SICK OPERATING GUIDELINES

CYBERSECURITY BY SICK

SICK

Sensor Intelligence.

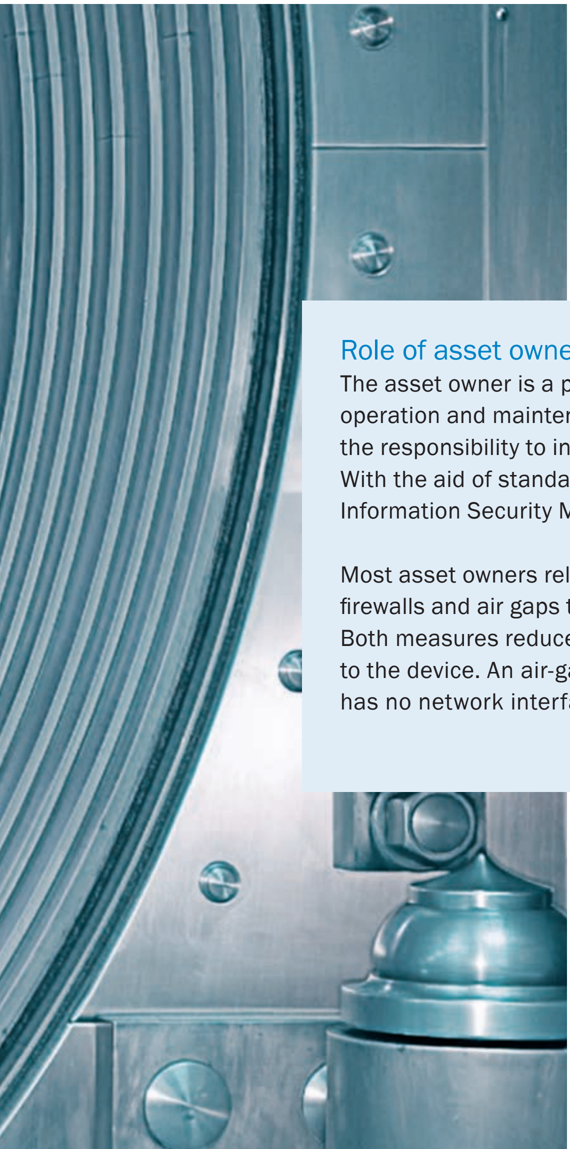
Industrial Information Security

WHY CYBERSECURITY MATTERS

At SICK, Cybersecurity covers the entire product life cycle. The increasing digitalization and growing network complexity of production plants increases the risk of cyberattacks. These attacks can originate inside or outside the production network (for example, they can come from the Internet or from wireless interfaces). For this reason, a comprehensive cybersecurity strategy is essential.

Transmitting data securely and protecting systems against manipulation by hackers present an increasing challenge, in particular due to the growing number of networks in Industry 4.0 environments. Today's Industrial Control Systems (ICS) are IP-addressable and connected. ICS and IT systems increasingly connect and communicate, and more ICS are remotely accessible than ever before.

The foundation for securing industrial networks requires the following: Deep insight into control plane communication protocols such as OSPF, IS-IS or BGP drawing the network topology; the capability to scan the network, identify devices, take inventory of devices present, snapshot their settings and continuously monitor activity on devices to detect unauthorized changes.



Role of asset owner

The asset owner is a person or organization responsible for operation and maintenance of a system. The asset owner has the responsibility to install and maintain security measures. With the aid of standards, an asset owner can implement an Information Security Management System.

Most asset owners rely on corporate IT measures, i.e. firewalls and air gaps to reduce the attack vector on ICS. Both measures reduce the number of possible connections to the device. An air-gapped computer or network is one that has no network interfaces connected to outside networks.

NETWORK SECURITY

When designing a network architecture for an ICS, network security can be achieved by introducing well-established design solutions for isolating and protecting network segments. Practical considerations, such as cost of ICS installation or maintaining a homogenous network infrastructure, often mean that a connection is required between the ICS and the corporate network. These architectural aspects are explained in the following sections.

Network segmentation into zones

Dividing the network architecture into zones differentiated by function to match the standards proposed in ISA-95 as closely as possible allows an infection to be contained within a single zone. This makes it difficult for an attacker to spread an attack to other zones. There should be at the very least three separated areas:

- Network Control
- “demilitarized zone” (DMZ)
- corporate local area network (LAN) – also referred to as “Office LAN”

The aim of network segmentation is to minimize access to sensitive information for systems and people without access permission.

Encryption of communication and logical isolation

Encryption of communication and logical isolation can be achieved using virtual private network (VPN) and virtual local area network (VLAN) technologies between zones. This measure also serves to avoid an infection spreading from one zone to another. Controlling and filtering of traffic by means of firewalls , proxies and elements intended to identify and separate traffic and communications at the level both of the network (IP, routing) and of the port, protocol and applications layer helps detect an infection when it attempts to cross over to another zone.

Extending security to the data-link and application layers

This brings in security measures for the data-link layer, such as access controls in accordance with 802.1x and filtering by media access control (MAC) address, and for the applications level through the use of a web application firewall (WAF).

Access controls based on whitelisting

Such controls implement rules for access based on recognized elements and deny access to all others. One area of considerable variation in practice is the control of outbound traffic from the control network, which could represent a significant risk if unmanaged. One example is a malware that uses HTTP tunneling to exploit poorly defined outbound rules. In addition to these rules, the firewall should be configured with outbound filtering to stop forged IP packets from leaving the control network or the DMZ. In practice, this is achieved by checking the source IP addresses of outgoing packets against the firewall’s respective network interface address. The intent is to prevent the control network from being the source of spoofed (i.e., forged) communications, which are often used in Denial of Service (DoS) attacks.

Wireless networks involve an additional risk

Wireless networks should be implemented only when absolutely necessary or because of a specific decision by the organization and always with clear justification. In their case, IEEE 802.1x mechanisms are used for authentication, including extensible authentication protocol transport layer security (EAP-TLS), which authenticates clients with certificates, can be used in combination with a RADIUS server. Access points should be situated on networks that are isolated or have the minimum possible interconnections with the ICS control network (none at all, if this can be achieved).

A robust protocol for wireless communications, such as WPA2 Enterprise with CCMP, should be in place and additionally a characteristic and unique service set identifier (SSID) should be used, with broadcast deactivated, but with filtering by MAC address in operation.

AVAILABILITY

In industrial control systems, latency and the transmission speed of messages are critical factors. These factors determine whether the design of the control network is able to face up to potential problems of congestion or loss of connectivity. Recommendations for enhancing the resilience of a network to these problems include:

- Using switches that add network functionalities to segment a VLAN and prioritize certain types of traffic on the basis of quality of service criteria.
- Using redundant topologies to bolster availability as well as implementing the Spanning Tree Protocol (STP) to keep control of the formation of network loops.
- Using the internet group management protocol (IGMP) together with a VLAN to provide better performance and restrict multicast messages in accordance with the type of traffic and the devices concerned.

REMOTE ACCESS

If access from infrastructures external to the control network is necessary, the use of VPN solutions would bring the encryption and authentication necessary to protect the connection. Specialized software, hardware, or both, should be used for remote access, together with suitable security policies in relation to updates, and to managing access and users.

NOTES

CONTACT INFORMATION

Reports and inquiries concerning the cybersecurity of products can be sent directly to the SICK Product Security Incident Response Team (PSIRT). The SICK PSIRT is responsible for the investigation, internal coordination and disclosure of security vulnerabilities.

You can contact us via web and mail:

➜ https://sick.com/psirt

➜ psirt@sick.de

Further information

SICK refers to further information on security in factory automation and process control published by numerous sources, i.e. BSI or ICS-CERT.

➜ https://sick.com/psirt

8024601/2019-07-29 · BEM · Pre USmod en49

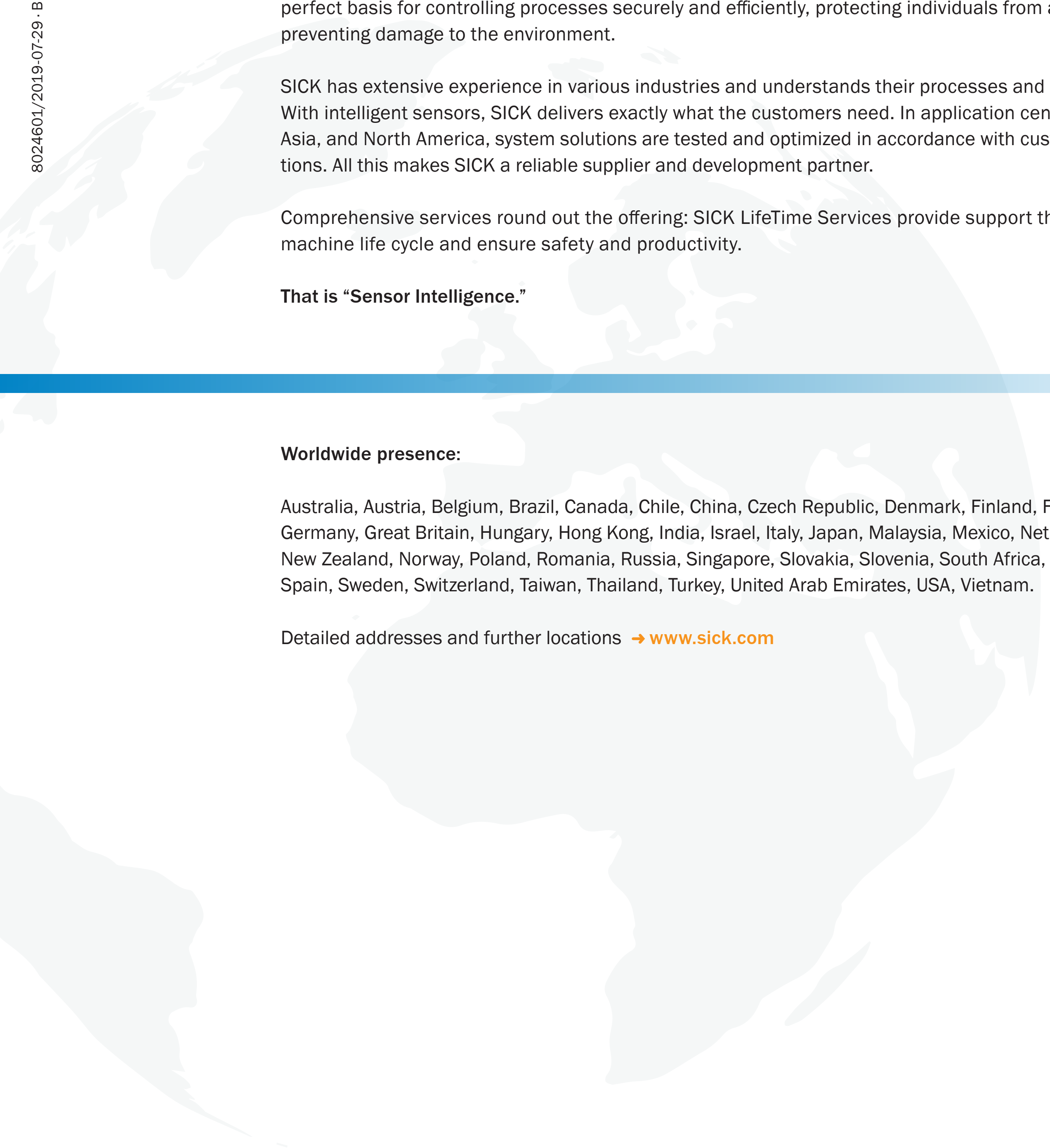
SICK AT A GLANCE

SICK is a leading manufacturer of intelligent sensors and sensor solutions for industrial applications. With more than 9,700 employees and over 50 subsidiaries and equity investments as well as numerous agencies worldwide, SICK is always close to its customers. A unique range of products and services creates the perfect basis for controlling processes securely and efficiently, protecting individuals from accidents, and preventing damage to the environment.

SICK has extensive experience in various industries and understands their processes and requirements. With intelligent sensors, SICK delivers exactly what the customers need. In application centers in Europe, Asia, and North America, system solutions are tested and optimized in accordance with customer specifications. All this makes SICK a reliable supplier and development partner.

Comprehensive services round out the offering: SICK LifeTime Services provide support throughout the machine life cycle and ensure safety and productivity.

That is “Sensor Intelligence.”



Worldwide presence:

Australia, Austria, Belgium, Brazil, Canada, Chile, China, Czech Republic, Denmark, Finland, France, Germany, Great Britain, Hungary, Hong Kong, India, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, New Zealand, Norway, Poland, Romania, Russia, Singapore, Slovakia, Slovenia, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, Turkey, United Arab Emirates, USA, Vietnam.

Detailed addresses and further locations → www.sick.com

SICK
Sensor Intelligence.

SICK AG | Waldkirch | Germany | www.sick.com