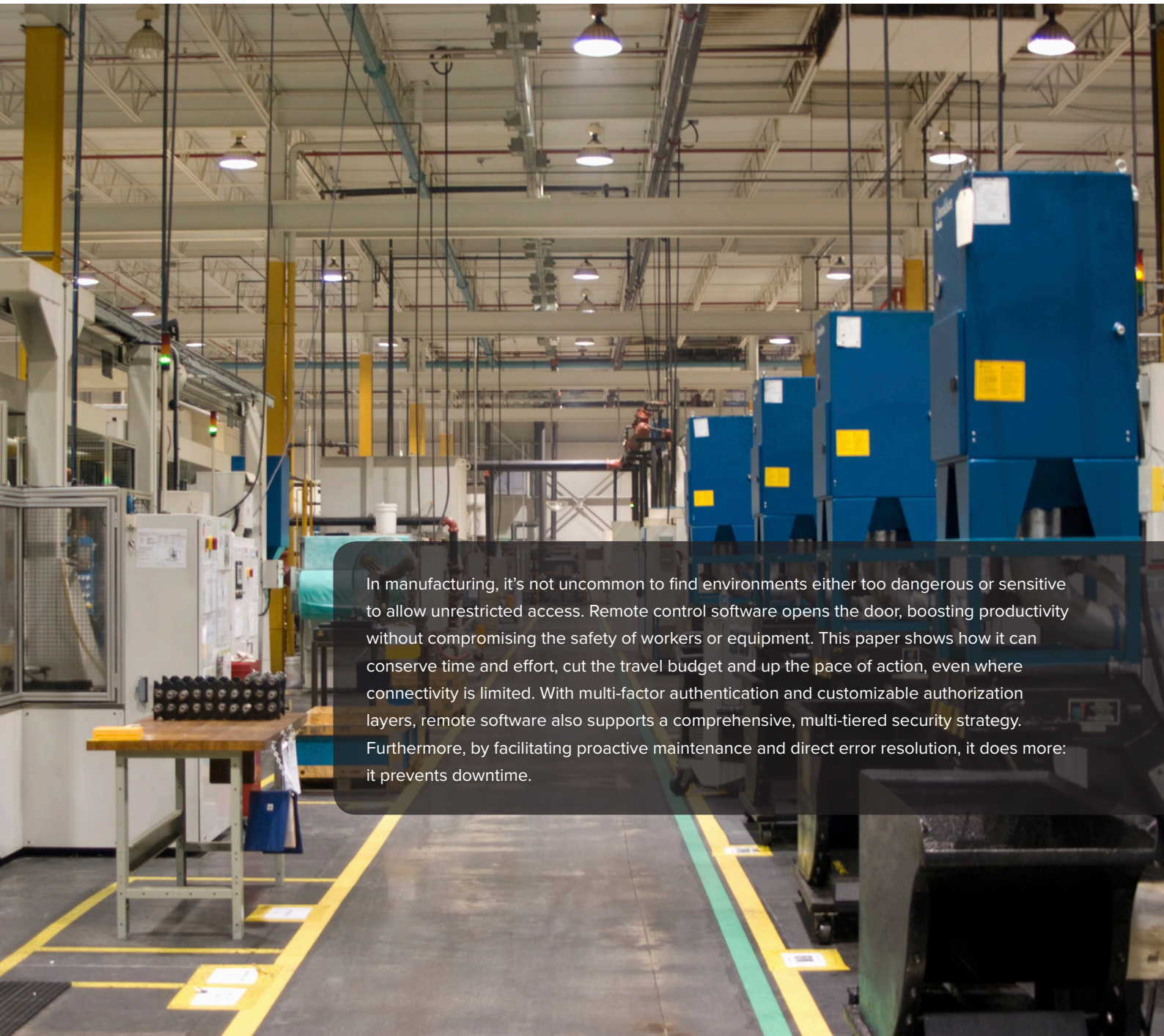
MANUFACTURING

NETOP® Remote Control

Remote Control in Manufacturing

Entering Closed Environments Without Opening the Door



In manufacturing, it's not uncommon to find environments either too dangerous or sensitive to allow unrestricted access. Remote control software opens the door, boosting productivity without compromising the safety of workers or equipment. This paper shows how it can conserve time and effort, cut the travel budget and up the pace of action, even where connectivity is limited. With multi-factor authentication and customizable authorization layers, remote software also supports a comprehensive, multi-tiered security strategy. Furthermore, by facilitating proactive maintenance and direct error resolution, it does more: it prevents downtime.

In the manufacturing industry, it's not uncommon to find environments that are either too dangerous or too sensitive to allow unrestricted access.

The restrictions may be physical, virtual or both. Workers must physically suit up before entering a clean floor or dealing with hazardous chemicals. Virtual restrictions, such as limited Internet access, are equally important. Online security breaches are not the only risk; even something so banal as an automatic software update could prove disastrous, if an unexpected reboot brings production to a halt.

Environments like these are closed for good reason. Their operators must protect worker safety and the equipment itself; they must adhere to compliance standards, such as OSHA. At the same time, they're responsible to maximize production and eliminate idle time to the greatest possible extent.

Remote access software strikes at each of these needs. It conserves time and physical effort, letting technicians control machines without having to walk onto the production floor. Even where connectivity is restricted, remote access ups the pace of action and cuts the travel budget. It offers technical safety provisions in the form of sophisticated, customizable layers of authorization (part of a comprehensive, multi-tiered security strategy). Finally, by facilitating proactive maintenance and direct error resolution, it does more: it prevents downtime.

Benefits on the Production Floor

The difference between one solution and another can be measured by the benefits it provides. In fact, these benefits reach beyond the production floor, as companies that have integrated remote software throughout the enterprise can attest. When evaluating a potential solution for your company, please bear in mind the following criteria.

COST SAVINGS – Travel Less, Produce More

Robotics, assembly automation, image processing, warehousing and transport systems – every aspect of the industrial process demands attention from time to time. Furthermore:

Quick and effective response to issues on the production floor often requires real-time access to information and status from industrial automation and control systems as well as the skills and knowledge to take corrective action or optimize the production process. (CISCO, 2009)

Many manufacturers do not staff in-house technicians with the skills to resolve these issues. It's simply not practical: failures may be rare, and specialists are few. Thus, the issue requires a service call – however, service calls cost. Someone has to pay for a technician's travel expenses, either the vendor or the customer.

Features to Select For

Within closed manufacturing environments, the benefits of remote software are oriented around four points:

- The return on investment should include a lower operating budget and fewer hours spent in downtime.
- Even in closed environments, it should be able to establish a connection between a control computer and the machines to be maintained – without compromising security.
- It should include customizable authentication options, ensuring need-to-know access for hundreds to thousands of individual technicians.
- Finally, it should equip operators to prevent errors proactively and trace problems back to their source for immediate resolution.

To avoid expense, some companies may opt to resolve issues virtually using high-risk, short-term connectivity, along with the extensive help of a specialized IT security team:

> This may appear attractive, especially when failures are infrequent. But a closer look shows that risk associated with manual, ad-hoc methods is too high, coordination is very stressful and benefits associated with advanced service support opportunities are precluded (“DEFINING STRATEGIES,” 2007)

Even with a technician in town, travel takes time – while downtime may be costing the company thousands of dollars a minute. In fact, technicians in-house cannot respond immediately either when facing hazardous or sensitive environments; they have to suit up first. In either case, if hands-on maintenance is needed, it’s likely the equipment will have to remain standing idle for the IT specialist’s protection while they work.

Remote access software presents an obvious alternative. It lets companies deploy technicians in-house, across town and across the world, securely, without the time or cost of waiting. With such a tool available, it no longer makes sense to send highly skilled technicians on long business trips. For a medium-sized company with a globally distributed customer base, remote access software cuts the budget and speeds error resolution.

It also prevents downtime. When problems arise on highly specialized manufacturing equipment, an operator can address them immediately through remote intervention, instead of letting production fall idle. Unscheduled downtime is remarkably expensive, initiating an enormous ripple effect whose total impact is difficult to fathom. With remote access, this is money saved.

Of course, scheduled downtime is best kept to a minimum, as well. Here again, a good remote solution proves its worth. A company should be able to keep machines running through remote diagnosis, achieving better productivity with fewer dollars spent on downtime. This is no small gain:

> Manufacturing systems, in particular, often operate at less than full capacity, productivity is low, and the costs of producing products are high... a large percentage of the total cost of doing business is due to maintenance-related activities in the factory; i.e. the costs associated with maintenance labour and materials and the cost due to production losses. (BLANCHARD, 1997)

By minimizing downtime – both scheduled and unscheduled – remote access software supports the ultimate profitability of the company.

CONNECTIVITY – Safe Contact for Closed Environments

Of course, potential profitability means little if the solution can’t establish a connection in the first place. Especially in closed environments, the importance of connectivity is not to be underestimated.

How to Establish Connectivity?

There are several viable approaches. For example, a solution may use its own gateway with only one open destination port to connect to an internal network of machine-integrated computers. Although these computers often have neither input nor output options, and are not visible to the company network, they may then connect to the control computer through the remote solution’s gateway.

To safeguard security, the software may be installed on the inside of the perimeter firewall; here it can be configured to allow only the TCP User Datagram Protocol (UDP) network protocol, while any change of protocol (or translation) can occur only through its own gateway.

Regardless of particulars, a remote solution should be able to overcome each obstacle to connectivity with a strategy that’s not only effective, but safe.

In these situations, where a digital connection does exist, it's often a single point of entry. The remote solution's job is to establish communication between the computer running the support module and any machines (or production lines) to be maintained, despite possible limits in bandwidth or dial-up connections. It also needs to get past the firewall without compromising perimeter security defenses or creating back doors into the manufacturing system ("Defining Strategies," 2007). Where data transfer is involved, it should provide industry-standard, regulation-compliant encryption.

If a remote solution cannot accomplish these things, it's simply not the right choice for a closed manufacturing environment.

AUTHORIZATION – Customized Settings Meet Complex Needs

In the past, all remote maintenance in mechanical and plant engineering happened over point-to-point connections. At that time, it was much simpler to control who had access to which systems. Today, however, entire production lines are integrated into the customer network, and a challenge is born: the manufacturer of a given machine needs access to perform its maintenance or repair; however, they must not be allowed to access other systems from other manufacturers.

The scenario calls for complex layers of authorization. However, the most common authorization tools, such as Active Directory, are not relevant in this setting. In automotive engineering, for example, the manufacturer of a given machine would not be listed in the Active Directory of the automotive company.

Thus, a remote solution must provide different levels of access, based on the context of the issue:

> Strong security is still a fundamental requirement for protecting operations from unauthorized or accidental access, but remote access solutions must also provide more granular control over the capabilities given to remote service providers. ("DEFINING STRATEGIES," 2007)

The best remote solutions provide a combination of safeguards, including multi-factor authentication, customizable logins and flexible authorization roles, which may be assigned to many individuals from a central console, ideally. Of course, an operator should be able to manage access settings on the machines themselves, as well.

With these tools, plant operators can protect their equipment, bar unauthorized technicians (whether in-house or external) from being able to access off-limit systems, while hand-picking the privileges each individual (or group) may exercise.

DOCUMENTATION – What Went Wrong and Who's Responsible?

In addition to authorization features, the best remote access solutions provide extensive documentation tools, with which users can trace what happened, when, where and by whom. If something goes wrong, an operator should be able to find out exactly where the problem originated, then track down which service measures have been affected.

Thinking Beyond Authorization

Bear in mind that the functionality of remote authorization represents only one level in what should become a comprehensive, multi-tiered security strategy. This strategy should include three categories: administrative, technical and physical, forming "a strong deterrent to most known types of threats and security breaches, while limiting the impact of any compromise" (Rockwell, 2012). When evaluating your remote software options, consider the big picture. Select a solution that supports the security policies you wish to implement as comprehensively as possible.

Even when all is well, a company must be able to satisfy its reporting requirements ("Defining Strategies," 2007). To that end, the solution should allow administrators to log each remote control session and create precise, comprehensive records, ideally stored at a central location. If needed, these records should be able to track remote activity, as well as on-screen events (mouse movements, for example).

The solution should also include a complex and flexible functionality supporting diagnosis, analysis and forecast. Manufacturers and their customers can use these data to determine the precise operating status of a unit and make appropriate maintenance recommendations. Some manufacturers use the documentation to make forecasts too, proactively identifying errors before they occur and thereby preventing machine downtime.

An Expanded Solution

Generally speaking, the benefits of remote access software are well received in the manufacturing industry. However, in many cases, the software is used only in production. Other areas of the company (headquarters, IT infrastructure or the customer help desk) are not always running the same remote solution that accomplishes so much on the factory floor.

However, in other enterprise environments – businesses devoted to IT or logistics, for example – it's much more common to see remote access software integrated throughout an entire company, saving hundreds of thousands of dollars by upping efficiency, eliminating travel and enhancing productivity.

In manufacturing, the potential benefits are similar, yet the opportunity to integrate remote software in other aspects often goes unnoticed. This is not for any lack of versatility on the part of the solution itself. Remote software can run on stripped-down, embedded systems (such as gas pumps or ATMS), inside handheld POS devices, on a back end server, at headquarters, in the help desk, and so on. In fact, to restrict the use of remote software to the manufacturing floor is to ignore an opportunity for greater efficiency, better profits, stronger customer service and an edge among one's competitors.

Reference List

Blanchard, Benjamin S. (1997). An enhanced approach for implementing total productive maintenance in the manufacturing environment. Journal of Quality in Maintenance Engineering, 3(2), 69-80.

Cisco Systems. (2009). White paper: Achieving secure, remote access to plant-floor applications and data.

Defining strategies for remote access to manufacturing assets (2007, January 13). AutomationWorld.com. Retrieved February 28, 2013, from http://www.automationworld.com/energy-management/defining-strategies-remote-access-manufacturing-assets.

Rockwell Automation. (2012, March). White paper: Scalable secure remote access solutions for OEMs.