Success Story

Industrial Cyber Security Designs a Network Architecture for Noranda Income Fund

Challenge

Noranda Income Fund (NIF), a privately held zinc refinery, needed to replace their aging IT networking infrastructure at their CEZinc processing plant at the same time as they recognized the need to secure their industrial control systems from the Business LAN. NIF wanted advice about how to achieve a secure process network as well as the equipment that would be required to build this new network.

Solution

NIF engaged Industrial Cyber Security to perform a security assessment and, based on its results, design a network architecture. The design incorporated network security best practices for an industrial control systems environment and provided guidelines to assist the facility with purchasing new IT equipment.

Advantage

- Industrial Cyber Security expertise in cyber security concepts and practices
- Industrial Cyber Security expertise in network security best practices in an industrial control systems environment
- Flexibility of the Industrial Cyber Security team to create a custom solution for their customers

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

Securing Control Systems

In 2001, Noranda Income Fund (NIF) faced two challenges:

- securing their industrial control systems from the Business LAN
- replacing their aging IT network infrastructure

Although NIF was familiar with network security in general, they did not have expertise in network security best practices for an industrial control systems environment.

NIF engaged Industrial Cyber Security to perform a security assessment and then design a network architecture based on the results of the security assessment. The architecture designed for NIF used a multi-layered defense-in-depth network approach.

The principle behind this approach is the segregation of all process equipment from the Business LAN, creating a network that is dedicated to process equipment, while allowing the movement of data that is necessary for business decision-making. A security controlled network layer, the Process DMZ LAN, is constructed between the Business LAN and the new Process LAN. Both the Business LAN and the Process LAN are able to communicate with systems on the Process DMZ LAN.

This design focuses security on a small and limited area of the network, reducing administration costs. All security programming on the firewall and the Process LAN router is now focused only on rejecting or authorizing communications to the Process DMZ LAN and not to process equipment. With a strong security perimeter in place, security risks to control systems are significantly reduced, allowing more time to deploy antivirus software and the latest security patches and service packs.

NIF implemented this architecture and it is still in place six years later. NIF found two advantages with Industrial Cyber Security. The first was Industrial Cyber Security's understanding of industrial control systems.

CIP compliance and, later, determining the cyber security features to be implemented. When the power company needed help implementing specific cyber security features and performing compliance-related tasks at each plant, Industrial Cyber Security mobilized over 20 staff from several of the North American offices.

"If you hire a typical networking company, they're usually IT guys who know very little about control systems," explains Martin Grenier, Superintendent of Information Services. "They don't understand that these things are controlling three-quarters of the plant and are worth millions and millions of dollars. Industrial Cyber Security brings that aspect to the table. They know what control systems are so they can understand the link between business systems and control systems."

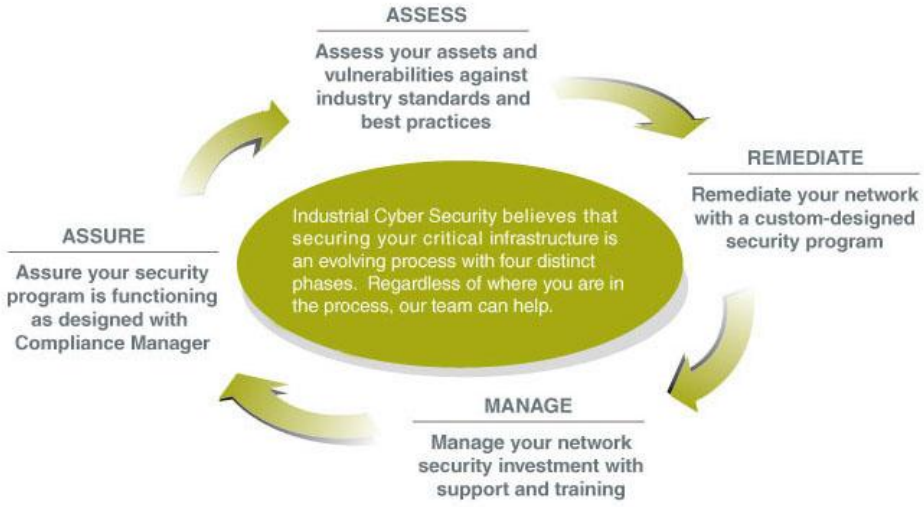
The second advantage was Industrial Cyber Security's expertise in network security best practices in an industrial control systems environment. "We'd have had to do a lot of research before we'd have come up with an architecture like Industrial Cyber Security was able to bring to the table because they had the experience already and had already done this," Grenier explains. "It saved us a lot of time from a learning curve perspective. We just needed to know what the best practices were from a networking point of view in the manufacturing environment."

About Noranda Income Fund

The Noranda Income Fund is an income trust whose units trade on the TSX under the symbol NIF.UN. The Fund owns the CEZinc processing facility located in Salaberry-de-Valleyfield, Québec. CEZinc is the second-largest zinc processing facility in North America and the largest zinc processing facility on the Eastern Seaboard, where the majority of its customers are located. Zinc concentrate is supplied to the processing facility by Xstrata Canada Corporation under an agreement that will last until 2017. The Fund is paid a processing fee for refining the zinc, and it earns additional revenue through zinc metal premiums, byproduct credits and metal recovery gains. The Fund's primary objective is to provide stable, monthly distributions.

The Security Solution

noranda Income Fund



POWERED BY MATRIKON

'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

Honeywell

SS 904
June 2011