WHITE PAPER

Connectivity in a Critical Infrastructure Protection (CIP) World

Cleo™

Move View Act®

Table of Contents

Introduction and Background

Energy and process industries must continue to operate profitably while meeting the challenges of ever-increasing physical and cyber security needs.

This paper focuses on the best practices embodied in NERC cyber security regulations with respect to the implementation of data connectivity between remote industrial and generating assets, SCADA, ERP, data historians, EMS, work order systems, predictive diagnostic systems, Computerized Maintenance Management Systems (CMMS), asset monitoring centers, and other applications.

Although compliance with NERC may not be required outside of the electric power industry in North America, the power industry in other geographic regions as well as other asset and process-intensive industries everywhere can benefit from the best practices discussed in this paper.

Background

The electric power generation industry faces significant changes in both physical and cyber security requirements governing generating plants, centralized monitoring, and other sites including outsourced data processing.

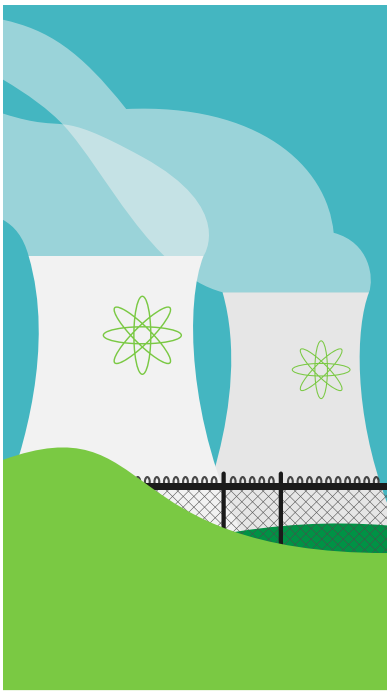
An example of such governing requirements includes The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIP-001 through CIP-011) which provide a cybersecurity framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

To protect generating assets and infrastructure from cyber-attacks, the regulations stipulate that generating asset owners and operators implement a risk-management strategy that defines Critical Cyber Assets, isolates such assets, and protects them with a minimum set of security management controls.

NERC Critical Cyber Assets are those assets and related systems which, if rendered unavailable, degraded, or compromised, have the potential to adversely impact the reliable operation of the Bulk Electric System. That is, if individual hackers, or worse an organized cyber-attack penetrated the system, the continuity of power generation, transmission, distribution, and/or the stability of the transmission grid could be put at risk. The framework prescribed by NERC is now being adopted in other energy and infrastructure industries beyond Power Generation.

About This Paper

Increasingly, such monitoring and decisions are made thousands of miles away in remote or centralized monitoring centers. How do you securely connect all of these end-points?



In industries where remote assets are operating in mining, oil & gas production, power generation, manufacturing, and elsewhere, large industrial equipment is instrumented with sensors and other operating controls which are, in turn, connected to SCADA systems, control rooms, data historians, monitoring centers, and much more.

In an effort to monitor, maintain, predict, optimize, and operate these industrial assets which include mobile, rotating, and non-rotating assets, an ever-increasing flow of data is concurrently piped to places where decisions are made. Sometimes those decisions are made within the same plant or site where the assets are operating. Increasingly, such monitoring and decisions are made thousands of miles away in remote or centralized monitoring centers. How do you securely connect all of these end-points?

This paper analyzes several typical approaches, evaluates the benefits and risks of varied solutions, and recommends an approach where cyber-attack risk pertaining to the connectivity of endpoints is better mitigated.

Typical Use Case

Essential in protection of Critical Cyber Assets is the creation of an Electronic Security Perimeter (ESP) as prescribed by CIP Cyber Security Standard CIP-005.

The purpose of the ESP is to contain Critical Cyber Assets and control and protect all access points to those assets. General users and noncritical business applications may no longer have direct access to important data from the critical assets for business, evaluation, and analytic evaluation and other decision-making purposes. This is due to security restrictions on two-way communications across ESP boundaries. As a result, important data must be moved from inside the ESP to outside the ESP to facilitatebroad er access to the data.

A number of communication connectivity cases are to be considered:

1. Communication between separate sites and centers within the ESP.

2. Communications between end-points within the ESP and outside the ESP.

3. Subsequent communication of secure data from within the enterprise, but outside the ESP to an outside service provider.

What is eeded to support these:

In each of these communication connectivity cases, it is important to establish secure communication channels that involve both independent and integrated measures, providing security at multiple layers. In order to assure reliable delivery of information, it is important that information be tracked as to the source, recipient, and other key meta-data about the transmission. This enables IT governance, and from a direct operational benefit, provides a direct means of monitoring, diagnosing, and remedying communication errors.

For important scheduled transfers of information, monitoring that can detect the absence of an expected data transfer within specified time parameters is helpful. Digging deeper into the typical transfers of information and the activities that support them, it is helpful to automate the means by which data security certificates are exchanged and implemented.

In some cases, the automated tracking of acknowledgment receipts is important. It should be noted that in case No. 2, where the source is within the ESP and destination is outside the ESP, reconciliation must occur outside the ESP. Since information can only flow from within the ESP outward, and not from outside the ESP inward, the transmission log itself must be transmitted to an enterprise application outside the ESP where receipt acknowledgments are also sent, since they cannot be sent back into the ESP. Reconciliation between acknowledgments and the transmission log may now occur.

Finally, in a growing number of cases, large amounts of data are being transmitted. It is increasingly important in those cases that checkpoint and restart facilities within the transmission component are available to ensure efficient transfer of data in cases where communication hiccups occur. Rather than restarting at the beginning of massively large files, picking back up from where you last successfully left off substantially improves the speed of transmission. In typical implementations within the Power Generation industry today, not all of these features are present.

Typical Access Outside the ESP

A common approach for providing access to plant, equipment, and asset condition data is to set up a "mirrored" data historian outside the ESP.

This data historian receives data that is transmitted from the data historian within the ESP located on the process network. Another approach is to place a data historian outside the ESP, yet within the enterprise, and to have the data transmitted directly from instances of DCS within the ESP. Once asset operators make data available outside of the ESP in this replicated system, plant personnel, remote-service providers, and software applications can access the data required to perform condition monitoring and evaluation activities.

Typically, the connectivity of transmission used here includes any of a short list of security measures used to protect a File Transfer Protocol (FTP) session:

- VPN tunnels – not good enough
- IPSec VPN
- SSL VPN

Problems and risks with typical approaches:
Some of the problems and risks associated with these approaches are listed here. Some of these problems are related to security. Others are related to the level of assurance of delivery offered by the approach, as well as the efficient use of resources to perform data transmission to intended recipients.

FTP: One of the problems here lies within FTP itself. FTP is generally weak in terms of the security inherent within the protocol. FTP was invented in 1971, long before the bulk of present day cyber-threats. FTP is "dumb" in the sense that if wrapping layers of security fail or are inadvertently turned off, FTP will still function. That is, the level of security that is integrated within FTP is weak and FTP is unaware whether or not other layers of security are functioning as required.

VPN: The VPN layer is simply an encryption approach for the session. Yet, encryption is just a small piece of the puzzle. It's a good additional measure if the underlying connection already has strong integrated and intrinsic security and provides a high level of delivery assurance.

There are a number of important considerations to include when selecting a more robust solution for secure and reliable remote connectivity:

1. **Tracking and governance:** There is no good way, without a phone call, to validate that the payload actually got to the intended recipient. This validation is needed for good IT governance and operational execution of effective data connectivity. You need the ability to easily diagnose and troubleshoot connectivity issues especially when the other connection point is outside of your business or in a hard to reach place. You need the ability to audit connectivity and know when expected content does or does not arrive.

2. **Big data:** As file sizes continue to grow and uses cases involving a growing number of smaller files arise, it may become advantageous to aggregate and algorithmically compress payloads for efficient and speedy transfers. Additionally, checkpoint and automated restart capabilities are increasingly a necessity in order to effectively transmit larger payloads of data.

3. **Consolidation:** As the number of connections grows, the proliferation, management, version control, and other aspects of connectivity, connection scripts, multiple FTP servers, end-points, security certificates, and other enabling artifacts becomes encumbering. Seek a solution that enables consolidation of all of these varied connectivity means without all of the scripts. The solution should automate security certificate management, enable ease of setting up and modifying connection points, and provide full security and auditability.

Other Alternatives

As an alternative to various forms of VPN, sometimes other methods such as SSL (Secure Socket Layer), TLS (Transport Layer Security), PGP (Pretty Good Privacy), or SSH (Secure Shell) are used.

One must consider that these protocols attempt to provide a secure pathway, but do not actually move data. So they are typically used in concert with FTP. Consequently, they leave the security-related and functional deficits previously noted regarding FTP fully intact, while adding a layer of protection that often is manifest with its own problems.

These alternatives are partial measures to further curtail risks, but still leave open significant and known avenues of attack. These measures do not always provide or enforce strong authentication of connections and do not protect communications between clients and the IPsec gateway in some network architectures. They have other known security weaknesses including cases where communication between the proxy server and application servers are unprotected as well as deficient authentication and encryption mechanisms.

Frequently when companies inventory their use of these varied protocols, they find a wide variety of relatively undocumented connection streams built using a diverse set of software and scripting languages. The portfolio of technologies and scripts supporting assorted connection points is expensive to maintain, impossible or at least very difficult to monitor and govern, and adversely subject to both quality and security risks.

Six Key Recommendations

1. **Map it out:** If you map out the various connection points between applications inside the ESP, within the enterprise but outside the ESP, and across company boundaries between the enterprise, vendors, customers, regulators, and partners, a diagram much resembling spaghetti begins to emerge. To gain greater insight into a better solution, add up all of the hidden costs of supporting this wide array of connectivity and explore the number of issues that cite connectivity as a contributing underlying root cause.

2. **Consolidate and centralize:** If you were able to consolidate a significant subset of the entangling connectivity within a centralized technology that also manages the security certificates, tracks and logs data transmissions, encrypts data both in motion and at rest, and obviates the need for firewall configuration changes in support of adding, deleting, or changing connectivity end-points, you would arrive at an easier solution that offers greater governance, reliability, and security.

3. **Beware of the inside job:** Beware the tendency to overly fixate on cyber-attacks originating from outside the enterprise. There is significant evidence that attacks and cyber crimes can more frequently originate from inside the enterprise. Protection of data while in motion and at rest within the enterprise, and between applications both inside and outside the ESP and enterprise as a whole, is practical to achieve with a centralized MFT solution.

4. **Avoid scripting languages:** Select a solution that enables easy configuration and implementation of additional connectivity end-points without involving scripting languages.

5. **Avoid firewall changes:** As additional end-points are added, it should not be necessary to make firewall configuration changes. Such changes often require specialized work of scarce resources that can add undue length to project timelines. Even worse, erroneous firewall configuration changes can lead to security breaches or unwitting blockage of intended connections.

6. **Research MFT capabilities:** Research the capabilities offered by a Managed File Transfer (MFT) solution. Not all such solutions are created equal, so be sure to consider the detailed capabilities of feature sets that support the requirements outlined in this paper in order to best achieve a secure, reliable, and efficient capacity to move information from point to point within your ESP, enterprise, and larger business data eco-system.

Future Trends

As a relatively new body of regulation, the NERC CIP guidelines for power generation will expand and address the continuing evolution of sophisticated cyber security. Other energy and asset-intensive industries will need to continue to anticipate and protect themselves from the continuing advances of cyber-attacks. Additional trends in the energy and power generation industries will challenge IT departments and change the way information is harnessed to further integrate and optimize the industry.

Big data: On the generating side of the industry, in a post-industry consolidation landscape, generators have larger and more diverse generating fleets spanning wind, nuclear, hydro, fossil, and beyond. With constant recalibration of fuel sources to balance efficiencies of renewables, coal, regulation, and aging assets, more equipment instrumentation can generate terabytes of sensor data into historians where, mixed with baseline performance data over the past year, performance and output can be optimized. Data from all over the fleet are combined to form big data which needs to be securely moved, viewed, and acted upon. On the distribution side, the advent of smart meters and more complex pricing and billing systems, combined with a continuing stream of regulation, translate into big data becoming bigger and power companies needing more robust means to handle it all.

Peer to peer: With the growing proliferation of boundary-cutting peer-to-peer data sharing technologies, companies need to promulgate clear policies that enable the protection of information in ways that promote the advantages of remote decision making while still protecting sensitive data, physical assets, and key process-control systems.

Data analytics and insights: Generators continue to need to better predict generating capacity in order to better meet demands, market and sell production, protect margins, and maintain price. To better predict capacity, one must understand the many trends in predictive parameters including the weather, usage patterns, and condition monitoring. Centralizing of condition monitoring and predictive analysis functions that rely on more frequent and diverse sensor data – and storing a year of that reference data – will provide better prediction of impending equipment issues and enable operators to pinpoint and schedule corrective measures.

Collaboration: As the boundaries of information sharing continue to blur between owners, operators, power consortiums, distributors, energy marketers, equipment manufacturers, service providers, control centers, and other parties, the control and governance of information will need to align with advances in information technology. This will facilitate the rapid flow of large amounts of critical data to decision centers that enable equipment operating analytics, predictive and diagnostic decisions, energy production data, and collaborative and balanced energy production among fossil and renewable sources.

About the Author

Joe Dupree

Vice President, Marketing

Joe Dupree leads marketing at Cleo. His role includes leadership of product strategy, competitive analysis, demand generation, brand management, communications, and public relations. With more than 20 years of software industry experience in roles that span technology product marketing, product management, and software engineering, Joe has helped global enterprises implement cost effective, secure, and governable information management and integration solutions. Joe has an MBA from the University of Maryland as well as a bachelor's degree in Computer Science from Siena College in Loudonville, New York.

Cleo™

Move View Act®