

Success Story

Cyber Security SAGE Solution Delivers Secure Industrial Control System Access for a Major Alberta Oil and Gas Company



Challenge

A major Alberta oil and gas company needed to implement a secure process control environment across three separate business units at their oil sands site. Some of the requirements they needed to address in this design included:

- secure remote access for control system staff and vendors
- an audit trail for all activity executed on control systems

Solution

The oil and gas company commissioned Industrial Cyber Security to deploy its Secure Administration Gateway Environment (SAGE) at the three business units. SAGE provided secure remote access for employees and vendors off-site. The oil and gas company also made the decision to deploy SAGE as a way to access control system applications even when employees were on site, thus limiting access to these systems and monitoring activity of those using these systems.

Advantage

By choosing to deploy SAGE, the oil and gas company was able to realize benefits in a number of different areas.

- Because SAGE is built by extending almost entirely on existing Microsoft® Windows® security features, both the cost of the solution and the effort to deploy it were minimized.
- SAGE's activity monitoring capabilities, together with unique user-based credentials, allowed for the creation of an audit trail of all activity on the control systems.
- Secure remote access contributed to improved efficiency and productivity for control room staff and significant savings in vendor travel costs for the company.

Industrial Cyber Security is Powered by Matrikon, which represents vendor neutrality. This product works with third-party control systems and applications.

The Need for Secure Access

Industrial Cyber Security was contracted by a major Alberta oil and gas company in the summer of 2007 to assist in the design

and commissioning of a secure process control environment across three separate business units at their oil sands site. The many requirements addressed in this design included:

- secure remote access
- controlled local access
- monitoring of all user activity

The provision of secure remote access would allow control system staff to access specific systems from off-site (at home or on the road) should they need to respond to issues or problems quickly. Remote access would also allow vendors to troubleshoot control system issues without the time and expense of traveling to the site.

The company also required the ability to limit local access to the control systems. At that time, employees shared a single user account that granted administrator access to all critical process control systems. The shortcomings of this practice in terms of secure access also raised another issue: with a shared user account, there was no audit trail for activity on the control systems.

The SAGE Solution

Honeywell was able to satisfy the oil and gas company's range of access requirements by deploying its Secure Administration Gateway Environment (SAGE) at each of the three business units at the customer's site. Because SAGE was built upon existing Microsoft Windows security controls and applications, the effort and cost of deploying the solution was minimized.

SAGE utilized a number of security features to ensure secure access, including:

- two-factor authentication
- separate user credentials for all users—both local and remote—to access the system

Each deployment of SAGE was customized by installing the process control-specific applications that were used in each business unit on their respective SAGE system and limiting access to employees who were members of a specific application group.

It was more than just the security technologies in use, however, that helped the oil and gas company to satisfy their secure access requirements. The company made the decision to establish a new corporate policy that required all of its employees to access control systems only through SAGE, regardless of whether employees were on- or off-site. As a result, SAGE became the portal for all access, not just remote access. Because Honeywell had provided activity monitoring software as part of the SAGE solution, an audit trail could be maintained for all activity executed on the systems.

Robust Solution

The SAGE solution has been in place at the oil and gas company's sites since its commissioning and has been adopted as the main remote access portal into the control system for all external users, including vendors. The SAGE solution has saved the customer significant vendor travel costs, as vendors now have the ability to remotely access their specific equipment directly from the offices, without the need to travel on-site.

The company has also been successful in its efforts to use SAGE as the main interface to each business unit's industrial control systems. This new policy has successfully limited local access to these systems and required all employees to use the monitored method of access. As a result, all user activity is logged for auditing purposes.

Microsoft and Windows are registered trademarks of the Microsoft Corporation in the United States and other countries.



'Powered by Matrikon' symbolizes that this product/solution is system and application independent.

For more information:

For more information about Industrial Cyber Security, visit our website www.honeywell.com/ps or contact your Honeywell account manager.
www.matrikon.com
security@matrikon.com

Honeywell Process Solutions

2500 W. Union Hills Dr.
Phoenix, AZ 85027
Tel: 877.466.3993 or 602.313.6665
www.honeywell.com/ps

