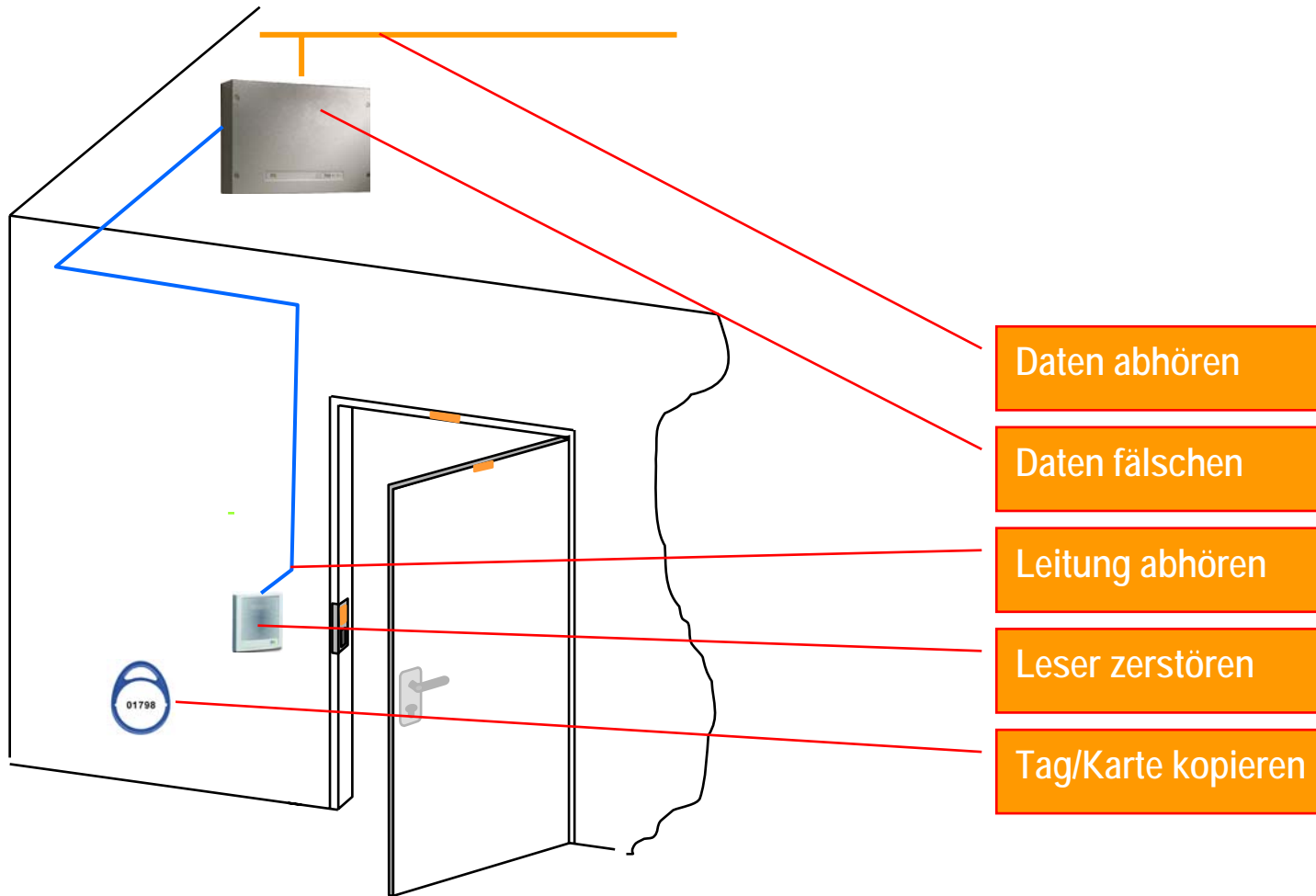




Wie sicher ist „sicher“?

Schwachpunkte bei Zutrittssystemen
und Konzepte für höhere Sicherheit

Trägerische Sicherheit bei Zutrittslösungen



Solche und solche Karten...



Billige Karten und Tags bieten sehr begrenzte Sicherheit

- Miro: Kopieren der Seriennummer „im Vorübergehen“
- Hitag: Schreiben auf Karte
- Mifare/Legic: Verschlüsselung, Kopierschutz

Leser zerstören oder abhören



- | Integriertes I/O-Modul
→ Kurzschließen des Relais
- | Vandalismuskontakt
 - INTUS 300: Magnetkontakt
 - INTUS 400: Mechanischen Kontakt (Schalter)
 - INTUS 500: Optische Lichtschranke
 - Feig-Leser: kein Kontakt
- | INTUS-Leser: Verschlüsselung der Daten zum Zutrittskontrollmanager

Daten fälschen



| Mehrstufiges Passwortkonzept für

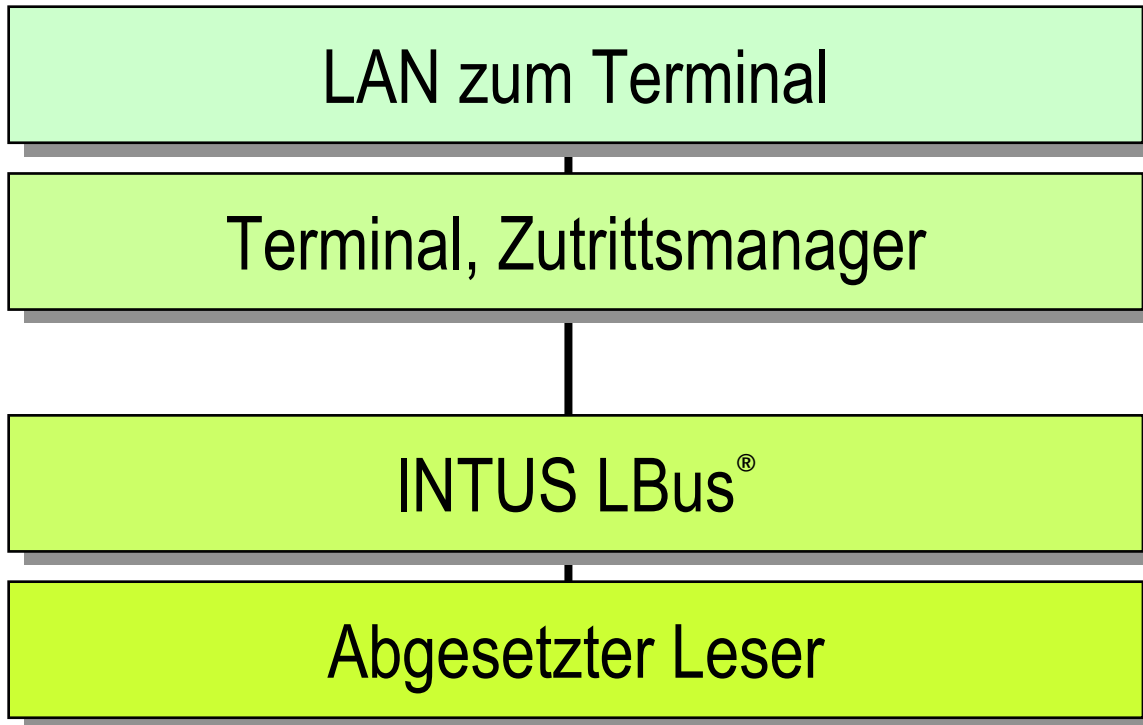
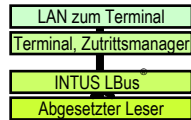
- Haustechniker
- Partner/Kunden
- Sicherheitsbeauftragte

| Integrierte Firewall

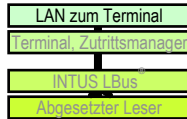
| Verschlüsselte Daten

- zum übergeordneten Leitrechner
- zum angeschlossenen Leser

INTUS Systeme bieten hohe Sicherheit auf allen Ebenen



Sicherheit on board

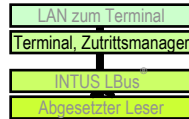


LAN zum Terminal

- | Daten-Verschlüsselung mit Code AES (Advanced Encryption Standard)



Sicherheit on board



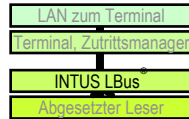
Terminal, Zutrittsmanager

- | Integrierte / Embedded Firewall gegen Attacken aus dem Firmennetz
- | Offline-Fähigkeit mit Notpufferung in allen Notsituationen
- | Gesicherte Übertragung bei Wiederkehr der Verbindung
- | Virenresistent: Geschlossene Einheit: nur 1 TCL-Programm läuft - Virus-Programme werden ignoriert
- | 3 Berechtigungs-Ebenen für Setup-Veränderungen = 3 Benutzer-Klassen
- | Verschlüsselte Ablage der Passwörter
- | Getrennte Wartungsgruppen, z.B. getrennt für Zeit und Zutritt

- | Hardware: Vandalismus-Kontakt.
- | Mechanisches Steck-Schloss bzw. Verschraubung



Sicherheit on board

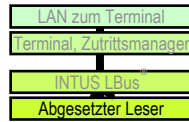


INTUS LBus®

- | LBus für den Anschluss von PCS-Peripherie
- | Übertragung mit gesichertem Übertragungs-Protokoll mit BSC (IBM)
- | Adressierung mit Checksumme, Quittungsmechanismus
- | Aktivierbare Verschlüsselung mit „RC4“ zwischen Terminal und abgesetztem Leser



Sicherheit on board

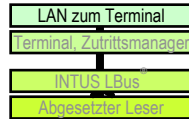


Abgesetzter Leser

- | Auf dem LBus aktivierbare Verschlüsselung mit „RC4“
- | Vandalismus-Kontakt



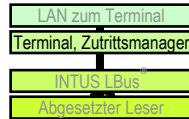
Technischer Hintergrund



LAN zum Terminal

- | Verschlüsselung mit Code AES (Advanced Encryption Standard) - Rijndael-Algorithmus, ein Block-Algorithmus, der als besonders sicher gilt und auch bei VPN verwendet wird. Der Algorithmus wird im 128bit Output Feedback Mode (OFB) betrieben, um einen Datenstrom beliebiger Länge verschlüsseln zu können. Bei jedem Verbindungsaufbau wird der Algorithmus aus Sicherheitsgründen neu initialisiert.
- | Verschlüsselung ist bei allen Rechnerschnittstellen verwendbar, also auch bei seriell (TTY oder Multipoint / BSC)

Technischer Hintergrund

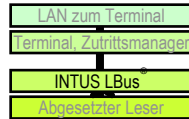


Terminal, Zutrittsmanager

- | Offline-Fähigkeit mit Notpufferung → kein Datenverlust bei Leitungsunterbrechungen, Rechnerausfall, Netzausfall → Gesicherte Übertragung bei Rückkehr des Normalzustandes
- | Embedded Firewall → verhindert Angriffe aus dem internen Firmennetz.
- | Immanenter Virus-Schutz: In TCL-Terminals kann nur 1 TCL-Programm laufen – Virus-Programm mit exe-Datei ist nicht lauffähig
- | Drei Berechtigungs-Ebenen für Setup:
 - Ebene 1 „Leser“ (z.B. für den Haustechniker)
 - Ebene 2 „LBus“ (z.B. für den Partner/Kunden)
 - Ebene 3 „Rechner“ (z.B. für Sicherheitsbeauftragte/IT-Manager)
- | Getrennte Wartungsgruppen → getrennte Verwaltung von 2 Applikationen durch 2 Abteilungen
- | Vandalismus-Kontakt → SW-Sprungziel mit einer programmierbaren Reaktion.
- | Mechanisches Steckschloss bei allen Terminals bzw. Verschraubungen an den ACM.

PCS. The terminal people

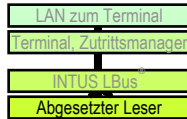
Technischer Hintergrund



INTUS LBus®

- | Für den Anschluss von PCS-Peripherie mit BSC-Protokoll (IBM) und gesicherter Datenübertragung.
- | Verschlüsselungsverfahren: RC4 (von PCS modifiziert, um Attacken zu erschweren).
→ Schutz gegen Replay-Attacken. Verschlüsselung optional aktivierbar, verwendbar in Verbindung mit abgesetzten Lesern, die die Verschlüsselung unterstützen wie INTUS 400, 500, 1600
- | Physikalische Ebene: RS485-Bausteinen mit sogen. Multipoint-Protokoll
→ mehrere Leser an einer Leitung.

Technischer Hintergrund



Abgesetzter Leser

- | Vandalismus-Kontakt: die abgesetzten Leser haben unterschiedliche Gehäuse-Kontakte, die überwacht werden können, was in der Verantwortung der Partnerapplikation liegt.
- | INTUS 300: Magnetkontakt
- | INTUS 400: Mechanischen Kontakt (Schalter)
- | INTUS 500: Optische Lichtschranke
- | Feig-Leser haben keinen Kontakt!