SICK AG WHITEPAPER

Security Concepts for the Remote Infrastructure of SICK

Business Cluster Integrated Automation, 2023-05

Author

Valentin Darting
Product management
Integrated Automation
SICK AG in Freiburg, Germany

SICK
Sensor Intelligence.

Content

1 Introduction

SICK offers its customers competent and fast remote service. In times of increasing cybercrime, many customers are concerned about the security of the solutions used by SICK.
SICK strives to achieve maximum security with minimum operating complexity. In doing so, SICK is guided by the recommendations and the catalog of measures of the German Federal Office for Information Security (BSI) for secure remote service (M 5.33).

This includes:

- Remote maintenance access can only ever be initiated from the customer's local IT system and can not technically be started from the outside.
- Logging of the execution of remote maintenance
- Compliance with the 4-eyes principle, i.e. no remote maintenance without the customer's approval
- Authentication and multi-level permissions management for service personnel
- Encryption of the transmitted data

This white paper explains the security concepts of the existing architectures at SICK in more detail.

2 Standard Remote Infrastructure

The Standard Remote Infrastructure at SICK consists of the Remote Infrastructure Platform (remoteservice.sick.com) and a gateway at the customer's site. The gateway can be implemented as a Meeting Point Router (MPR), Remote Service Connect or as a Workstation. A detailed description of the three types of gateway can be found in the following section

2.1 Remote infrastructure platform

The structure of the remote infrastructure platform as the central point for communication is based on the client-server principle, which is known from the Internet. The clients are the initiators of the connections to the server and represent the endpoints.
All data streams from the individual connection partners converge on the platform. In addition to managing and approving users, master data, and remote maintenance connections, this system is also responsible for securing this data. All accesses are encrypted from the endpoint to the central server, either for control or for information exchange. The gateway at the customer's site is used to establish a secure connection to the platform. The remote infrastructure platform is based on a hardware-based rendezvous system in the cloud.
This means that the gateway at the customer's site as well as the service technician from SICK must be authenticated and authorized before a connection is established. Only then can a secure connection between the customer system and the Service department be established. On the customer side, it is only necessary to implement connection sharing in the firewall. SICK is fully responsible for the secure operation of the platform.

2.2 Architecture of the remote infrastructure platform

The architecture uses a star-shaped connection structure, i.e., all connections are made via the central remote infrastructure platform. Only this platform provides the https and OpenVPN services on the web, all other components utilize these and therefore use only outgoing connections. In particular, there are no direct connections between service technicians and machines. Events such as the loss of laptops or employee changes that result in authorization changes or security vulnerabilities can be handled centrally. This architecture eliminates the need to perform administrative functions on client devices.

2.3 Identity and access management with the SICK ID

All users must be authenticated and authorized before connecting to the customer system from the remote infrastructure platform. This is achieved using the SICK ID. The SICK ID uses the Open ID Connect protocol for this.
OpenID Connect is an open protocol and a standard method of user authentication.
Identity providers, such as Facebook, use it to allow users to access other websites or apps after signing in without having to sign in again (single sign on)[1]

[1] https://www.okta.com/de/identity-101/whats-the-difference-between-oauth-openid-connect-and-saml/

The password only has to be entered once at the identity provider and is not shared with other services.
The identity provider assumes a central role in the course of authentication, as it is responsible, among other things, for defending against a brute force attack and for compliance with security policies (e.g. multifactor authentication) present.
The SICK ID serves as an identity provider and authorization server.

The remote infrastructure platform sends an authorization request to the SICK ID when the user signs on. After successful authorization of the user based on the SICK ID and after password entry or multifactor authentication, a JSON web token is sent from the authorization server to the platform. The period of validity of the access token is configurable and is usually valid for five minutes. Furthermore, the token is signed and can thus be easily checked for manipulation. The following diagram provides an overview of the registration process:

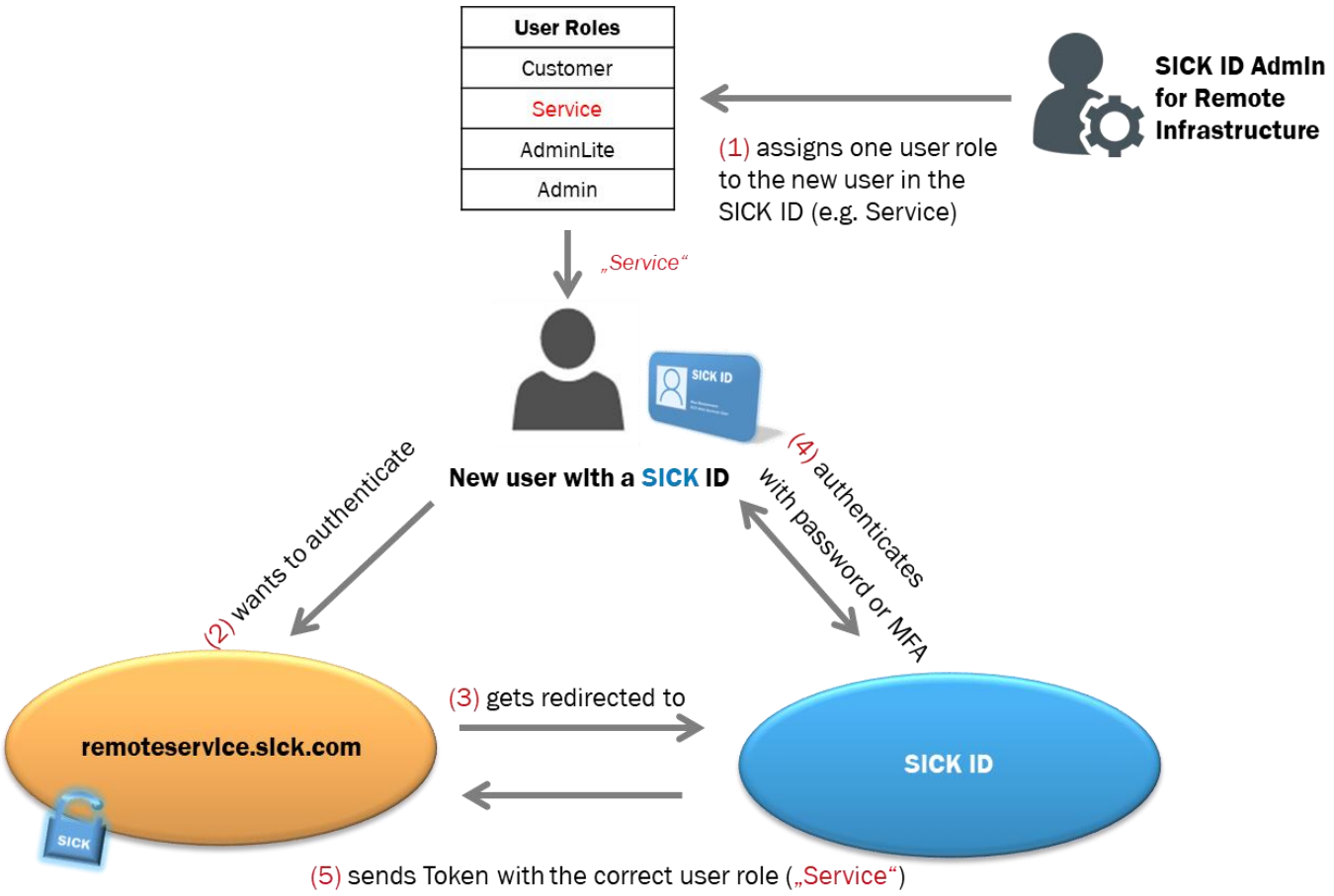

Figure 1 Sign in process using the SICK ID

2.4 Protocols used

2.4.1 HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is commonly used for encrypted communication between browsers and web servers, including online banking, shopping portals, and many platforms that save personal data. In the standard remote infrastructure, the widely used web server Apache is used as the communication endpoint.
HTTPS, when used with current browsers, uses encryption algorithms currently considered secure, such as AES with a key length of up to 256 bits.
The OpenSSL libraries are used for encryption.

2.4.2 OpenVPN

OpenVPN is a widely used protocol for securely establishing encrypted VPN connections. This is a so-called TLS/SSL VPN, which is used to forward OSI layer 2 or 3 network packets. Depending on the intended use, this enables individual endpoints and services (port groups) or complete subnets to be made accessible for remote maintenance.
A negotiation of the encryption and the initial authentication is done via time-limited x.509 certificates and private keys (TLS protocol). These data are part of a specific OpenVPN configuration file that is dynamically generated by the remote infrastructure platform before the start of each remote maintenance connection.
This configuration is transferred from the remote infrastructure platform to the respective endpoint of the VPN (e.g., service technician or MPR) via the secure HTTPS connection path.
The CA used to sign the x.509 certificates as well as the associated private keys are generated internally on the remote infrastructure platform. For remote maintenance, each connection partner will always receive a new configuration file, valid for a limited time, that can only be used to set up one connection and is then worthless.
Encryption is performed using the AES (Advanced Encryption Standard) encryption algorithm, which is currently regarded as secure, and a key length of 256 bits.

2.5 Meeting Point Router

Figure 2 The Meeting Point Router (MPR)

2.5.1 Intention

The Meeting Point Router (MPR) is part of SICK's remote infrastructure. The MPR is based on a simple industrial PC that is equipped with two network interfaces and serves to separate the machine network (LAN) from the customer network/Internet (WAN).
The aim is to be able to establish a secure connection to components in the machine network and to approve this connection for remote maintenance by in-house employees or third parties.
All data will always be routed via the central remote infrastructure platform, which represents the central switching and control point of the architecture.

2.5.2 System overview

A hardened and customized version of the current Ubuntu Linux LTS (Long Term Support) distribution is used as a basis for the MPR. When used in conjunction with a local web server and browser, and through customizations of the user interface and system services, this creates a self-contained system.
The user functionality is limited to the management of remote maintenance connections and diagnostic options as well as importing new configurations via a USB stick.

The configuration settings are usually selected via the remote infrastructure platform and stored there centrally. These configurations are rolled out via a file that is stored on a USB stick and transferred to the MPR via this route.
The system has an integrated stateful packet inspection firewall, which may be configured differently depending on the project, but in the basic version only allows essential outgoing communications. The customer network (WAN) and the machine network (LAN) are completely separated from each other and data exchange must be explicitly permitted.

2.5.3 Networking of the system using existing components

The MPR itself serves to separate the customer network and the machine network.
The network interface of the customer network (WAN) is designed for outgoing connections to the remote infrastructure platform via the Internet. Accessibility from the Internet is not necessary or recommended for the MPR. To allow communication with the remote infrastructure platform, outgoing connections to the respective system and the corresponding response packets must be allowed.
The machine network is connected to the interface (LAN) provided for this purpose. There are no restrictions on communication there. In the basic configuration, however, no requests are forwarded from the machine network to the customer network and vice versa.
During a remote maintenance connection, the components connected to the machine network are accessible via a secure connection. In general, all Ethernet or IP (Internet Protocol) based components can be reached via remote maintenance.

2.5.4 User interface

A user interface for enabling remote maintenance connections is provided on the MPR. This can be used either locally by the machine operator via a touchscreen, or via the network using a web browser.
The end user thereby retains full control at all times of any remote maintenance activities on their machines and can intervene if necessary. If a connection to the remote infrastructure platform cannot be established, the user receives a detailed network status report through the built-in diagnostics. This information can be forwarded to the internal IT department on site or to external support for problem resolution.
Whether access to the web interface is only possible from the machine network (LAN) or also from the customer network (WAN) depends on the particular project with the manufacturer/operator.

2.5.5 Touchscreen

The end user can view the current connection status at all times via the touchscreen. Remote maintenance can only be established after manual approval. If the user wishes, the existing connection can be terminated immediately at the press of a button.

2.6 Procedure for a remote maintenance connection

In this example, a problem is established on a machine that cannot be resolved on site.
The operator calls the SICK service hotline. A case is opened and the machine now needs to go "online".

Initiation of a connection by the operator of a machine

- The operator presses the "Connect" button on the touchscreen of the MPR
- The MPR sends a request to the remote infrastructure platform via the control channel (HTTPS).
- The MPR receives a configuration file for setting up the data channel
- After successful verification of the digital signature, the data channel (OpenVPN) is established
- The MPR and the assigned machine appear as "online" in the web interface of the remote infrastructure platform

2.6.1 Connection setup by a SICK service technician

- After logging into the web interface of the remote infrastructure platform, the service technician navigates to the

machine file

- On pressing the "Connect" button in the web interface of the Remote Infrastructure platform, an OpenVPN configuration is created and sent out
- The service technician connects with OpenVPN and has access to the machine

2.6.2 Termination of the connection

There are three scenarios for terminating or interrupting the connection:

1. The operator presses the "Disconnect" button on the MPR via the touchscreen or the web interface

2. On the service technician's system, the "Disconnect" button is pressed in the "OpenVPN" client or in the web interface of the remote infrastructure platform

3. An administrator terminates the remote maintenance connection via the web interface of the remote infrastructure platform on behalf of the service technician/customer or the MPR

In cases 2 and 3, only the operator of the machine can re-establish a connection

2.7 Connection technology

Before each connection is established, a one-time valid configuration file is generated on the remote infrastructure platform. This file contains all the data needed to establish the connection and is downloaded by the MPR after authentication via a secure web access over HTTPS.
The MPR establishes a secure point-to-point connection to the remote infrastructure platform via OpenVPN. All communication passes through this central remote infrastructure platform, which logs all remote maintenance sessions and allows only the configured accesses through its dynamic firewall. Encrypted communication is thereby provided on the transport route via the OpenVPN tunnel.
It is possible to use separate protocols to implement complete end-to-end encryption within the tunnel.

2.8 TUN routing mode (OSI layer 3)

The configuration for remote maintenance connections at SICK is the routing mode. The remote maintenance connection forwards all IP-based communication (OSI layer 3) between the service technician and the appropriately addressed device in the machine network via a tunnel interface (TUN). While doing so, access to the respective services enabled for the remote maintenance session is restricted (IP addresses and ports). To avoid overlapping of frequently used private network ranges, proxy addresses are used here to facilitate interoperability. The advantage of this mode is that the remote maintain engineer can only access the explicitly enabled services, but not the entire machine network.

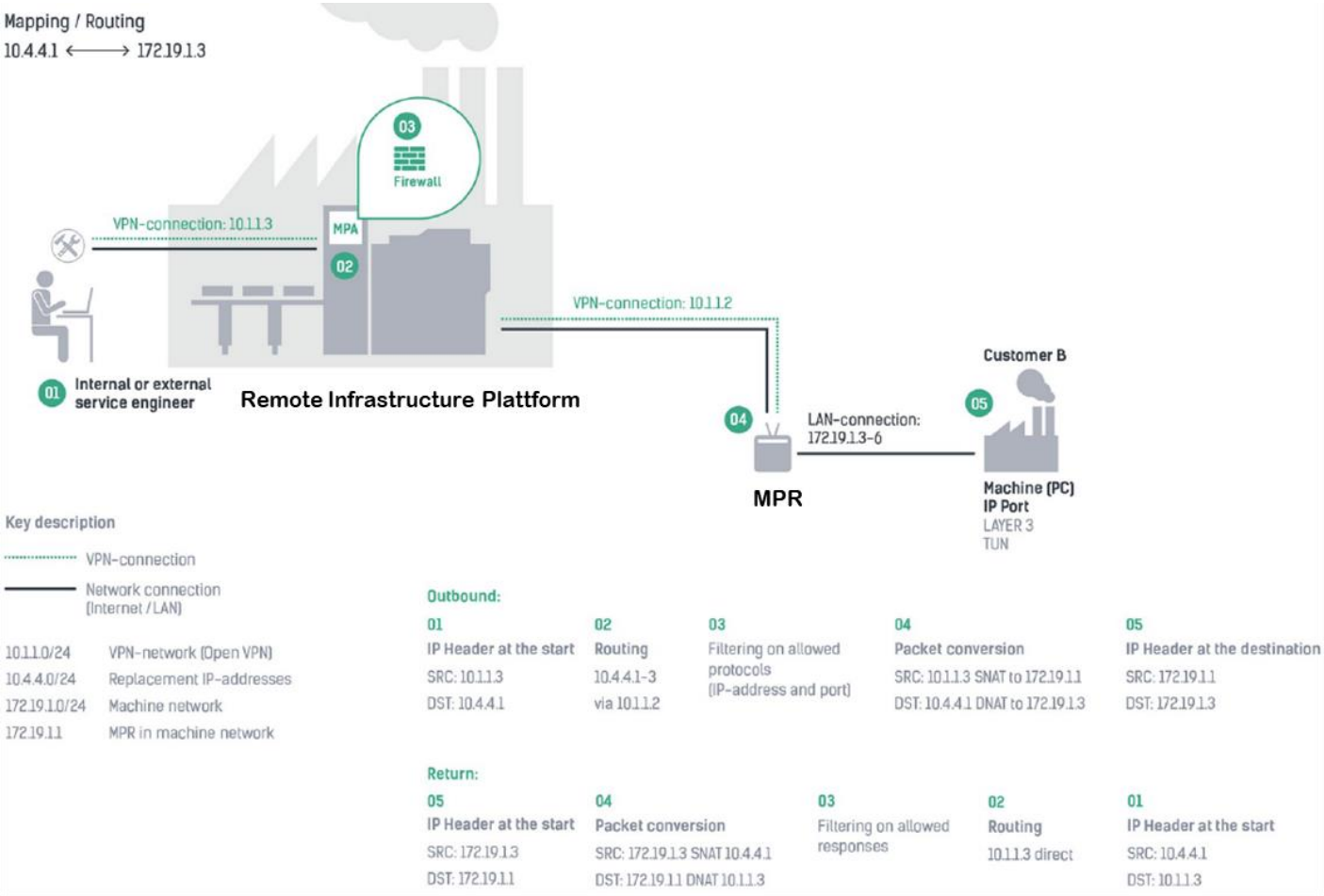

Figure 3 TUN routing mode

2.9 Network protocols used

Each MPR communicates with other components in the network, for example to request an address for IP based communication or to synchronize the time. The following network traffic can therefore be observed and constitutes intended behavior:

2.9.1 Outgoing communication

- ARP: Address resolution on OSI layer 2 (Ethernet)
- ICMP: Ensure control flow and diagnosis of the connection (IP Protocol Number 1)
- BOOTP/DHCP: automatic network configuration (IP UDP port: 67)
- NTP: Time synchronization, important for certificate-based authentication (IP UDP port: 123)
- DNS: Address resolution on OSI layer 3 (IP TCP/UDP port: 53)
- HTTPS: Web access to the remote infrastructure platform (IP TCP port: 443)
- OpenVPN: remote maintenance (IP TCP Port: 443)

2.9.2 Time synchronization using Network Time Protocol

A correct time is necessary in many cases for security mechanisms to function, especially when X.509 certificates are used that have a limited validity.
The MPR therefore synchronizes its time with publicly accessible systems.
The servers of the Physikalisch Technische Bundesanstalt (PTB) are used. If these cannot be reached, a time server of the company PerFact Innovation GmbH & Co. KG is used. The registered addresses are as follows:

- ptbtime1.ptb.de
- ptbtime2.ptb.de
- ptbtime3.ptb.de
- Fallback: ntp.perfact.de

2.9.3 Establishment of the connection to the remote infrastructure platform

The remote infrastructure platform is one of the endpoints of every communication and is usually located at the manufacturer/operator of the system to be remotely maintained. Two communication channels are used between the MPR and remote infrastructure platform. The connection is always initiated by the MPR. The protocols and ports used are:

- HTTPS (443): Web access to remoteservice.sick.com
- OpenVPN (443): Remote maintenance access via remoteservice.sick.com

2.10 Remote Service Connect

At SICK, Remote Service Connect refers to solutions that do not require an MPR to connect to the remote infrastructure platform.
Connection setup, protocols, and encryption mechanisms correspond to those of the MPR.
Unlike the MPR, the user interface is not provided via a touchscreen.

2.10.1 Remote Service Connect app

The Remote Service Connect app was developed to connect the SICK AppSpace environment to the remote infrastructure platform. This is currently implemented using Sensor Integration Machines.
The Remote Service Connect app offers the same functionality as the MPR. This includes a firewall, the separation of the customer and machine network, and the establishment of secure connections using a VPN.

2.10.2 Remote Service Connect Docker container

The Remote Service Connect Docker container is designed to connect specialized hardware to the remote infrastructure.
The Docker container has been optimized for the Telematic Data Collector, or TDC-E for short.
In principle, nothing stands in the way of implementing the container on other hardware capable of running Docker.
The container is a clone of the MPR software image and thus offers the same functionality as the MPR.
The firewall in the TDC-E must be configured manually because the Docker container does not have direct access to the Ethernet interfaces and the firewall.

Figure 4 Telematic Data Collector

2.11 Workstation account

A workstation account is used to access the remote infrastructure from an Internet-enabled control computer. This computer must have a compatible browser and access should be restricted to the IP addresses of remoteservice.sick.com.
Likewise, if compatible, an OpenVPN client can be installed on the control computer to establish VPN tunnels directly from the operating system. For this purpose, a configuration file for establishing the connection can be generated at the push of a button in the web portal and transmitted via HTTPS. This file is valid only for one connection attempt and only for a short time, so sharing it with third parties will not compromise the system.

2.12 Potential attack scenarios

2.12.1 Gateway (MPR, Remote Service Connect and workstation)

Since the MPR and Remote Service Connect are not accessible from the Internet, the possibilities for attack are limited to access attempts from the customer and machine network.
The following protocols and ports can be accessed on the gateway:

- HTTP (IP TCP 80) – forwarding to HTTPS only
- HTTPS (IP TCP 443) – web interface
- SSH (IP TCP 22) – maintenance access (limited to private/public key cryptography and only accessible via the “machine network” or OpenVPN connection)

The integrated web interface (HTTP/HTTPS) of the MPR is secured using a combination of user name and password.
The default password used for this purpose and stored in the project should always be changed during commissioning by the person responsible for the machine.
SSH maintenance access can only be accessed from the machine network or via an existing remote maintenance connection using OpenVPN. The private/public key method, which is considered secure, is used for authentication.

2.12.2 Attacks on the connection technology

2.12.2.1 Control channel (HTTPS)

For authentication on the remote infrastructure platform via the Internet, a unique identifier is stored on the MPR during rollout. This identifier replaces the use of username and password and therefore must be kept secret.
In the event that an access code is stolen from the MPR, it can be used to access some web pages of the remote infrastructure platform. These enable a connection configuration to be requested.
This can only be used, however, to share local network devices, so an attacker would only be able to access their own resources. In particular, there is no access to resources of other devices that are also connected via the remote infrastructure platform.

2.12.2.2 Data channel (OpenVPN)

OpenVPN is run in certificate-based authentication mode and validated against a self-signed CA stored on the remote infrastructure platform. In addition, dynamically generated time-limited certificates are used so that even brute-force attacks on the private key cannot guarantee success.
Both the HTTPS server and the OpenVPN server provide end-to-end encryption that cannot be broken by common means. However, as with any TLS communication, there is the possibility of a “man-in-the-middle” attack to interrupt the communication between the browser and server.
The necessary manipulations to achieve this, however, always require intervention in the underlying IT infrastructure such as DNS servers or proxy infrastructure.
In any event, this should be prevented administratively in the interest of the IT security of every company.
Some companies exploit this possibility supposedly in the interest of their own IT security (which is relatively easy, since all of the above-mentioned components are accessible to the in-house IT department) to examine malware by means of a TLS/SSL-encrypted data exchange.
However, this permanently undermines the concept of end-to-end encryption and thus undermines the trust of users who

assume secure communication via HTTPS.

2.12.3 Attacks on the application server

Besides attacks on the connection technology, there is the possibility of attacking the web application itself.
The software components and the implementation of the web application on the remote infrastructure platform are well maintained and regularly checked for known security vulnerabilities. The internal security architecture of the web application strictly demarcates the individual areas from each other. Areas that grant user-dependent access to user data are protected by a role concept and filters for master data. These check, when a particular path or record is accessed, the authorization of the user in the specific application context.
These include machine files, documents, and connections, among others.

2.13 Risk estimation

The architectural structure of the remote infrastructure concentrates the attack possibilities on a central server as well as the connections to it. Compared to frequently used decentralized VPN or dial-in architectures, it is possible to quickly respond centrally and block the access of the affected user, for example in the case of lost end devices.
In particular, the avoidance of direct communication between the service technician and the machine network and the necessary distribution of access data to the service technicians significantly reduces the number of conceivable attack scenarios. The above-mentioned potential for attacks on the HTTPS connections would make it possible to display manipulated pages to the user or to gain access to entered information. It is not possible, however, to deceive the server about one's own identity and thereby gain access to information that is not intended for the user.
The remaining risks are manageable. The potential attack scenarios are concentrated on a few points that can be monitored well due to the centralized structure. Comprehensive system logging can be used to ensure that attacks are logged and do not go unnoticed during the regular system reviews.

3 Enterprise Remote Infrastructure

In addition to the SICK Standard Remote Infrastructure, SICK offers a solution that is completely tailored to the respective customer.
This is required if the customer does not allow hardware from SICK in their local network and already operate their own infrastructure for remote access (e.g. for other service providers).
In the case of SICK Enterprise Remote Infrastructure, two redundant virtual machines are created per customer in Microsoft's Azure cloud environment, also called Remote Cloud Portal. On these virtual machines, the service technician can then connect to the customer network via a VPN. Different operating systems can be installed on the virtual machines by customer request. Most of the time it is Windows Server or Windows 11.
The virtual machines are located in separate network security groups. These restrict traffic based on IP address, protocol and port.
SICK meets some further requirements as well with the Enterprise Remote Infrastructure solution
These include, for example:

- Multi-factor authentication for access to the Remote Cloud Portal
- One virtual machine for all service technicians (access from a private, local PC is not allowed)
- Virtual machines are active only when needed
- Hash synchronization with Azure AD Connect (single sign-on)
- All managed virtual machines and disks in Azure are encrypted with a Microsoft-managed key
- Microsoft Defender for Cloud is active by default on all virtual machines

The following graphic provides an overview of the architecture of the implemented solution at SICK

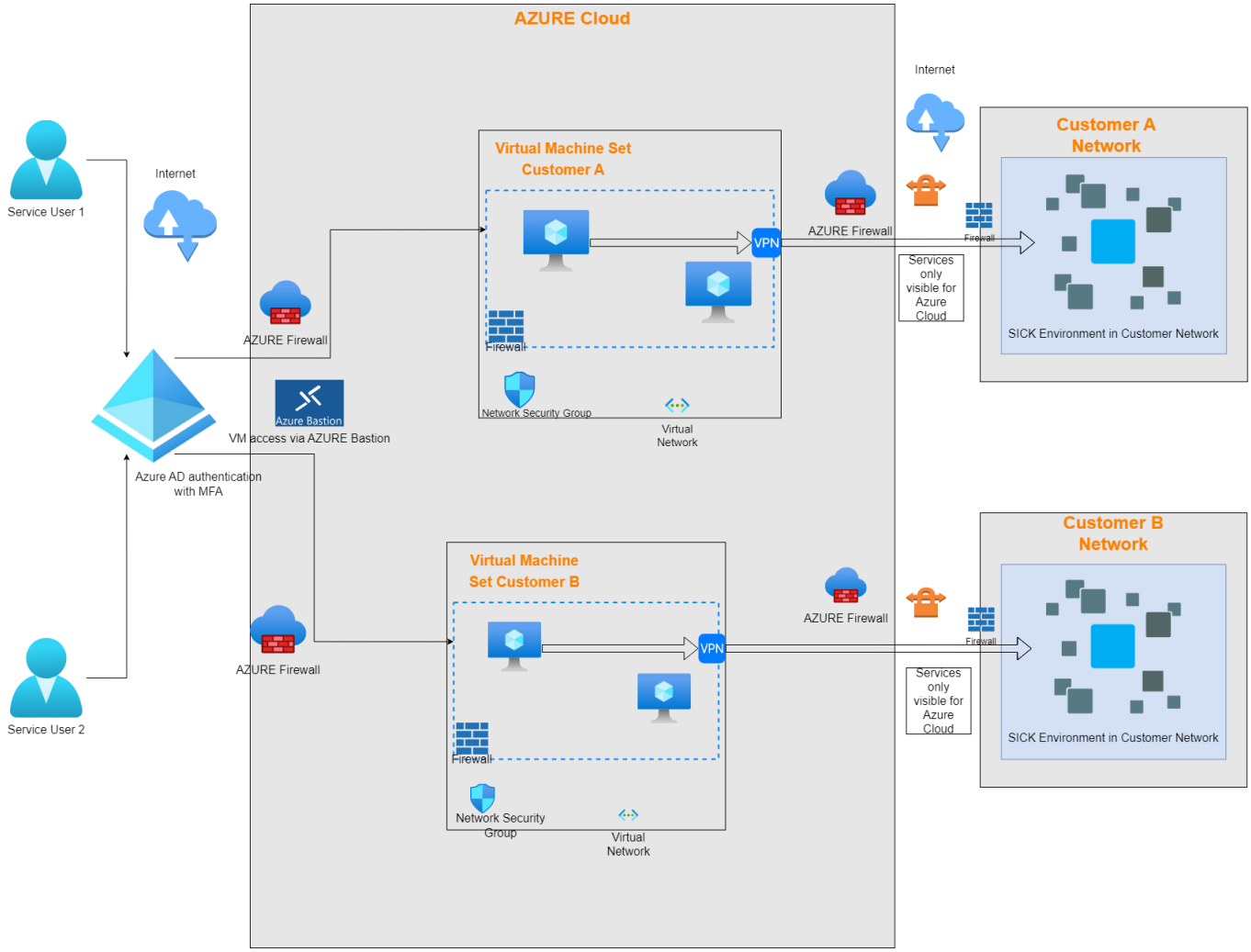

Figure 5 Architecture of the Remote Cloud Portal

3.1 Procedure for a remote maintenance connection

- The service technician logs in to the Remote Cloud Portal using their local user account.
- They confirm the login with another factor, e.g. an authenticator app
- The service technician starts the virtual machine assigned to their customer
- He establishes a connection to the virtual machine via Azure Bastion
- On the virtual machine, the software for a remote maintenance connection is started and the connection to the customer server is established

3.2 Protocols used

The protocol and connection technology used for remote maintenance is specified by the customer. Known and implemented solutions are based on virtual private networks (VPN). These are almost always implemented as SSL VPN (end-to-site) or IPsec VPNs (site-to-site).

3.3 Identity and Access Management using Azure AD

SICK's Azure Active Directory is used for identity and access management. This is fully synchronized with the local Active Directory. Only selected administrators assigned to the customer project are allowed to give users access to the virtual machines.
Each login and access and each remote maintenance connection is uniquely assigned to the corresponding user in an auditable manner. In the implemented least-privilege principle, permissions are defined that allow only the absolutely necessary options for each role.
For example, the service technicians are not able to install additional software on the virtual machines or to gain access from there. The password must also be changed every 90 days.

3.4 Resilience and disaster recovery

Backups are made of the virtual machines on a regular basis. Furthermore, all logging and diagnostic data is stored for at least 550 days.

3.5 Emergency response plan

For Enterprise Remote Infrastructure, there is an Emergency Response Plan that precisely documents how SICK deals with different security incidents. This includes, for example, promptly informing the customer if the information security of our solution could be compromised.

3.6 Change management

If anything (e.g. the software) needs to be hanged on a virtual machine, SICK strictly adheres to the 4-eyes principle. Each change is tested, reviewed and approved by at least two people on the development team.

3.7 IT security in the Azure platform

Azure's infrastructure, from hardware resources to applications, is fully designed for the concurrent hosting of millions of customers and provides a trusted foundation for companies to fulfill their security requirements.[2]
Since large security breaches can destroy entire business models in a potential attack scenario, particular attention is paid to certified and agreed security standards.
Microsoft's cloud computing service is characterized by extremely high security standards and sophisticated compliance functions.[3] The effort that Azure invests in IT security is something that many SMBs simply cannot afford in their data centers.
Furthermore, you have to get away from the idea that the data is safer in your own data center.
Microsoft Azure applies the zero-trust approach:
The assumption is that all users, devices and services, including internal ones, represent potential risks.
Thus, five principles apply to keep attack vectors as small as possible:

- Secure access to all resources regardless of location
- Access controls are performed using the least necessary privilege
- Always check, never trust
- All data traffic is logged and checked
- The network is developed from the inside out

SICK works together with certified and experienced partners who take care of the managed services as well as the secure operation of the Azure platform.
Thanks to an ideally conducted planning phase, during which the topic of cloud security was taken into account from the outset, the architecture implemented by SICK offers a particularly high level of security.

2 https://docs.microsoft.com/de-de/azure/security/fundamentals/overview

3 https://www.seidl-software.com/cloud-security-wie-sicher-ist-microsoft-azure/

SICK AG | Waldkirch | Germany | http://www.sick.com/

SICK
Sensor Intelligence.