Industrial Control System Security white paper

The top 10 threats to automation and process control systems and their countermeasures with INSYS routers

Introduction

With the advent of *M2M (machine to machine)* connectivity and *the Internet of things*, businesses are presented with the opportunity to remotely monitor, maintain and manage their remote devices (sometimes referred to as assets); this strategy can drastically increase operational efficiency and reduce running costs. Automation and process control system networks are an ideal example of how the advances in technology can be realised. With the use of WAN technology, such as cellular and broadband, businesses can keep in constant contact with their control networks, ensuring that system uptime and system availability are kept at a maximum. Connecting a control system network to a WAN (or public network) does present some security concerns that must be understood. This white paper discusses some of the cyber security threats to businesses that adopt WAN connectivity for their devices.

Top 10 threat overview according to the BSI [1]

In the table below we can see the top 10 cyber threats to automation and process control system networks.

NO.	THREAT	DESCRIPTION
1	Unauthorised use of remote maintenance accesses	Maintenance accesses are intentionally created openings of the ICS network to the outside but are often not protected sufficiently.
2	Online attacks via office / enterprise networks	Office IT is usually connected to the Internet on many paths. Usually, there are network connections from the office into the ICS network, so that offenders can invade this way.
3	Attacks on used standard components in the ICS network	IT standard components (commercial off-the-shelf, COTS) like operating systems, application servers or databases usually contain faults and weak points that are exploited by offenders. If these standard components are also used in the ICS network, this will increase the risk of a successful attack on the ICS systems.
4	DoS (D) attacks	Network connections and necessary resources can be compromised and systems can be caused to crash by (distributed) denial of service attacks, for example to disturb the functionality of an ICS.
5	Human misbehaviour and sabotage	Deliberate acts – regardless whether by internal or external offenders – are a massive threat for all protection objectives. Besides this, negligence and human failure are a major threat especially regarding the protection objectives of confidentiality and availability.
6	Introduction of malicious code via removable media and external hardware	The use of removable media and mobile IT components by external employees is always a great risk regarding malware infections. This aspect was important for Stuxnet for example.
7	Reading and writing messages in the ICS network	Since most control components communicate via plain text protocols and thus non-protected at the moment, eavesdropping and introducing of control commands is often possible without much effort.
8	Unauthorised access to resources	In particular internal offenders or subsequent attacks from outside have a walk-over if services and components in the process network implement insecure methods for authentication and authorisation.
9	Attacks to network components	Network components can be manipulated by offenders, to make man-in-the-middle attacks or easy sniffing for example.
10	Technical misbehaviour and force majeure	Failures due to extreme environmental conditions or technical failures are always possible – risk and damage potential can only be minimised here.

1) Source: BSI-A-CS 004 | version 1.00 dated April 12, 2012

Preventative measures using the INSYS security features

The table below corresponds to the top 10 cyber threats to industrial automation and control system networks; it provides guidance on the most appropriate methods available, when using INSYS routers, to prevent these threats from damaging your remote assets.

NO.	THREAT	PREVENTATIVE MEASURES
1	Unauthorised use of remote maintenance accesses	• VPN • Network segmentation • Firewall • Authentication • Blacklisting / Whitelisting • Key switch functions
2	Online attacks via office / enterprise networks	• Network segmentation • Firewall • Authentication • VPN
3	Attacks on used standard components in the ICS network	• Remote firmware update • Waiving standard office IT standards • Linux components individually selected for INSYS
4	(D)DoS attacks	• Redundant connections
5	Human misbehaviour and sabotage	• Disable web interface • Blacklisting / Whitelisting • Key switch functions • Policies and procedures • Services are only enabled if absolutely necessary
6	Introduction of malicious code via removable media and external hardware	• Network segmentation • Port based security
7	Reading and writing messages in the ICS network	• Network segmentation • VPN
8	Unauthorised access to resources	• VPN • Firewall • Authentication • Network segmentation • Key switch functions • Port based security • Blacklisting / Whitelisting
9	Attacks to network components	• Monitoring log files • Message dispatch
10	Technical misbehaviour and force majeure	• Redundant connections • Redundant devices • Configuration backup

Glossary

Authentication
The authentication during connection establishment ensures that the communication partner is definitely the one he claims to be, Example: The VPN client authenticates to the VPN server and this authenticates its communication partner. Pre-shared keys (PSK) or better certificates are used as an authentication method.

Blacklisting / Whitelisting
Users, IP or MAC addresses that are to be blocked from accessing services or locations are entered into negative lists (black lists). Principle: Everything is allowed which is not forbidden! This is the opposite principle of whitelisting.

The web interface is the central user interface for configuring all INSYS devices. Its structure is consistently identical for intuitive, quick and trouble-free use.

Configuration backup
Operation must be resumed quickly on hardware failures. It must be possible to restore a backup of the complete configuration on the replacement device.

INSYS security features:

- Backup of the complete configuration including all keys and certificates into an encrypted BIN file.
- Devices of INSYS will recognise when restoring that this is a file with a configuration, regardless of the file name.

Disable web interface
This can be used for protecting the device configuration settings against accidental change, sabotage and spying by participants from the LAN and/or WAN.

INSYS security features:

- Disabled for LAN participants.
- Disabled for WAN participants (remote).
- Disabled for LAN and WAN participants (can only be cancelled by resetting to default settings).

Firewall
An active firewall blocks all data packets generally, to allow communication, permitted data packets must be explicitly specified using rules. Principle: block everything, allow only the necessary.

Firewalls are mostly situated at the coupling point between private and public network as well as at the coupling point of network segments (LANs) in case of network segmentation. The main tasks are:

- protecting a secure network from attacks from an insecure network.
- preventing unauthorised access to private networks (LANs).
- enabling authorised access to public networks (WANs).
- limiting the use of services or protocols.

- protecting network segments mutually (cell protection).

INSYS security features:

The firewall of the INSYS icom routers allows you to create rules as per various aspects:

- Data direction.
- Protocol.
- IP version.
- Sender IP.
- Destination IP.
- Destination port.
- Dial-In user name.

Key switch functions

This achieves a physical access protection; only authorised persons can operate the switch with their key. This controls a signal at a digital input of the INSYS routers for connection establishment and closure.

INSYS security features:

- Dial-Out connection.
- OpenVPN-Tunnel.
- PPTP tunnel.
- IPsec tunnel.
- Serial Ethernet connection.

Without key switch OFF, the connection will be terminated again either by the remote terminal or after expiry of the configured time (idle time, maximum connection time, time).

Linux components individually selected for INSYS

Linux distributions contain various services and libraries. INSYS selects each used component individually and checks it carefully; this is how the hardened Linux operating system of INSYS evolves.

INSYS security features:

- Only necessary services are being installed.
- The availability of the sources is ensured
- Transparency and verifiability by using free software.

Message dispatch

Status or fault messages are generated and dispatched based on events. Such messages are a type of condition monitor and inform responsible persons or automated control centres about normal processes or faults.

INSYS security features:

- Monitoring of numerous events like system start, VPN tunnel established, digital input closed or pulsed, Dial-Out or Dial-In connection established, SIM card switched or IP address obtained via DHCP.

- Dispatch as SMS, e-mail or SNMP trap with individual message text
- The content of a status page of the web interface and/or a log file can be attached to an e-mail.

Monitoring log files

Instead of a delayed evaluation of log files, INSYS icom routers will monitor significant events (abnormal connections or unauthorised connection attempts) and send a message immediately.

INSYS security features:

- Immediate message dispatch (SMS, e-mail, SNMP trap) on:
  - Ethernet link (connection established)
  - Ethernet link lost (link lost)
  - Incorrect web interface login

Network segmentation

Manufacturers and external service providers sometimes have external accesses for maintenance and programming. Secure authentication methods and a firewall provide security.

If access for remote maintenance is permitted, further systems or networks may be accessible via a maintenance access. If unintended or unauthorised access to a further system is possible, this presents a security problem.

Therefore, an acceptable granular segmentation of the networks is necessary in order to minimise the "range" of remote maintenance access.

Policies and procedures

Only the interaction of technical, physical and organisational measures as well as their regular check and update will provide maximum security.

This is based on clear guidelines and processes for internal and external personnel, for handling data carriers, e-mail, social networks, passwords, firewall rules, back doors, software installations up to mandatory advanced training programs and security checks.

Port based security

Even if remote accesses are routed via a firewall that allows and monitors the access to the target system, unused Ethernet ports must be disabled.

Used Ethernet ports must be monitored so that it is possible to detect if a network cable is disconnected or connected without authority.

INSYS security features:

- Managed switch, configurable local and remote via web-interface.
- Monitoring of active Ethernet ports and message dispatch (SMS, e-mail, SNMP trap) upon Ethernet link (established, lost).
- Disabling unused Ethernet ports via web interface.

Redundant connections

DoS(D) attacks rarely affect different infrastructures (fixed line network and cellular connections) at the same time.

A cellular connection will be provided in parallel to a fixed line connection as a solution. This allows you to maintain a backup connection in case the fixed line connection is attacked - the inverse solution is also possible.

Redundant devices

using several devices that operate in parallel, one device operates as active and the other operates in stand-by, it will take on the tasks of the defective device in case of a failure.

Devices and services of INSYS routers help you with backing up the configuration for a quick restoration of the original configuration on a replacement device including all certificates.

Remote firmware update

A manual update at the site is often complex and expensive for remote stations. Offenders could also exploit the weak points of outdated systems. Remote updates via secure connections eliminate these defects.

INSYS security features:

INSYS routers can look for the following updates independently on a secure server in the LAN or WAN, download them via HTTP or FTP and install them.

- Firmware.
- Configuration (ASCII and binary).
- INSYS sandbox (image).
- Extension applications (image).

Services are only enabled if absolutely necessary

Services that are not installed or not started cannot be attacked and present no security risk.

INSYS security features:

- Only selected and necessary services are installed on devices of INSYS.
- Services are only started on INSYS devices if they need to be used.

VPN

VPN stands for Virtual Private Network. VPNs are encrypted connections via data networks. The objective is to tamper-proof communication between VPN partners from different local networks (LANs) via insecure or public networks (Internet). They use encryption and authentication for connection establishment and transmit encrypted data (cryptography). The assignment of permissions causes closed user groups. Well-known examples are IPsec and OpenVPN. The INSYS router products support OpenVPN, IPsec and PPTP.

Waiving standard office IT standards

Increased standard information technology is being used in automation and control networks like Windows PCs, databases and software-based PLCs. This makes these networks viable for attack scenarios known from the Internet, since potential offenders have know-how and attack tools freely available on the Internet.