Secure Remote Access (SRA)

Providing secure remote access to critical control applications

In an ever evolving digital landscape with constant uncertainties, there is an increasing demand for secure connectivity to enable people to work from home or remote locations.

Many organizations require that people can connect to industrial control system components as if they were still located physically on site, with the highest levels of security considered. Whether for maintenance, support, or even aspects of system operation; fast, reliable and secure connections are required wherever your key experts are located.

Typical VPN solutions are complex to set up and maintain and provide limited or no access to OT systems. Hardware systems don't provide the flexibility and access required to the resources needed to keep your operation running smoothly.

The Schneider Electric™ Cybersecurity Services team provides a solution that enables your key personnel to remotely access their OT assets and applications while away from site in a secure and safe manner. This connectivity enables them to monitor their assets, and subject to appropriate authorization, permit them to control and carry out maintenance tasks on the asset/applications. If needed, this functionality can be extended to third party vendors as well.

Our solution sits within the existing client infrastructure and uses existing hardware, to the extent possible, within the client's location.

Key Benefits

- **Reduce risks** for remote connections to OT systems.
- **Enables fast, secure access** as required to support key operational roles.
- **Easier to manage** than VPN with greater security, OT connectivity and full audit capability.
- **Full monitoring and auditing,** provide confidence and meets audit protocols.
- **Knowledgeable and experienced experts** from Schneider Electric™ provide implementation and maintenance support.

se.com/cybersecurity

Life Is On Schneider Electric

Solution Features

The Schneider Electric™ Secure Remote Access (SRA) solution is a subscription-based service that allows enterprises to extend access to critical assets - without compromising security.

There are two main components of the solution:

1. **SRA Platform installation (one-time expense)**
   - Schneider Electric™ installation, deployment and step by step initial configuration.
   - Work can be performed remotely, with support from local customer resources.
2. **SRA Subscription services**

   Provided as a recurring Schneider Electric™ annual subscription for:
   - Secure Remote Access (SRA) platform for the central and site components.

     Software for central server:

     Software loaded on the IT side of customer's infrastructure that can be configured to allow remote sessions and has access to the internet. These sessions can be regulated by an administrator who authorizes or declines the users.

     Software for site server:
   - Software loaded on the OT side of the customer's infrastructure that connects the remote user to the specific asset on which the remote user is authorized to work.

     Post deployment maintenance support for the platform and operations
     - It is assumed that existing servers at the client's site will be used.
     - Installation and deployment to be done remotely - details below.

Prerequisites

- Network - a basic security infrastructure with corporate and process control networks segmented with firewalls as listed in Figure 1 below.
- SRA central server - a bare bones server or Virtual Machine infrastructure on the IT side for the SRA central software installation. A Virtual Machine image can be imported into the customer's virtual infrastructure.
- Site server - a bare bones server or Virtual Machine infrastructure on the OT side for the SRA site software installation. A Virtual Machine image can be imported into the customer's Virtual infrastructure.
- Available Windows Remote Desktop license(s) for target assets.
- A technically capable customer employee or representative, available on-site, to install and configure the software and update the firewalls on site by following instructions and guidance contractually provided by a Schneider Electric™ Cybersecurity Center of Competence (CoC) engineer over an audio or video call (or in-person where possible).

Figure 1 – Typical project activities

1	Mobilization and kickoff
2	Architecture review
3	Functional design specification
	Roles and accounts definition
	Firewall configuration
4	Installation
	SRA central server installation & validate internet connectivity
	SRA site server installation & validate connectivity with central server
	Setup community and testing
	Setup RBAC related to target asset stations and test
5	System testing
6	Training for administrators
7	User training

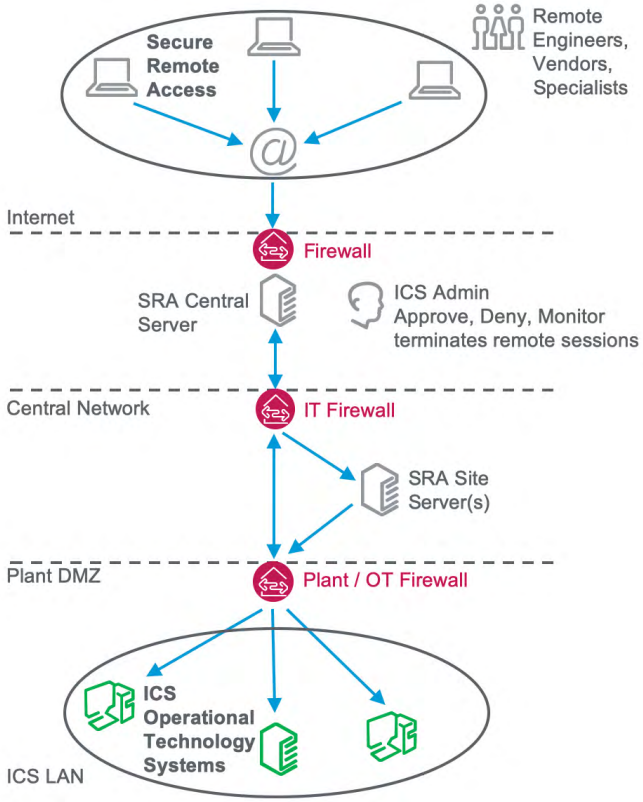
Life Is On Schneider Electric

Installation / Deployment Activities

- The designated resource at the customer's site will be instructed by a member of the Schneider Electric™ CoC in a step-by-step process to install the platform and update the firewalls.
- Once the platform is installed and running correctly, the SRA central system can be configured to allow remote access sessions as required. No setup is required on the end user (remote user) side, only a web browser pointing to a specific URL that references the SRA central server. Both the client interface and the SRA central management console are intuitive and user friendly.
- The site server can be configured to direct the remote user to the specific asset where they are permitted to work. Once configured, the server works independent of any intervention.

Sample Architecture

- Single, manageable interface that all external users connect through, providing a single point of control.
- Enables secure remote connectivity for testing, maintenance and support on Industrial Control Systems.
- Network administrators have full visibility and control over 3rd party and employee accesses before, during and after a remote session takes place, including terminating sessions.
- Supports typical OT application use cases.
- Enforces password management and access control.
- Provides access to registered users for pre-defined systems.
- Fetches a replica of the requested asset's interface, forwards user's input only to the authorized asset.
- Use new or existing site servers with remote Schneider Electric™ support.



Experienced, Capable and Globally Available

Schneider Electric™'s global team of cybersecurity experts understand the unique needs and challenges for OT systems and technologies. Our focus is on finding solutions that fit your unique requirements, regardless of the systems you use.

We work with leading cybersecurity product experts to bring the right solution to your operation to ensure that your people, processes, and technologies are protected.

Contact us today to learn more about our Secure Remote Access offer, as well as other key capabilities and solutions.

se.com/cybersecurity

Life Is On Schneider Electric

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex

cybersecurity-services@se.com

998-20906222