Industrial Control System Security

Top 10 threats for automation and process control systems and countermeasures with INSYS icom products

INSYS icom

Industrielle Datenkommunikation

Top 10 threat overview acc. to BSI [1)]

No.	Threat	Explanation
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 also network connections from office into ICS network, so that offenders can invade on 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	(D)DoS 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 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 nor or 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 Web link

Measures by INSYS SECURITY INSIDE

No.	Threat	Measure
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 components ▪ Linux components individually selected for INSYS
4	(D)DoS attacks	▪ Redundant connections
5	Human misbehaviour and sabotage	▪ Intuitive configuration "keep it simple and secure" ▪ Access to web interface can be disabled ▪ Whitelisting ▪ Blacklisting ▪ Key switch functions ▪ Policies & Procedures ▪ Devices and services "Made in Germany" and "Designed by INSYS" ▪ Services are only enabled if absolutely necessary
6	Introduction of malicious code via removable media and external hardware	▪ Network segmentation ▪ Port-based security
	Continued on next page	

Measures by INSYS SECURITY INSIDE, continued

No.	Threat	Measure
7	Reading and writing messages in the ICS network	▪ Network segmentation ▪ VPN
8	Unauthorised access to resources	▪ VPN ▪ Firewalls ▪ Authentication ▪ Network segmentation ▪ Key switch functions ▪ Port-based security ▪ Whitelisting ▪ Blacklisting
9	Attacks to network components	▪ Monitoring log files ▪ Message dispatch
10	Technical misbehaviour and force majeure	▪ Redundant connections ▪ Redundant devices ▪ Configuration backup

- Use INSYS icom products with INSYS Security Inside.
- Use the technically well-founded advice of our employees

  Phone +49 941 58692-0

  E-mail insys@insys-tec.de

- We would be glad to give you professional advice!

Currently on the homepage of INSYS icom

- Industrial Control System Security
  Protective measures against the top 10 threats

- BSI analyses about cyber security
  Top 10 threats

- First-hand information
  Guidelines and organisations

- Security and risk management
  Integral and continuous process

- Security glossary
  INSYS Security Inside and general measures