Executive Summary

What will industrial automation systems look like in 10, 20 and 50 years from now?

Everyone seems to have “smart” devices these days. And companies have been busy coming up with new ways to take advantage of the resulting networked information. In the industrial automation world, the trend of connecting more and more devices to the network is called the Industrial Internet of Things, or the IIoT.

Part of the vision of the IIoT is that all relevant data will be available in real-time, leading to faster and smarter decisions. This in turn will lead to the design of more flexible and efficient processes. Many of these industrial processes will use devices with sensing technology to perform automated tasks with efficiency and precision. With the increase in complexity of automated processes, however, comes the opportunity for things to go wrong – especially with a limited human presence in most industrial applications. The ability of these devices to provide diagnostics and feedback has already become critically important.

The success of the IIoT vision largely depends on the underlying communication technologies achieving high performance levels. If the communication infrastructure cannot meet the demanding requirements, many applications will not work as intended. Currently, there are many ongoing efforts to close the remaining gaps with new, innovative enhancements in data communication technologies. There are several challenges to overcome, but from today’s perspective, it will one day be possible to provide all the necessary elements to make the IIoT vision a reality.

One of the gaps the industry is trying to solve is how to provide remote access to plants and machines around the world to allow real-time data exploitation. With this ability, OEMs can offer added-value services like predictive maintenance to minimize systems downtime and even go one step further to offer Machines as a Service.

Belden offers a simple and secure way to provide remote network access, programming and diagnostics for predictive maintenance with the Hirschmann Secure Remote Access Solution. This combined hardware and software system offers companies leverage on the increased connection of devices brought on by the Industrial Internet of Things.
Predictive Maintenance

Predictive maintenance techniques are designed to help determine the condition of in-service equipment in order to predict when maintenance should be performed. This approach promises cost savings over routine or time-based preventive maintenance, because tasks are performed only when warranted.

The main advantage of predictive maintenance is to allow convenient scheduling of corrective maintenance, and to prevent unexpected equipment failures. The key is “the right information in the right time.” By knowing which equipment needs maintenance, maintenance work can be better planned (spare parts, people, etc.). What would have been “unplanned stops” are transformed to shorter and fewer “planned stops,” thus increasing plant availability. Other potential advantages include increased equipment lifetime, increased plant safety, fewer accidents with negative impact on environment and optimized spare parts handling.

Predictive maintenance differs from its cousin preventive maintenance because it relies on the actual condition of equipment, rather than average or expected life statistics, to predict when maintenance will be required.

While predictive maintenance will help machine operators save costs by reducing unplanned downtimes, it will allow machine manufacturers to improve their business as well. For example, knowing about machine failures helps manufacturers plan and offer new maintenance services based on guaranteed uptime or optimize warehousing costs with just-in-time inventory of spare parts. Moreover, it will help increase product quality and shorten release cycles.

Predictive maintenance is only one example in the manufacturing industry where the intelligent usage of data adds value to existing concepts. In the same way, the IIoT will offer new possibilities in optimizing production or logistics processes.

How IIoT refines the concept of Remote Maintenance

Remote maintenance services have been used in the manufacturing industry for many years to maintain spatially distributed machines and equipment. Using a dedicated line, service engineers can establish a connection to a machine and access its control system. Depending on the available transmission mode and access rights, the engineer can provide passive assistance to on-site machine operators or even take active control of the system. The benefits are obvious: remote maintenance slashes travel and personnel costs while improving customer service by offering faster response times.

A recent surge in demand for remote management has fueled a boom in the availability of remote maintenance software for industry applications. However, many of these programs lack the necessary flexibility and “intelligence.” Typically, a separate PC or desktop environment must be set up for each active machine. In addition, the applications are not usually integrated in the existing system environment, so the data they collect cannot be incorporated into these systems unless it is entered manually or copied from a USB stick. However, these problems need not exist as technology already provides everything needed to address them.

Modern M2M software replaces the rigid structure of isolated local computers and 1:1 connections as it offers the possibility of connecting, managing and controlling an unlimited number of machines in virtual networks. This way, service engineers have an overview of all machines and can take action in the operating process remotely from one single access point. This provides a great benefit, but what manufacturers really profit from is the availability of all machine data.

Requirements for a Secure Remote Access Solution

Prior to selecting an industrial communication solution that may be both strategic and mission-critical to the business, a managing decision maker will typically have a number of concerns and questions about the main requisites to make the choice:

- The solution must be designed specifically for the automation industry and has to respect industry requirements that may differ from other sectors like banking.
- The solution must be secure, as this is one of the main concerns for plant managers when enabling external connections to their devices.
- The solution has to offer end-to-end encryption and cannot allow leaks or add vulnerabilities to the system.
- The solution must be easy to deploy and service by maintenance engineers without requiring highly skilled or certified IT experts.
- The solution must comply with safety standards. Remote connections to machines need to be signalized and must respect operational safety (think of motion-based equipment).
Hirschmann Secure Remote Access Solution (SRA) components

Let’s explore an example of a remote access system that meets the needs of IIoT-driven automation environments.

The Hirschmann Secure Remote Access Solution (SRA) provides a protected cloud system that can be set up with minimal assistance. Permanent IP addresses are not required, and there is no need to reconfigure firewalls. This enables secure access for remote programming and diagnostics without disrupting existing systems.

The system is suitable for many different industries, including food and beverage, machine building, automotive and any application that requires remote access to geographically-dispersed plants and machinery. Remote access reduces the need for travel and allows staff to work more efficiently by handling multiple systems simultaneously.

At the core of the Secure Remote Access Solution is the GateManager that enables customers to connect their operator stations to their remote devices. The GateManager can be installed in a server in the company network or optionally in a public cloud service. LinkManager software, running on PCs or mobile devices, connects operator stations to the GateManager. SiteManager software running on PCs, on the OWL Cellular Router or on the Hirschmann GECKO managed switch connects the remote devices to the cloud.

The simple set-up, ease of use and secure technology make the Secure Remote Access Solution ideal for the implementation of Predictive Maintenance in the IIoT Era.

- The solution must be scalable. In an IIoT scenario, growth in the number of devices and connections must be anticipated.
- The solution must be fully supported, and yet it must be independent of the vendor and future-proof in terms of technology and standards.

Another critical aspect is the solution provider. The provider of the solution must be a dedicated and financially healthy company with resources to provide global support during the whole life cycle of the product.

Transparent Internet Access via Corporate Network

Hirschmann Secure Remote Access Solution operation

The employee of a machine builder, on the right in this diagram, needs to get access to some equipment located on a customer’s site, on the left in this diagram. This access may be for maintenance, troubleshooting, or even a software update.

The connection between the Internet and the customer’s network is protected by a firewall. The firewall will block incoming calls. So it is impossible for the machine builder to get direct access to the customer’s network.

The problem can be solved if both the machine builder and the customer make outgoing connections to a server on the Internet. The connections will use TCP/IP ports which are commonly open on firewalls, for example ports 80 or 443, used for HTML data. So normally no reconfiguration of the firewalls is necessary.

Whichever topology is used, there is an important point to remember. The devices being monitored are never communicating over the Internet. Or to put it in a more technical way, these devices do not need a default gateway. Only the PC running the agent software is connected to the Internet.

In this topology, there is an Engineer with a laptop running the LinkManager client software, see the right side of the diagram. The GECKO or the Windows PC is collecting information about the supervised devices and sending this information to the GateManager server.

All the routing is already in place. In this case, the SiteManager PC can be connected anywhere on the factory floor network. The SiteManager application then needs to be configured. This is certainly the simplest topology.

“Today, some companies prefer to keep data exclusively within their organization. By hosting the GateManager server on the corporate network, rather than the Internet, data never needs to leave a company’s jurisdiction.”

Mark Cooksley, Belden Product Manager
Cloud-based Secure Remote Access Solution versus traditional VPN links

Cloud-based Secure Remote Access Solution and traditional VPNs basically have the same purpose. They allow two IP-enabled devices to communicate securely with each other remotely over the Internet, just as if the devices were connected on the same physical network. Although traditional VPN is widely used and suits the general purpose of interconnecting remote networks quite well, it has some serious drawbacks for remote device monitoring and management.

1. Subnet conflicts
Networks connected via traditional VPN must not use the same local subnet. But a Machine Builder / System Integrator managing hundreds of customer installations is bound to run into lots of locations using the same subnet addresses. Asking the customers to change their addressing schemes is rarely an option, and juggling with NAT rules to deal with the existing addressing schemes can quite simply be a nightmare.

With the Hirschmann SRAS, all sites could have the same subnet, and all equipment could have the same IP address. The engineer and the remote device are simply linked to each other IP-wise at connect.

2. Pre-configured connections are required
Connection between traditional VPN peers cannot be established dynamically upon request but have to be configured beforehand. This needs involvement of IT personnel, and takes time – every time.

Once the engineer with the LinkManager Client has an account on the GateManager represented by his personal x.509 certificate, the GateManager administrator can easily associate the account with exactly the site or group of equipment the technician should have access to, and it is immediately updated in the list of sites available in the LinkManager client.

3. Advanced routing challenges
Connecting two remote networks with traditional VPN via a central VPN concentrator requires configuration and management of advanced forwarding routing rules. Additionally, routing equipment usually needs to be able to support NAT-T and UDP encapsulation.

Relay VPN does not use routing and subsequently no NAT rules are required. IP addresses are simply linked via a central proxy server. Traditional VPN is suitable for one-to-one or many-to-one connections, but not one-to-many (one engineer to many sites), or many-to-many (many engineers to many sites). A cloud-based system for remote access easily administers thousands of engineers needing access to thousands of sites, including management of individual access rights, and even limits access to specific types of equipment, or specific protocols/services of equipment.

4. Firewall opening challenges
Traditional IPSec-based VPNs require special ports to be open, and some firewall protocols allowed to communicate through this configuration may be exploited by attackers.

All relay VPN connections from SiteManager and LinkManager are established inside out, and only standard Web ports are used (such as 443). All these encrypted connections are terminated at the central Internet based GateManager server. Through these encrypted connections, the linking between engineers and devices is dynamically established.

5. Firewall blocking challenges
VPN routes everything and not just the protocols you need, unless efforts are put into creating and managing a number of firewall rules also.

The device agents defined on the SiteManager and LinkManager are automatically limited to only allowing access to the ports or services defined for the agent type. Only these are activated when a LinkManager connects to the agent representing the end device.

6. Certificate management
A good VPN solution is usually based on x.509 certificates that are exchanged or signed by a Certificate Authority (CA). This adds overhead and makes it tedious to set up individual connections.

GateManager acts as the CA authority for both SiteManager and LinkManager clients. The client access is secured by a two-factor system (certificate and password). But the x.509 certificate of the Belden solution is not only a security measure. With LinkManager we have included in the certificate all the configuration details and thereby eliminated the need for the user to configure anything.

7. Activity logging
The principle of traditional VPN is to connect two networks and have everything accessible between the two peers. Therefore, logging is at best only done when establishing the connection, but once connected nothing is logged.

The GateManager server will not only centrally log who made the connection and to which device, but also when the connection was established, and what services were accessed. The log is kept centrally on the GateManager and cannot be deleted by administrators.

8. Managing the “concentrator”
Typical IPSec-based VPN solutions require an IT-administered concentrator, since it requires networking knowledge. Also, individual concentrators must typically be installed at each service provider in order to avoid very complex triangular routing and firewall setups. SSL VPN-based solutions overcome some of the issues of IPSec-based VPNs.

The “concentrator” in a cloud-based solution is a central service in the cloud, where each service provider gets an isolated account. Here the administrator issues account certificates and controls dynamically what equipment and which services were accessed. There is no networking or other IT skill set required.

Cloud-based Secure Remote Access Solution versus traditional dial-up modems

Dial-up modems have been used successfully for decades. Many Internet based solution attempts have been made to eliminate the obvious disadvantages, but it has often been at the expense of the advantages of the dial-up modem concept.

The cloud-based Secure Remote Access Solution has been designed with the workflow of the dial-up modem solutions in mind. It should just be as easy to comprehend, but much easier to deploy and manage, while also addressing the security aspects.
1. Improve speed

Obviously a dial-up from the speed of traditional analog lines. New machines require larger PLC/HMI programs, and transmission time becomes critical. Using the Internet as the carrier is the obvious choice for any remote management solution. Reliability of the connection can also be achieved by having back-up lines.

2. Re-using the existing Internet infrastructure

Dial-up modem solutions obviously need a phone line for both the service engineer and the factory site. Establishing a new analog phone line is expensive and typically takes weeks from ordering to installation, if even available. Additionally you will typically be charged dial-up fees and minute rates. For largescale or global deployments, this is not an option.

A cloud based-solution utilizes the existing IT infrastructure. The local station can connect out through the corporate network firewall and also create a complete separation between the corporate network and the technical network hosting the industrial equipment. Even users that have full access to all equipment in the technical network cannot get access to the corporate network. Optionally, it is possible to make use of a separate Internet connection.

3. Automating the “phone book”

Dial-up solutions are easy to understand and manage. Each site has a unique public phone number. These solutions typically make use of a spreadsheet with dial-up numbers and passwords that are distributed to the service engineers. Adding a new site, however, requires the phone book to be updated. Typically the entire phone book would be distributed to all service engineers, even if some only required access to a few sites.

In a cloud-based solution the “phone book” is centrally administered, by associating customer sites and equipment groups to the accounts. When the service engineer connects with his account, he only sees what the administrator wants this user to see. If the administrator associates a new device or customer site to the account, it will be immediately available to the assigned engineer.

Furthermore, the two-way authentication system (certificate and password) to login into the system will require no further user password access to the remote equipment assigned by the central administrator.

4. Allowing multiple concurrent connections

Dial-up modems limit the number of concurrent users. Typically the line will just be busy when a user attempts to connect while another user is online. This may be acceptable if the modem is dedicated to one service on the machine, but not if the modem is supposed to be an entry point for multiple services on the device.

A cloud-based solution would allow simultaneous access by multiple users to multiple services on the same device (HTTP, TELNET, FTP, remote desktop, PLC programming, SCADA systems, etc.). Also SiteManager supports access to multiple machines at the same site. Additionally, the account management system assures that on the same machine one user can access only certain services (e.g. HTTP), and another user can access other services (e.g. PLC programming ports) depending on each one’s privileges.

5. Revoking access for former employees

A known problem of dial-up modems is the security issue when service engineers leave the company, as they will have access to phone numbers and passwords. A disgruntled former employee can make much damage.

When a user of a cloud-based solution leaves the company, the administrator disables the associated account and instantly the user’s certificate will be invalidated. Also the administrator can issue a time-limited certificate that expires (perhaps after a day or a week) for specific maintenance purposes.
Other Network Topologies for Secure Remote Access

Internet Access via Corporate WLAN Networks
In this scenario, the factory floor network does not have a connection to the corporate network, and therefore no Internet access. A stand-alone Wireless LAN Client is used to create a connection to a Wireless LAN Access Point which is connected to the corporate WLAN.

Internet Access via Cellular Networks
In this scenario, no Internet access is available at all. So Internet access is provided by a 3G or 4G cellular modem. In the diagram below, the OWL, a Hirschmann cellular router, is providing the connectivity. But this will work just as well with a simple USB modem solution. Many standalone routers, including the Hirschmann OWL family, allow an Internet connection to be established by sending an SMS message to the router. In any case, the Internet connection should only be established when remote access is required.

GateManager Hosting Options
The simplest solution is to use a Hirschmann–hosted GateManager. These are pre-configured and ready for immediate use. A second option is for a company to use its own cloud server. For example, the GateManager is available as an Amazon Web Services machine image. The third option enables a company to host the GateManager on its own corporate network.

Main benefits of a Predictive Maintenance program
There are many advantages of using a predictive maintenance program:

- Provides increased component operational life and availability
- Allows for preemptive corrective actions
- Decreases equipment and/or process downtime
- Lowers costs for parts and labor
- Provides better product quality
- Improves worker and environmental safety
- Raises worker morale
- Increases energy savings

Main benefits of a cloud-based Secure Remote Access Solution
Expanding network reach without complex programming brings additional benefits:

- Secures remote access, diagnostics and PLC programming via a flexible hardware and software solution
- Allows the use of your standard PLC and HMI tools, just as if you were onsite
- Provides instant support to ensure machine uptime with a global reach
- Facilitates machine operation without physical access
- Enables service to global customers without the expense of travel
- Connects to remote devices via a secure cloud link
- Reduces the IT knowledge required to set-up system
- Eliminates the need of permanent IP addresses
- Firewall friendly – no need to reconfigure company firewalls
- Avoids the complexity of virtual private networks (VPNs)
- SiteManager software runs inside Hirschmann GECKO switches
- GateManager can be hosted by customer or in a cloud service
Summary

Predictive maintenance is no longer an option in industrial operations. It’s a mandate. You have to find more ways to reduce downtime, prevent injury, extend the lifetime of capital investments, be more energy-efficient and cover broader – sometimes global – geographies.

Traditional methods through VPNs, dial-up modems, corporate WLANs or cellular networks don’t measure up to today’s faster, more powerful cloud-based solutions. Plus, you’re likely juggling the need for centralized control across your operations without the constant hassle and cost of moving engineers and service technicians from site to site.

But choosing a platform for your predictive maintenance program can be confusing and intimidating. In this white paper, we’ve shared our analysis of various topologies and how they fare in today’s IIoT-connected marketplace. We’ve also explored one cloud-based solution that combines hardware and software to simplify remote network access, programming and diagnostics with utter security and reliability – the Hirschmann Secure Remote Access Solution.

With minimal IT expertise required, the three-component Hirschmann SRA solution gives you state-of-the-art protection as you remotely connect to, assess and even modify or repair PLCs and other network components. You get immediate, real-time results to keep production lines up and running, worry-free.

Managing multiple remote locations from a headquarters location requires a cloud-based solution built for speed and security.

The system’s three parts are:

**GateManager** – operates as a cloud service; hosted by Hirschmann or hosted by your company

**SiteManager** – makes it possible to connect remote devices to the GateManager cloud; runs on a Windows PC or Hirschmann GECKO switch hardware

**LinkManager** – provides secure, on-demand access to remote devices via the cloud; can be run from anywhere on a computer, tablet or mobile phone as long as there is a connection to the GateManager server; no local network access is needed

With technology revolutionizing every aspect of industrial production, make sure your predictive maintenance program can meet all your demands for safe, reliable operation.
Belden Competence Center

As the complexity of communication and connectivity solutions has increased, so have the requirements for design, implementation and maintenance of these solutions. For users, acquiring and verifying the latest expert knowledge plays a decisive role in this. As a reliable partner for end-to-end solutions, Belden offers expert consulting, design, technical support, as well as technology and product training courses, from a single source: Belden Competence Center. In addition, we offer you the right qualification for every area of expertise through the world’s first certification program for industrial networks. Up-to-date manufacturer’s expertise, an international service network and access to external specialists guarantee you the best possible support for products. Irrespective of the technology you use, you can rely on our full support – from implementation to optimization of every aspect of daily operations.

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today’s applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at www.belden.com and follow us on Twitter @BeldenIND.