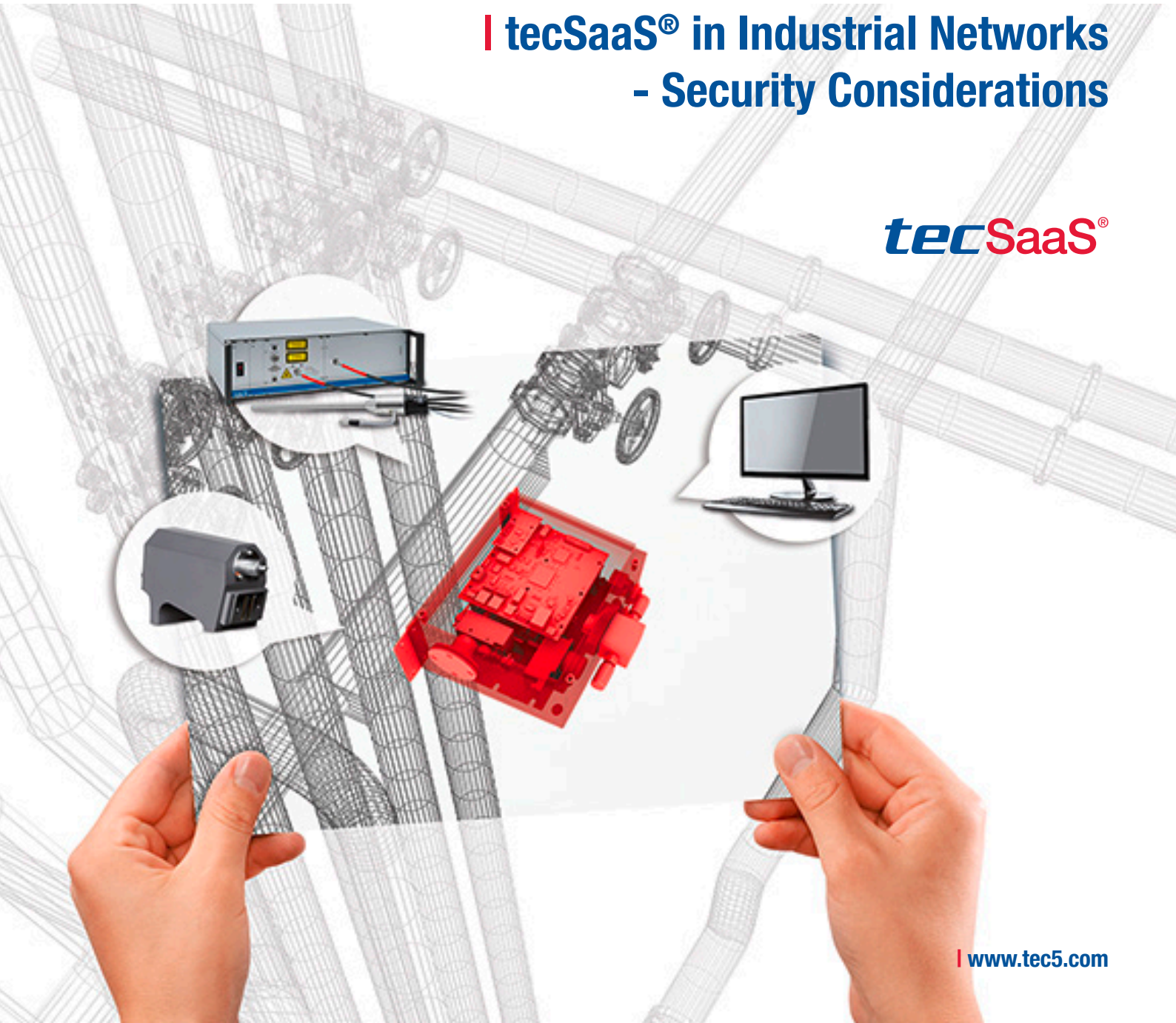
tec5 five
Technology for Spectroscopy

White Paper

tecSaaS® in Industrial Networks - Security Considerations

tecSaaS®



www.tec5.com

[How does a tecSaaS® based embedded spectroscopy system fit in the security concept for ICSs [Industrial Control Systems]]

Industrial control networks are evolving from stand-alone domains to interconnected networks that co-exist within corporate IT environments. The use of smart, autonomous sensors and their administration requires additional control and data interfaces, thus introducing new security threats and vulnerabilities to the ICS. In addition to using IT security technologies in the control system, the embedded spectrometer itself has to be designed based on a comprehensive security concept.

On the other hand, control systems have timing requirements in addition to specifications related to operability and availability. Adding security strategies to a low latency and high throughput system may introduce additional delays, thus degrading the timing or even preventing acceptable system performance.

A holistic approach, one that uses specific countermeasures to create an aggregated security conception, can help defend against cyber security threats and vulnerabilities that affect an industrial control system. This approach, often referred to as "defense-in-depth," can be applied to industrial control systems and can provide a flexible and useable framework for improving the level of cyber security.

The tecSaaS® system was developed with a strong focus on network security and comes with a set of measures to prevent manipulation and misuse.

However, an implementation in a single system component can't be the only answer, as it has to fit the system integrator's security concept.

This white paper outlines the relevant aspects of the tecSaaS® system, which can contribute effectively to a "defense-in-depth" strategy and thus reduce security risks.

[Conception of tecSaaS®: Designed for IT Security]

Starting already in the product definition phase, the relevant requirements were defined and the implementation concepts were oriented towards a security concept, which makes the products suitable for the conceptions of networked industrial applications. This procedure is in accordance with the recommendations issued by consortia engaged in industry 4.0, like e.g. NAMUR NE 153.

[Secure by Development]

- tecSaaS® runs on especially designed, dedicated hardware made for spectroscopy and process measurement, hardened against environmental impacts
- Real time operation system [RTOS] and interface drivers were selected from renowned international manufacturers and licensed including "source code"
- In this way, full in-house source code control is assured and – if required - fast modifications, such as in cases of security issues, are possible
- Source code validation, analysis, review techniques and guidelines [e.g. MISRA C] are used in the development process
- Combined with a modular software architecture, continuous development and maintenance of custom and generic software modules is very effective

[Hardware Security]

- tecSaaS® runs on especially designed, dedicated hardware made for spectroscopy and process measurement, hardened against environmental impacts
- Proprietary architecture and interfaces result in a good intrinsic protection of the system against reverse engineering or manipulation attempts
- Unlike off-the-shelf, universal embedded electronics, the system offers restricted interface functionalities [e.g. access to USB memory devices only] and no unused interfaces which could be vulnerable to attack
- A hardware crypto engine effectively supports data encryption and validation of signatures

[Software Security]

- tecSaaS® does not use a runtime environment [e.g. Java] nor APIs for scripting or programming. The system is based on a firmware image and setup by configuration files, which means it is immune to common computer viruses, worms, etc.
- The configuration settings and update files are protected against unauthorized access by signatures
- tecSaaS® offers user management with several access levels and suitable permissions
- Authentication starts on protocol level and each message can be protected by state-of-the-art encryption

[Security in Field Integration and Use]

- Extensive monitoring options help to detect malicious behavior
- Possibilities to disable [optional] services [Web, Process, FTP, …] on runtime by configuration or to exclude unwanted services directly by building custom firmware images
- Fine-grained read-write permissions for the process interface
- Process data validation by checksum functions

For more information about security strategies for ICSs please refer to:

https://ics-cert.us-cert.gov/Recommended-Practices

NAMUR NE 153: Automation Security 2020

Technology for Spectroscopy

Headquarters
tec5 AG | In der Au 27
61440 Oberursel, Germany
P. +49.(0)6171.97 58-0
sales@tec5.com | www.tec5.com

www.tec5usa.com