

…werden Sie sicher !

Dr. Andreas Wetzel, Leiter Gebäudeautomation, SAUTER Deutschland