Best Practices for Critical Infrastructure Protection (CIP) in Process Industries

How NERC CIP regulations show the way for predictive-diagnostic solutions in power generation, oil & gas, and other process industries
Best Practices for Critical Infrastructure Protection (CIP) in Process Industries

Introduction

Energy and process industries must continue to operate profitably while confronted with increasingly stringent physical and cyber security needs. This paper focuses on the best practices embodied in NERC cyber security regulations with respect to the implementation of Proficy SmartSignal predictive-analytic and predictive-diagnostic applications. While compliance is not required outside power generation, all industries can benefit from the lessons learned.

Background

The electric utility industry faces significant changes in both the physical and cyber security requirements governing its generating facilities. Specifically, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIP-002 through CIP-009) provide a cyber security framework for identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. To protect these assets from cyber attacks, the regulations require utilities to implement a risk-management strategy that first defines the Critical Cyber Assets and then isolates and protects them via a minimum set of security management controls.

NERC Critical Cyber Assets generally are those cyber assets and associated systems which, if rendered unavailable, degraded, or compromised, have the potential to adversely impact the reliable operation of the Bulk Electric System (i.e., adversely impact the continuity of power and transmission grid stability). These approaches are now being adopted well beyond Power Generation.

Industry Approaches

In addition to establishing a physical security boundary, key to the protection of Critical Cyber Assets is the creation of an Electronic Security Perimeter (ESP). The purpose of the ESP is to contain the Critical Cyber Assets and control and protect all access points to those assets. As a result, general users and non-critical business applications may no longer have access to important data from the critical assets for business, evaluation, and decision-making purposes. This is due to security restrictions on two-way communications across the ESP boundary. As a result, important data must be moved from inside the ESP to outside the ESP to facilitate access to the data.

This includes moving plant-condition data (e.g., flow, pressure, temperature, and vibration data obtained from digital control systems, the plant process computer, and/or the plant historian) through the ESP to software applications used by companies and their suppliers for performance-monitoring, predictive-diagnostic, equipment-reliability, and preventive-maintenance programs.

To date, the process-industry approach to creating an ESP is to place Critical Cyber Assets and their supporting systems inside a single or multi-tiered defensive security perimeter with the intent of isolating the process network (e.g., the process-control systems, their associated information systems, and the network they use for communications) from the general business and corporate networks.

This isolation generally is being accomplished through 1) the use of firewalls, intrusion detection/prevention systems, white listing, etc.; 2) the installation of unidirectional hardware, such as data diodes; or 3) limitation and control of physical access. The intent of these approaches is to allow outbound communications (“data push”) from the process network to the business and corporate networks, while eliminating any inbound communications traffic into the process network.

Data Access Outside the ESP

A common approach to providing access to plant-condition data is to set up a “mirrored” data historian outside of the ESP, which receives data “pushed” from the historian within the ESP that is directly located on the process network. Another approach is to place the data historian outside the ESP and to have the data “pushed” directly from the DCS or other source. Once a plant owner makes data available outside of the ESP in the replicated system, plant personnel, remote-service providers, and software applications can access the data required to perform monitoring and evaluation activities.

Recommendation

While every customer’s situation is different, and no one solution will be best for everyone, it appears that industry is settling on a best practice of setting up a “mirrored” data historian outside the ESP. Data to this historian can be “pushed” through a hardware-based data diode or through software-based security but, either way, the goal is to provide access to process and operating data on the general business or corporate network.

With data being provided by this mirrored historian, the SmartSignal predictive-analytic and predictive-diagnostic solutions can be run on the general business or corporate network under standard corporate IT security policies. The same holds true for GE Intelligent Platforms-hosted situations, except that a VPN tunnel must be established to the mirrored historian server.
The included figures show recommended NERC-CIP-compliant network configurations for both a premise-based environment and a hosted environment.

The premise-based figure (Figure 1) assumes that a historian exists inside the ESP and that a “mirrored” historian receives data that is pushed from within the ESP. However, the data historian within the ESP is optional, since the “mirrored” historian can be configured to receive data directly from the plant DCS without using a second historian.

Similarly, the host-based figure (Figure 2) assumes that an optional historian within the ESP exists. Additionally, Figure 2 assumes that the customer has added an optional DMZ to further limit access to the customer’s facility.

The actual configuration that a customer chooses will be determined by the customer to meet its specific security, technical, and business needs.

Figure 1: Premise-Based Solution
For on-premise implementations, the customer’s servers host the Proficy SmartSignal predictive-diagnostic solution. In most cases, the “mirrored” historian and servers hosting the SmartSignal applications are located within the same business or corporate network, making access easier for the SmartSignal solution to pull data. If data is available from multiple sources, separate asset models will be created to avoid time-series conflicts. A customer also accesses the processed data via the business or corporate network. GE Intelligent Platforms can access the solution by a customer-provided remote access. The remote access is, typically, a software VPN solution, IPSec, or CITRIX.

Figure 2: Hosted Subscription (with optional DMZ)
For hosting solutions at GE Intelligent Platforms, a secure IPSec tunnel is established between the customer network and the GE Intelligent Platforms facility. The Proficy SmartSignal predictive-diagnostic solution pulls data from the “mirrored” or “limited mirrored” historian outside the customer’s Electronic Security Perimeter (ESP). The data is processed and stored at a GE Intelligent Platforms hosting facility. A customer accesses the processed data via a secure public internet address.
Future Trends
As a new regulation, NERC CIP guidelines for power generation will evolve and probably become more stringent over time. Oil, gas, and other industries will continue to mature in their approaches, as well. GE Intelligent Platforms will continue to monitor the development of regulations and trends, making recommendations as needs change. As access to plant data is business-critical for many reasons, we fully expect industry will continue to develop solutions that facilitate access to data for decision making while still protecting key process-control systems.

References
CIP Standards
NRC 10CFR73.54