RED LION®

EXCELLENCE. REDEFINED

Whitepaper

IT SECURITY
IN INDUSTRIAL REMOTE ACCESS

TABLE OF CONTENTS

Introduction

Many of the machines and production lines used in industrial manufacturing are now networked together. This network of control systems, operating devices, and even drive systems and the associated access to the Internet is the prerequisite for remote access.

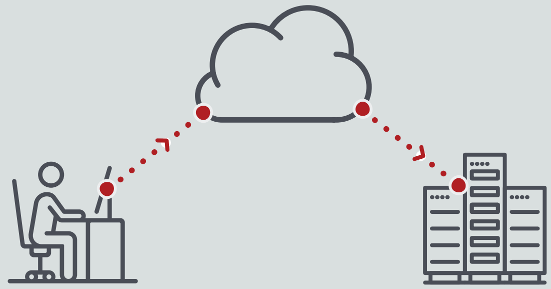
With remote access, a user connects to a control system (PLC, CNC) or an operator device like an HMI (human-machine interface) over the Internet from an arbitrary location. This user can then have process data displayed or can intervene in the control program.

Control systems are typically not designed with IT security in mind. Once a user has successfully connected to an unprotected control, they can access the rest of the corporate network relatively easily. This kind of access must be blocked, however. Accordingly, control systems or other devices provided for production lines or machinery need to be protected with appropriate IT security safeguards before they are connected to the Internet. Effective IT security systems for remote access work on two levels. On the one hand, they manage access rights for machinery or the corresponding remote access endpoints. This makes sure that only authorized users gain access to these machines. In addition, IT security measures need to protect against more wide-ranging cyberattacks from outside the company. This involves making appropriate structural and organizational changes – both in terms of hardware and software. IT security models are a fundamental part of achieving the right level of IT security in a company. The earlier that this topic is covered in the design and planning of the machine or production line, the greater the protection that can be offered by the final security model.

> ”
>
> IT security models are a **fundamental part** of achieving the right level of IT security in your company.

This white paper first takes a look at the basic working principles of the remote access system provided by Red Lion. This is followed by a detailed presentation of the relevant components in terms of their security aspects, plus a solution strategy designed to meet the strictest IT security standards.

BASIC PRINCIPLES OF **REMOTE ACCESS**



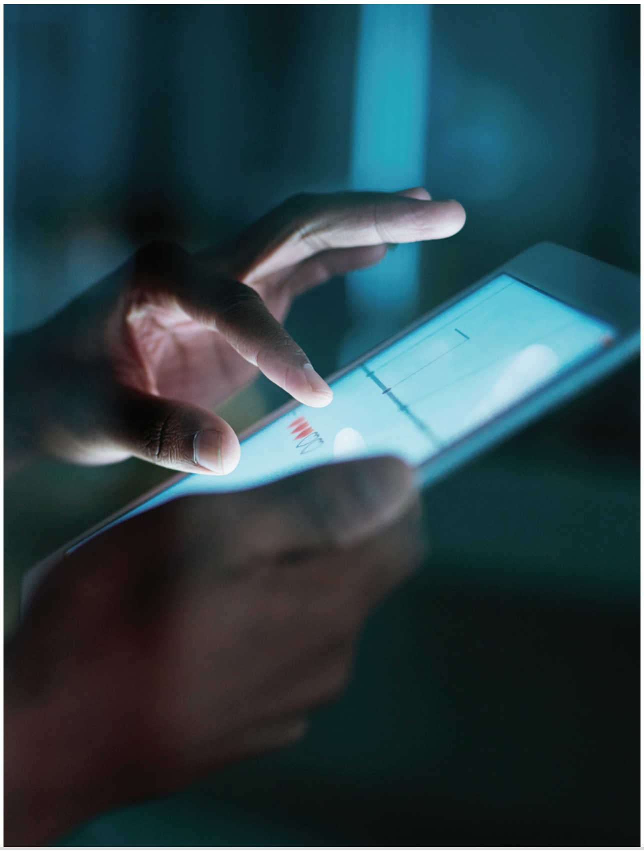
(Above) Schematic diagram of a remote access system. The user first logs into the cloud service and is then granted access to the machine.

A remote access system lets an authorized user – such as a service technician – connect to a PLC or an HMI[1] as a device over the Internet from an arbitrary location. While this sounds simple, it is much more complex in practice. The user's route to remote access doesn't simply work by linking their computer to the machine over the Internet but also involves a cloud-based service. The user first connects to the cloud over the Internet and the cloud then provides the user with access to the machine for which they have access rights.

Remote access: a three-part system

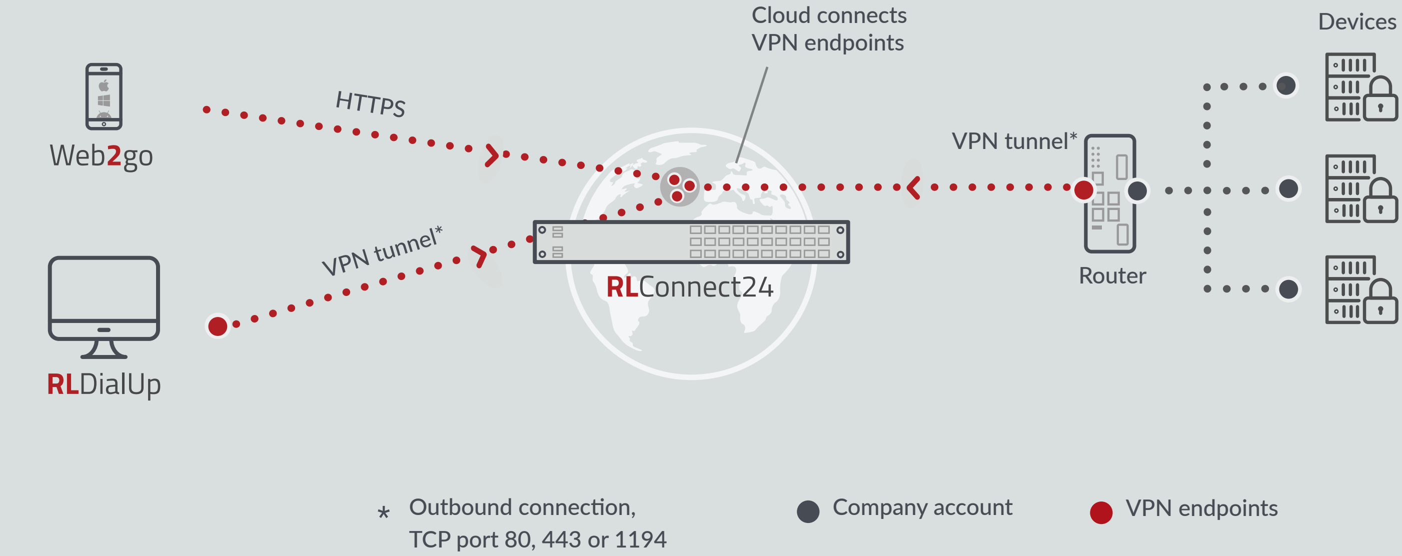
An industrial remote access system is therefore made up of three components: The first and most central component is the cloud itself. The cloud receives the user's request and establishes the connection to the control system. The second component in the system is the security protecting remote user access: only authorized users are given access to the cloud. The third and final component is the connection between the cloud and the control system or some other device. This is handled by a router placed between the machine or device and the Internet, which only allows authorized traffic through to the corporate network.

The Red Lion ecosystem comprises an industrial remote access system with cloud connectivity and an industrial router. The system accounts for all of the relevant security factors and features. With Red Lion, the cloud is synonymous with the RLConnect24 Remote Service Portal, which is used to store the access rights as well as the router configurations. The Portal also establishes the connection between the user and the machine.



[1]) HMI: Human Machine Interface

Ecosystem



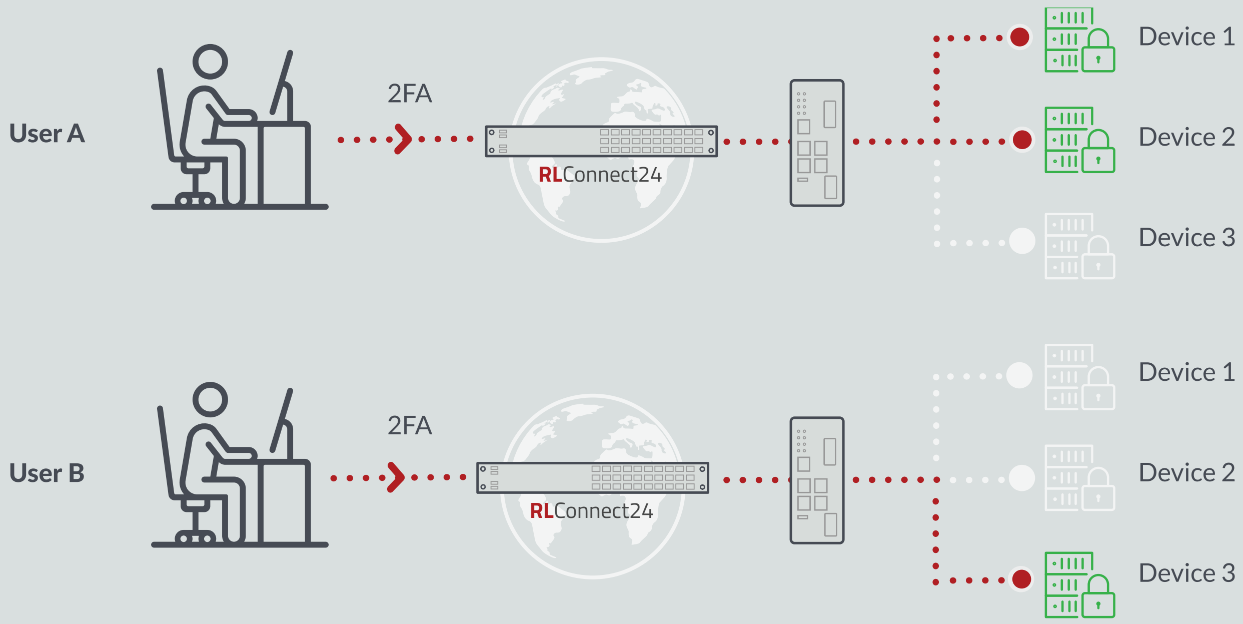
Ecosystem with web-based user access or client connection to the RLConnect24 Remote Service Portal plus RA70S router with integrated firewall.

Access protection

The connection is established as part of a virtual private network or VPN. This network is used to set up a VPN tunnel between the computer and the cloud, as well as a VPN tunnel between the cloud and the machine. Outbound connections are utilized in both cases from the user and machine side. The cloud connects these two VPN tunnels together to create a secure connection between the computer and the router. This secure VPN tunnel is used to transfer data between the user and the device.

User access can be handled by the web-based interface Web2go, which is compatible with any browser, or set up as a VPN client connection with RLDialUp. The RA50 & RA70 industrial routers offer interfaces for industry-standard control systems and devices, and can be used to manage individual access rights to the endpoints. The router's built-in firewall also provides protection from unauthorized third-party access.

OUR
SECURITY MODELS



User A is given access to device 1 and 2. User B is given access to device 3.

Access protection

The authorized user makes use of an outbound connection to connect to the Remote Service Portal and logs in using one of the login options such as two-factor authentication (2FA): Apart from entering their individual username and password, the user also receives a PIN code via email or Google Authenticator: this code also has to be entered as part of the login process. Only then is the user granted access to the system. Once logged in, the user sees the available devices within the machine or production line to which they have access.

Data protection

The cloud is used to store all of the data associated with the remote access procedure. This includes personal user data such as names, email addresses, and passwords, as well as the corresponding user rights to the various components on the machine side. Each connection made between a user and a device on a machine or production line is always established only by and with the cloud. This is because only the cloud has the data needed to identify the user and can assign this user the corresponding rights to devices via the router. The secure transfer of data between two VPN endpoints is assured by the configured VPN tunnels as well as the maximum-security encryption standards used by the communication protocols.

Machine/production line protection

Machinery and production lines are protected by the router. The router separates the machine network (OT network) from the corporate network (IT network). Users can only access the machines and production line components for which they are authorized. All accesses are logged with details of usernames, times, and durations.

IT SECURITY FEATURES FOR **THE ECOSYSTEM**

A comprehensive and integrated security model takes into account each domain within the system, from user access to cloud-based data administration, followed by access to the machinery and production line components via the router. In this context, the Red Lion ecosystem provides the following features:

Encryption

VPN connection with AES 256-bit encryption using the TLS1.2/SSL security protocol. This is a strong encryption standard that also permits secure deployment as part of business-critical applications.

Connections

All connections used are outbound connections. This ensures seamless integration with the existing IT environment. Security strategies already in place can be left untouched.

Authentication

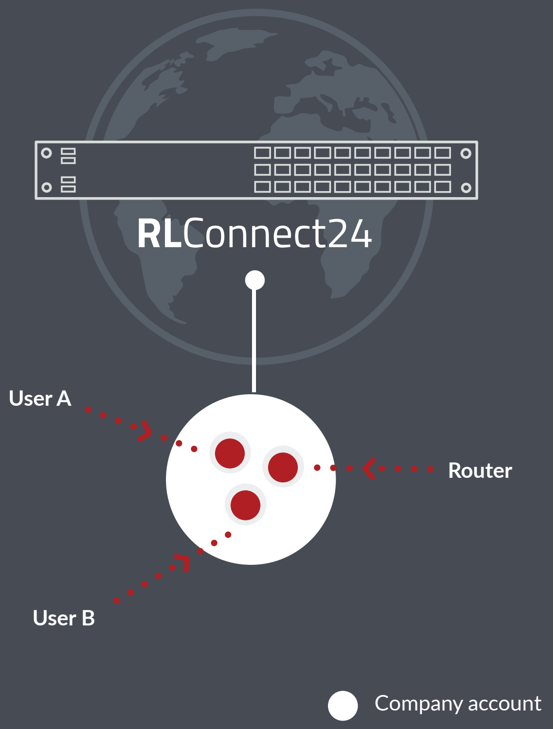
Username and password with certificate-based and optional two-factor authentication (2FA) via email or Google Authenticator is used as a guarantee of user authenticity.

Tests

Regular automated and manual penetration tests are deployed to ensure server security.

THE CENTRAL INTERCHANGE:

THE REMOTE SERVICE **PORTAL**



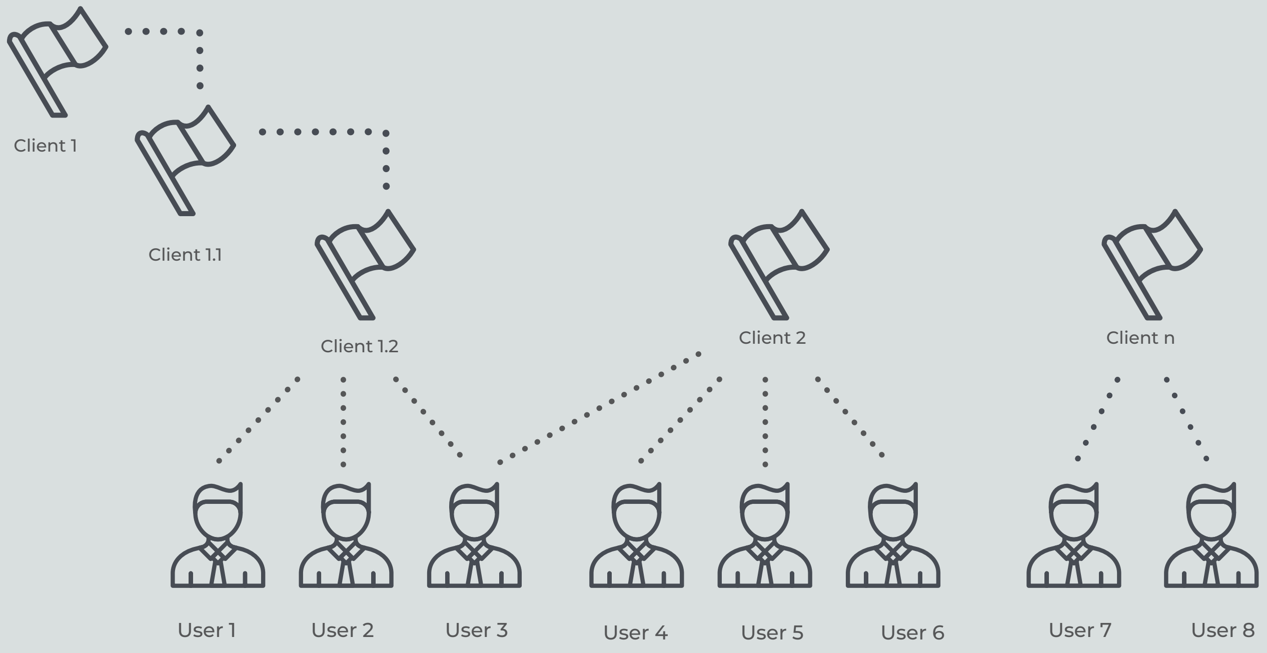
The Remote Service Portal is a self-contained system. Each company is given its own account (corporate account) within this cloud service.

This account provides access to a secure area within the overall server or cloud structure, which comprises a dedicated, secure VLAN (virtual network) as well as a dedicated company database. This means each account is self-contained and standalone.

At the heart of the remote access system – and also its central interchange – is the RLConnect24 Remote Service Portal and cloud service.

This portal is used for the administration of all projects, users and devices. Employees with administration rights specify the user rights for both internal and external employees. This ensures that only uniquely authenticated users are allowed to access a secure area of the network. Access rights to the router and the devices lying behind it – i.e. the machinery and production line components – are also strictly controlled and defined by policies set by the administrators.

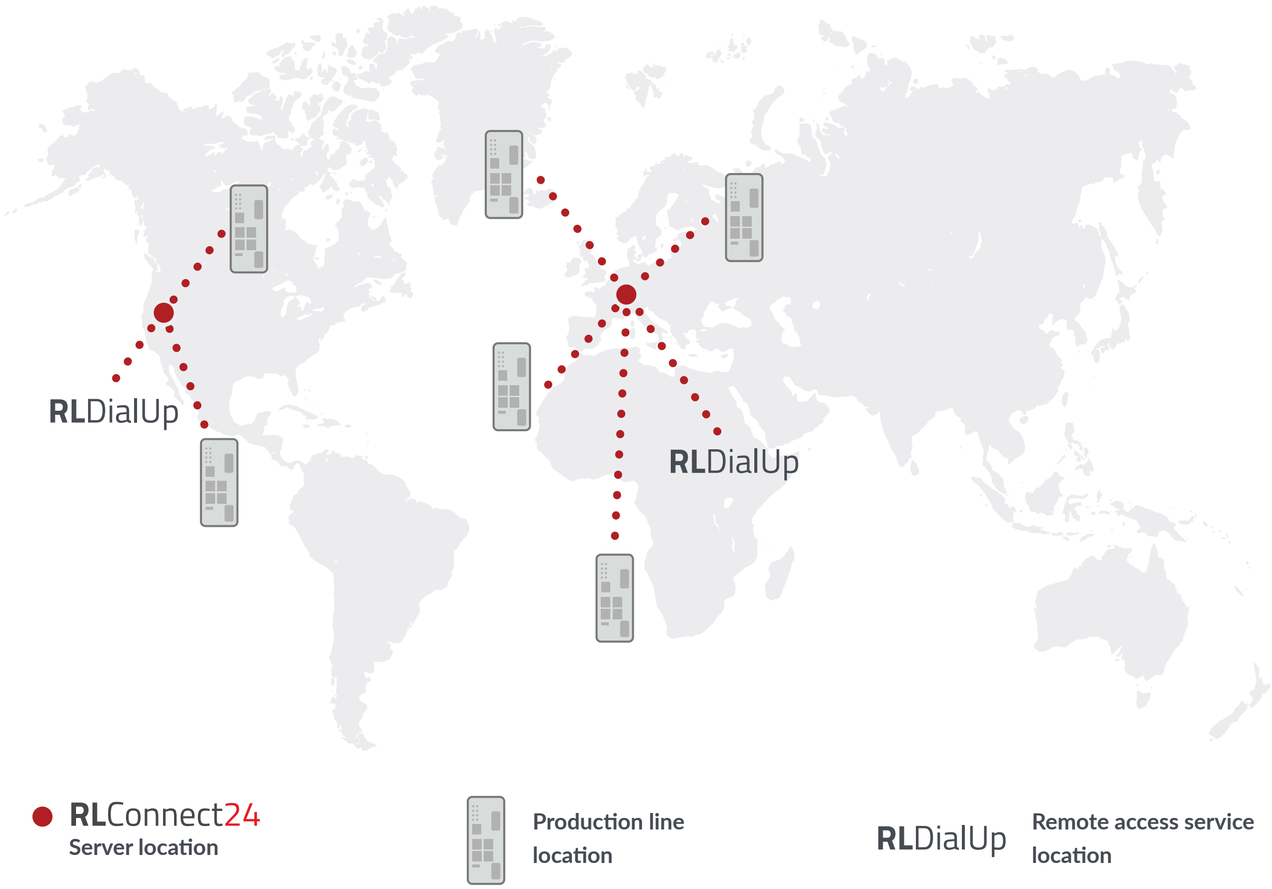
Each and every connection between a user's PC or mobile device at one end and the machine interface at the other end is established only by the cloud service. Accordingly, this Portal is the only legitimate route for gaining access to the machine network. Both on the machine side and the user side, access to the cloud is made only by means of outbound connections. This use of outbound connections means that inbound connections are blocked by the corporate firewall, which provides significant improvements to IT security.



Sample user administration diagram

Strict user-access control

Rights management requires clear definitions and assignments, and can be designed on an individual basis or consolidated into system clients. Individual rights can also vary for each user from one component to another: the user can receive comprehensive rights of access for some router data and be granted only read-only access or no access at all for other types of information. Defining these kinds of fine-grained rights is up to the administrator. Rights of access are therefore defined clearly at all times. To add a further level of control to user/rights management, the client system can be used to define rights or sub-rights to projects and devices at a finer and more precise level of detail. Rights management and verification is all handled by the cloud. Each access is logged with details of the username, time and duration of access and can therefore be traced at any time.



Servers

In physical terms, the cloud or RLConnect24 Remote Service Portal runs on computer architecture in a data center. This Portal provides the administration interface that is used to handle remote access simply and intuitively.

This service can be provided globally with low-latency access times by means of just a few servers located worldwide. Red Lion runs from a total of two server locations based in the USA and Europe.

Each server location is autonomous and is operated within a secure area inside the high-security data center. The individual locations are not networked together. When a company account is created, the company chooses a fixed location to be used from this point onwards. The data are then defined and stored securely at this location. Each location has a unique IP address. This ensures that there is only one point of access to this server location. This simplifies the integration of the components with machinery and production lines, since each integration of the remote access system requires only a single interface and therefore the entry of just one IP address.

Alongside the hosted server model, Red Lion also offers an on-premises solution. With this solution model, myRLConnect24. virtual can be integrated into a variety of IT environments – both in-house (on company premises) as well as in selected hosting centers run by the company. This ensures that the company has sole and unrestricted access to all system data and functionality. In addition, the on-premises variant also offers additional features such as Active Directory (LDAP) integration for users and a white-label option.

The third aspect relevant for IT security is the connection made from the user to the Remote Service Portal. The user has two options here. The simpler variant is to use a browser to log into the Portal over a secure HTTPS connection. The connection to the device is also a secure HTTPS connection handled by Web2go. If a transparent TCP/IP network connection needs to be established, however, then access is made from a PC with the VPN client program RLDialUp. This program provides the secure VPN tunnel required for this variant.

Web-based visualization

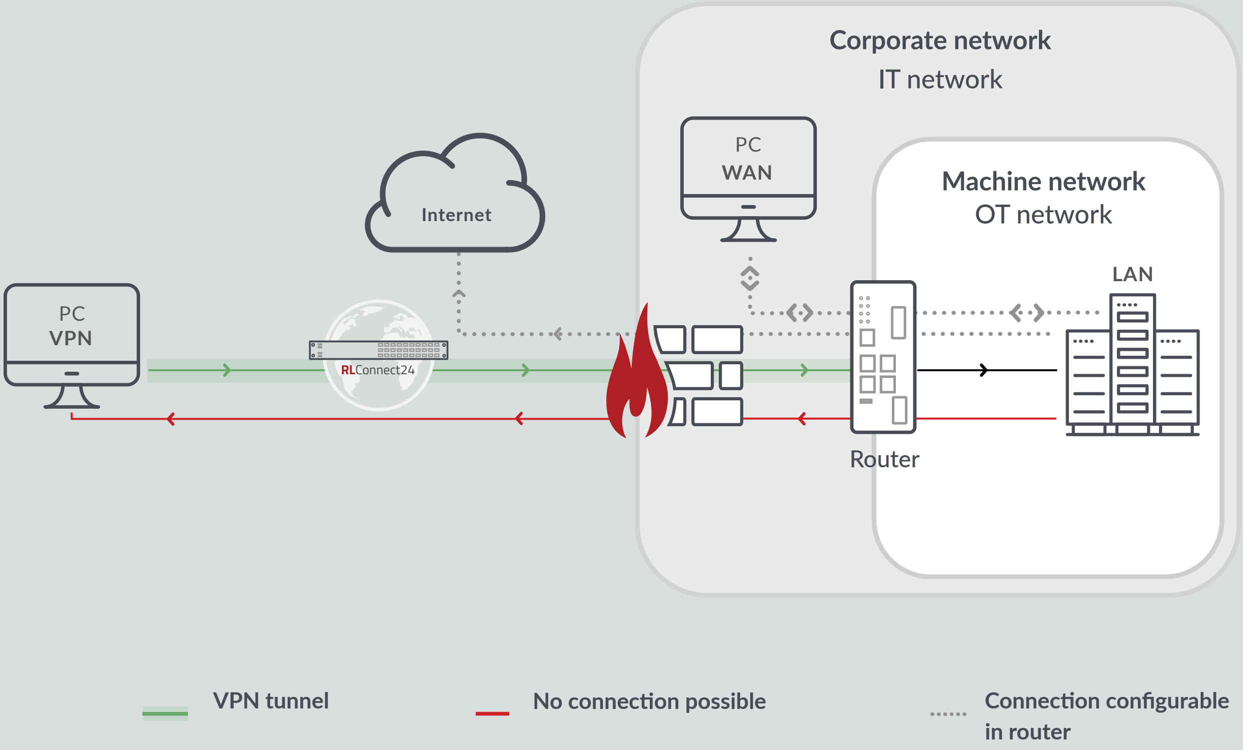
The web-based variant offers the option of monitoring and visualizing system states as well as accessing applications and user interfaces. As a first step, the user connects to the cloud over HTTPS with a web browser. Following this, Web2go then establishes a connection to the device. No other tools or programs are needed.

On the machine side, the router allows only traffic through for protocols such as RDP, VNC, or web in this case. The user can open a Remote Desktop connection to access HMIs or to access control displays and indicators, and can also intervene as permitted by the respective application. All access is permitted that would also be possible if the user was operating the device locally. Each access is logged with user name, time, duration and device and is therefore transparently traceable.

Remote access to the network

To establish protocol-independent TCP/IP network connections and allow access to control systems (for example), the VPN client software RLDialUp must be installed on the PC being used for remote access. The user can only access the control systems if they are using this software to log in to the Remote Service Portal. All of these access sessions are also logged, with details of the user, time, duration, and selected router all being recorded.

MACHINE SIDE: ROUTER



Integrating the router into the corporate network

The router connects the machine or production line to the Internet. The router is positioned between the corporate network and the company's machine network.

Integrating the router into the corporate network

An enterprise network is usually split into a corporate network (the IT network) and a machine network (the OT network). The corporate network is separated from the Internet by the corporate firewall. The router, in turn, separates the machine network (LAN) from the corporate network (WAN). A remote user at the "VPN" PC accesses the router via the VPN tunnel, from where they can then access their authorized devices on the LAN. This connection cannot be used to access the corporate WAN. The router also controls access between the WAN and LAN. When on company premises, an employee can use their "WAN" PC to access the OT network from the IT network, which is also possible vice versa with an appropriate router configuration. A connection to the "VPN" PC from the LAN is never permitted, nor can it even be configured.

Router technical specifications

Since the router uses outbound connections to the cloud, no inbound ports need to be opened in the corporate firewall, so the network is protected from direct access from outside the company. Once the router has used this approach to set up a VPN tunnel to the cloud, data can be transferred between the cloud and the router, and between the user and the device. The router needs to offer the very highest level of IT security, both as regards operation and in terms of its hardware. Red Lion follows both these approaches – known as Security by Default and Security by Design – in parallel.

Security by Default

Security by Default relates to the router configuration. In its out-of-the-box configuration, all of the router's security features are activated. All traffic from IT to OT is blocked by the firewall, with only the absolute minimum permitted from OT to IT. This ensures the very highest level of IT security. If security features need to be deactivated, the router configuration must first be changed. To maximize the level of IT security during commissioning, each router is shipped out with an individual and unique password. Red Lion has deliberately avoided using default out-of-the-box passwords for its routers.

> The very **highest level** of IT security.

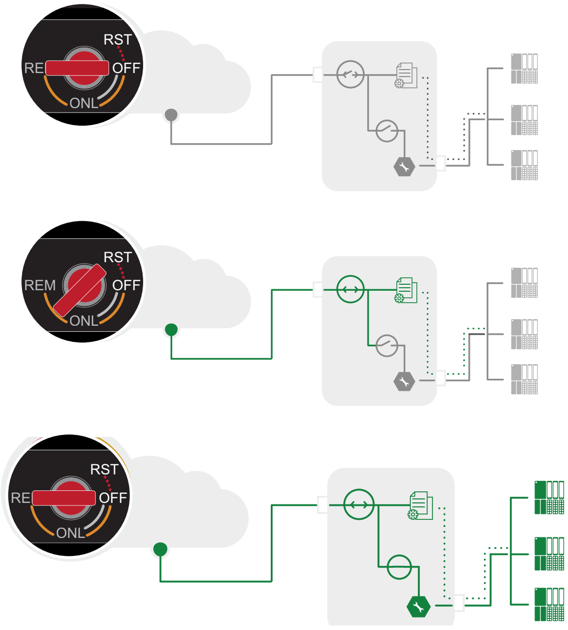
Security by Design

At all times, Red Lion has focused on achieving the highest level of IT security at the product or system development stage, and aligning all actions taken with this philosophy. This is implemented with Security by Design. The foundation for the chain of trust is established by the boot software. This software is stored in read-only memory (ROM). Accordingly, this software cannot be changed during operation. The firmware is signed with a certificate issued by Red Lion. The boot software verifies the firmware stored in memory as part of the secure boot process. The firmware is only loaded and started if the firmware was signed with the certificate stored in the router. Configuration data and user data are encrypted and stored in non-volatile RAM (flash memory). The individual key to decrypt these data is stored in the hardware secure element, which is comparable with a safe. This means that only the router itself has access to the data.

Router with key switch

The RA70K router features an integrated key switch. This switch can be moved to one of three key positions, as well as an extra actuating position "RST" for resetting the router to its factory settings.

RA70K router with key switch



▨ Internal services, data

⬢ VPN/LAN routing

When in the "OFF" position, the router blocks all traffic to the Internet and is also shown as offline in the cloud.

In the "ONL" position, the router is online, has access to the cloud, and is also shown online in the cloud. In this switch position, access is permitted only to the router's internal services, such as the configuration interface.

Only when the switch is moved to the "REM" position is a connection allowed between the remote user and the LAN, and routing to the device is possible. If a router with a key switch is deployed, each remote access session will require a local contact person available on site. This person operates the key switch, thereby enabling access to the LAN. To prevent cases of unauthorized remote access, each router is provided with a set of two keys: a black key and a red key. The black key can only be turned to the "ONL" and "OFF" positions. The "REM" and "RST" positions can only be reached by using the red key.

IT security features

- Equipped with a stateful firewall featuring an IP filter, simple NAT, 1:1 NAT, and port forwarding
- All of these security settings are activated out of the box (Security by Default)
- OpenVPN as the VPN connection protocol
- Routine security patching
- Comprehensive IT security features such as secure boot and hardware secure element

USER SIDE:

CONNECTION TO THE REMOTE SERVICE **PORTAL**

The third aspect relevant for IT security is the connection made from the user to the Remote Service Portal. The user has two options here. The simpler variant is to use a browser to log into the Portal over a secure HTTPS connection. The connection to the device is also a secure HTTPS connection handled by Web2go. If a transparent TCP/IP network connection needs to be established, however, then access is made from a PC with the VPN client program RLDialUp. This program provides the secure VPN tunnel required for this variant.

Web-based visualization

The web-based variant offers the option of monitoring and visualizing system states as well as accessing applications and user interfaces. As a first step, the user connects to the cloud over HTTPS with a web browser. Following this, Web2go then establishes a connection to the device. No other tools or programs are needed.

On the machine side, the router allows only traffic through for protocols such as RDP, VNC, or web in this case. The user can open a Remote Desktop connection to access HMIs or to access control displays and indicators, and can also intervene as permitted by the respective application. All access is permitted that would also be possible if the user was operating the device locally. Each access is logged with user name, time, duration and device and is therefore transparently traceable.

Remote access to the network

To establish protocol-independent TCP/IP network connections and allow access to control systems (for example), the VPN client software RLDialUp must be installed on the PC being used for remote access. The user can only access the control systems if they are using this software to log in to the Remote Service Portal. All of these access sessions are also logged, with details of the user, time, duration, and selected router all being recorded.

Technical data for web-based remote access

- Secure, mobile web access via HTTPS
- Access to web servers and IP cameras
- Support for RDP/VNC protocols without dedicated clients or apps
- Only a standard, HTML5-capable browser is needed
- Independent of operating system on the device
- Enables monitoring and visualization independently of desktop PCs

Technical data for remote access with client VPN software

- VCOM: Tunnels virtual COM ports to the COM interface from RA70
- USBoverIP: Tunnels a virtual USB port to the USB interface from RA50/70
- SEARCHoverIP: Multicast for industry-standard PLC programming environments
- TCP/IP Ethernet protocols

IT **SECURITY**

As an independent mid-sized enterprise, we are a pioneer in the field of solutions for Internet-based industrial communications. Our specific business focus is secure connections to machinery and production lines for remote access, data capture, and IoT applications.

Security is a question of awareness

Which security risks arise in the context of industrial communication? We ask ourselves this question at every stage in development. Secure systems and equipment can only be the result of a secure development process. The development engineers who work at Red Lion have relevant certification according to a TÜV expert certification program for secure software development (TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.)) and expertise in the field of IT security.

Security is a shared goal

Red Lion works closely with a number of IT security companies. This ensures we can uphold the security promises made for our solutions and have our development work validated. We are also an active member of the Industrial Security Working Group at TeleTrusT. This work has produced the IEC62443-4-2 evaluation method, which we use to measure and test our product security. Our broad experience and the range of perspectives offered by our employees are decisive factors that ensure our products are designed securely but without losing sight of usability.

Security by design

Our goal is to design business workflows and use cases to be as secure as possible, and to ensure IT security is incorporated from the outset in development work. Keeping potential points of attack in mind is therefore an important part of the development process. Another all-important aspect is usability. We always aim to reduce complexity to a level where user error is virtually impossible. This applies across the entire product lifecycle. Even when a device is ready to be scrapped, it still cannot be used for the extraction of any useful data.

> We see IT security as a **board-level responsibility** and something on which our future success is absolutely dependent. Understanding how IT and OT can work **together** is a challenge that we gladly accept.

RED LION
EXCELLENCE. REDEFINED

Security as a process

We see pen tests as an important part of the product maintenance process – and not as the last step before a product launch. Our security testing work always begins before the product is officially released on the market. We audit and validate R&D decisions, conduct routine penetration tests, monitor new threats and their effects as soon as they appear, and prepare systematic updates and patches. In our company, IT security is a process that lasts as long as our product lifetimes.

Security as culture

IT security is a part of our corporate DNA. Our R&D staff regularly attend TÜV-certified training courses and we have also established an active **Product Security Incident Response Team** (PSIRT) within our own company. At all times, we strive to deliver products that offer state-of-the-art security.

Our security strategy: an overview

We are an active member of the Industrial Security Working Group at TeleTrusT. This work has produced the evaluation method for IEC62443-4-2.

The "State of the Art" document as published by TeleTrusT is one of our key IT security guidelines.

Our Product Security Incident Response Team (PSIRT) continuously monitors all development work, and conducts analyses to determine how new threats and newly discovered vulnerabilities could impact our products.

We commission regular penetration testing for our products and services from certified external IT service providers.

Certification and auditing

Our products are subjected to both automated and manual penetration testing at regular intervals by independent IT security consultants. After each penetration test, an in-depth analysis session is organized for the penetration testers and our developers.

Industrial applications have a number of different certification options, such as the IEC 62443 standard. We have worked closely with TeleTrusT here to develop a catalogue of tests that is now applied to our products. The IT security "State of the Art" as published by TeleTrusT is also an important tool that we use in our product development.

TeleTrusT

TeleTrusT (IT Security Association Germany) is a wide-ranging network for excellence in IT security whose members are drawn from domestic and international manufacturing, public administration, and research, as well as partner organizations with similar objectives. Our products are entitled to bear the "IT Security Made in Germany" and "IT Security Made in EU" labels as issued by TeleTrusT.

Alliance for Cyber Security

The German Alliance for Cyber Security works closely together with the Federal Office for Information Security (BSI). As an active member, we are the first to know about potential security threats. This ensures that our development engineers are not only able to respond to these risks but can also take steps to prevent them. The effectiveness of these prompt interventions is demonstrated by the automated and manual penetration tests successfully passed by our products. They are also an incentive to plug every security hole and make every effort to ensure IT security standards are met.

CERT@VIDE

CERT@VDE is an IT security platform set up by the German Association for Electrical, Electronic & Information Technologies (VDE) for companies working in industrial automation, with the aim of coordinating IT security risks. The platform offers manufacturers, integrators, plant engineers, and operating companies working in industrial automation an opportunity for the in-depth and confidential exchange of views and information, as well as specific support on the topic of cyber security. A CERT (Computer Emergency Response Team) is often a customer requirement and therefore forms part of purchasing conditions. To stay competitive, companies must ensure that they can provide the corresponding resources.

RED LION®

EXCELLENCE. REDEFINED

Red Lion has been delivering innovative solutions to global markets since 1972 through communication, monitoring and control for industrial automation and networking - enabling companies worldwide to gain real-time data visibility that drives productivity. Red Lion is part of Spectris plc, the productivity enhancing instrumentation and controls company.For more information, please visit http://www.redlion.net.