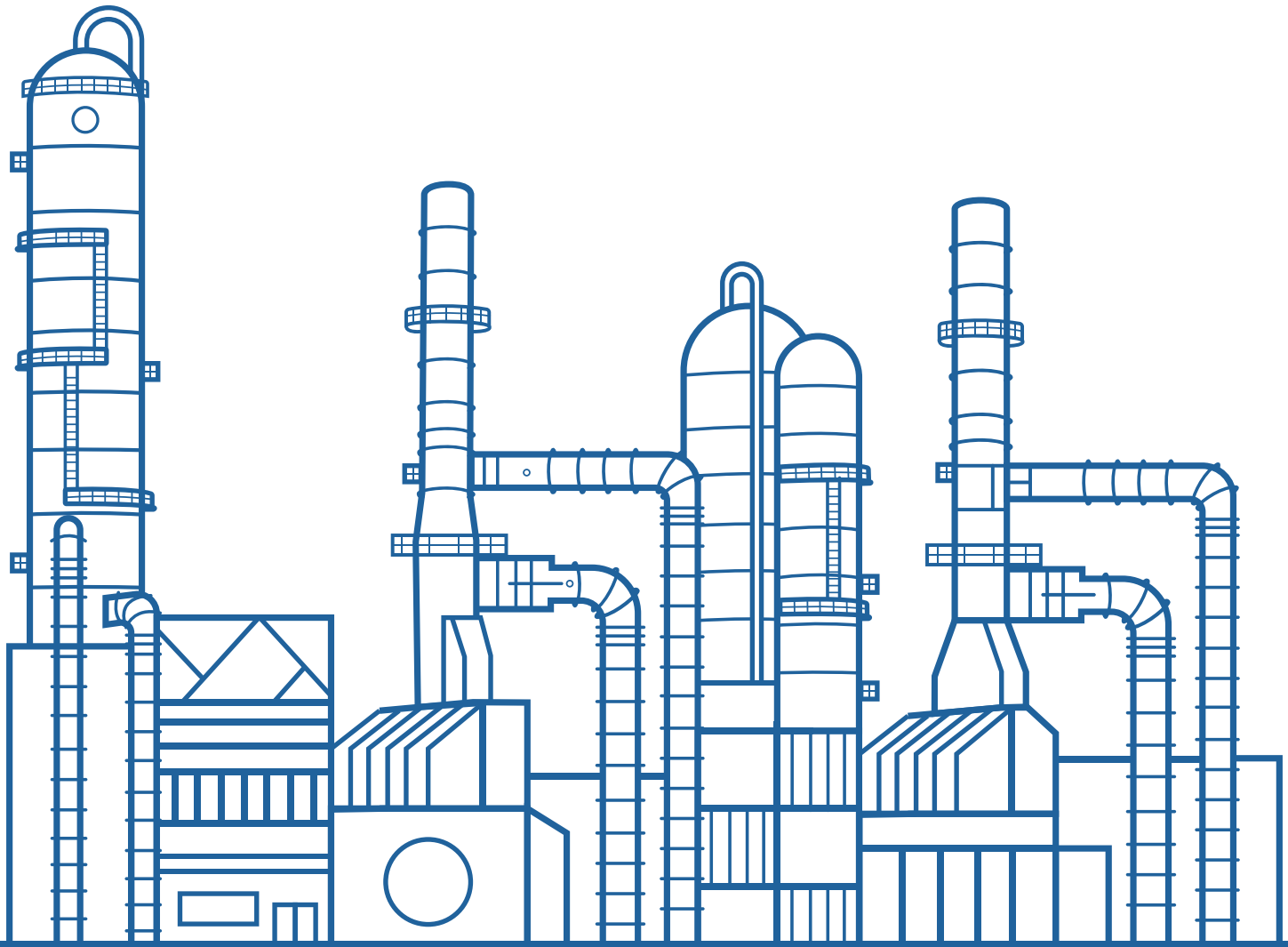
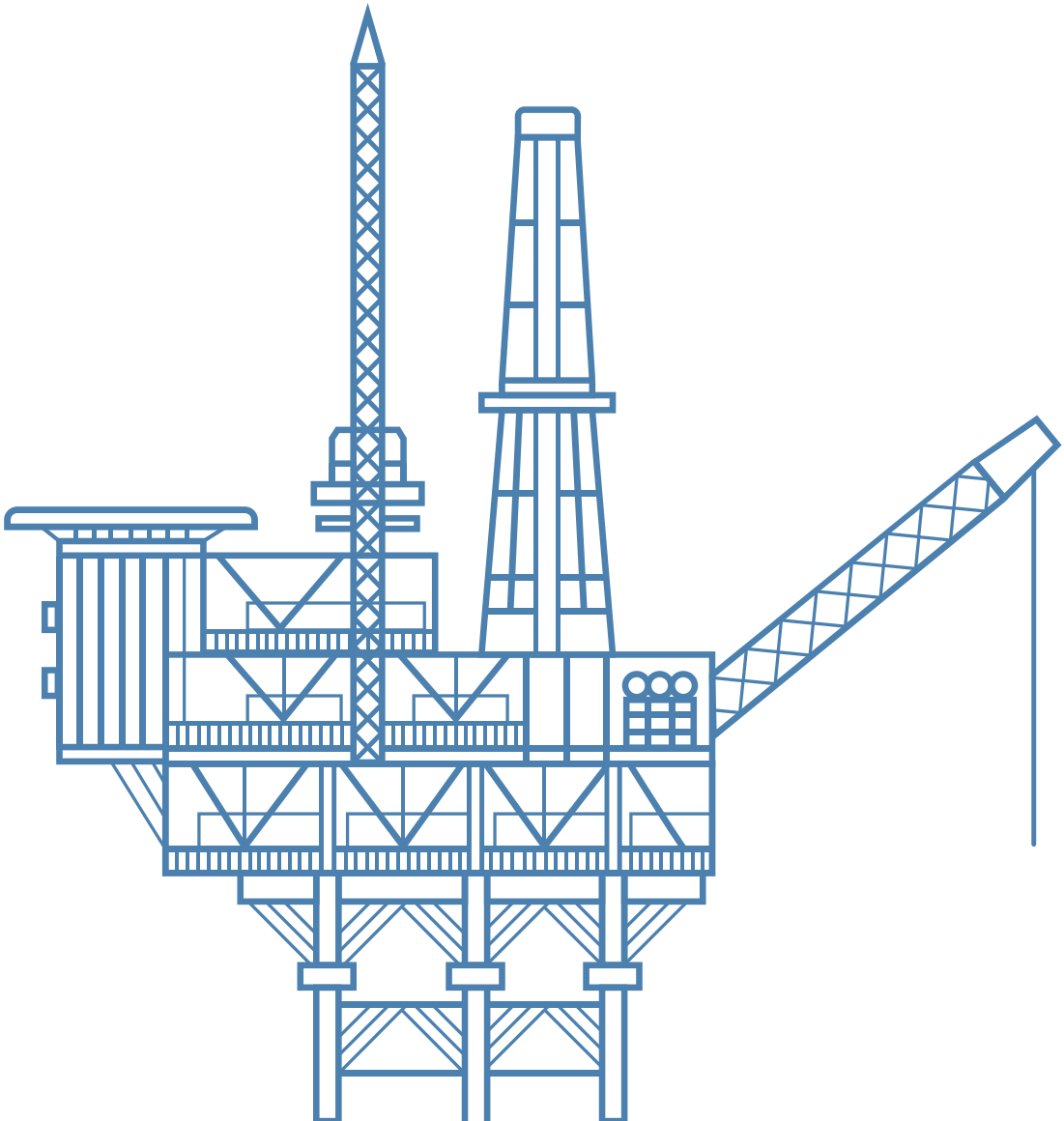
VERACITY
INDUSTRIAL NETWORKS™

Overcoming Cybersecurity Challenges in Industrial Control Systems



White Paper by Earl Shockley

TABLE OF CONTENTS



BACKGROUND

The risk of a catastrophic coordinated cyberattack on U.S. energy delivery systems (collectively known as "the power grid") that is delivered via vulnerable Industrial Control Systems (ICSs) and results in prolonged and widespread power outages is not a new concern of energy industry executives or government policymakers. Owners and operators of energy sector assets understand the potential impact of coordinated physical attacks and cyberattacks, which threaten the reliability and resilience of U.S. energy delivery systems. They have lived through the havoc and disruptive economic and social effects of the prolonged and widespread power outages caused by the 2003 North East Blackout and the 2011 Southwest Blackout.

However, given the industry-standing focus on grid reliability, an overall lack of qualified cybersecurity experts, and a general reliance on the fact that a cyberattack on the U.S. power grid resulting in widespread outages has not yet occurred, energy sector utilities have fallen behind in their cyber protection strategies. A continual reliance on legacy systems and protocols designed decades ago, coupled with the growth of networks and communication protocols, has left the energy sector vulnerable and behind the eight ball. The increase in sophisticated cyberattacks and the use of "bolt-on" in-line security devices as protection contribute to the loss of necessary awareness and cyber risk management intelligence that can proactively address vulnerabilities and threats facing ICS platforms and networks that serve our most critical infrastructure. The energy industry has lost the ability to respond resiliently to sophisticated intrusions because it lacks a flexible and proactive approach to cybersecurity.

On December 23, 2016, this risk went from a hypothetical to reality when a regional electricity distribution company in the Ukraine experienced a coordinated cyberattack and illegal breach of an ICS that controlled more than 30 substations (110–23 KV). The attack affected 225,000 customers in three different distribution service territories for several hours. This attack highlighted real-time vulnerabilities for the aging legacy ICSs that control U.S. energy delivery systems. As the complexity of the power grid evolves, the consequences of cybersecurity risks that have escaped the focus of the electric industry could become catastrophic. Though attacks on power grids in the United States and other developed countries are imminent, intrusion is not. Facilities should take solid steps to ward off what nation-states and criminal organizations may consider the ultimate prize: crippling a country's power arteries.

EXECUTIVE SUMMARY

Traditional industrial networking technologies are not designed to protect critical infrastructure; they are designed for corporate business operations. Typical Ethernet technologies within the electric industry consist of legacy systems that include a mixture of equipment, technologies, protocols, and functionality. Many of these systems are complicated and not designed to communicate effectively, and situational awareness and detection of the critical assets within the topology are often lacking. The risk of third-party intruders accessing key energy sector ICS networks increases as the means to mitigate these intrusions falls behind the intruders' evolving cybertechnology. This technology includes Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Intelligent Electronic Devices (IEDs). Some legacy ICSs can be exploited by untalented hackers, whose intrusions cannot be addressed by legacy system engineers. Perimeter (North-South) security tools that have been "bolted-on" to these ICSs networks provide limited protection against intrusion. Integrated (East-West) security is necessary to prevent or mitigate breaches before they result in catastrophic failures, but given current technology this protection would require the replacement of large portions of an ICS.

This system-wide vulnerability is exacerbated by industrial adoption of IP-based communications and microprocessor installation in industrial equipment. As the technical complexity of these systems evolves, the need for secure and resilient critical technological upgrades will become key to business operations.

CHALLENGE | PROBLEM STATEMENT

It is reasonable to address larger, more comprehensive problems with a segmented approach. Holistic challenges such as ICS cybersecurity can be overwhelming and complicated. Security solutions often create more challenging system-wide issues. Attacking comprehensive problems with individual statements helps us to focus on solving analysis and planning issues step by step. This paper identifies two individual problem statements that address the comprehensive issue of ICS security.

Individual Problem Statement #1

Lack of ICS Network Visibility and Control

Devices installed on ICS networks and the communication between them are not clearly discernible. An independent "line of sight" into ICS topology activity is essential—you cannot secure what you cannot see, and you cannot avoid or respond to threats that you cannot identify.

Individual Problem Statement #2

Legacy Infrastructure Issues

Legacy ICS infrastructure lacks engineered communication. Most ICS infrastructures are a mixture of hardware, software, OEM vendors, and integrators. Most are built with Capital Expenditure Projects (CAPEX) executed in phases over extended periods of time. Rarely does the extended project include a phase for communications re-engineering after all systems have been migrated. The infrastructure must continue to communicate and share process data because all assets are responsible for running the same physical process.

PROBLEM IMPACT | ENERGY IMPACT

These individual problem statements represent significant energy sector vulnerabilities. The growth of Distributed Energy Resources (DER) such as renewable energy facilities, demand response, smart grid, and energy storage facilities increases the complexity of the attack surface and require more comprehensive security measures.

The evolving impact of a catastrophic coordinated cyberattack on U.S. energy delivery systems that is delivered via vulnerable ICSs and results in prolonged widespread power outages is not a new concern for energy industry executives. Owners and operators of energy sector assets understand the potential impact of coordinated physical attacks and cyberattacks, which threaten the reliability and resiliency of U.S. energy delivery systems. This impact has been summarized in risk assessments conducted by governments and corporations, and it is managed through corporate Enterprise Risk Management programs. Energy industry executives typically outline budgetary requirements based on organizational risk portfolios. High-risk items

are usually addressed with appropriate budgets. Cybersecurity and the resilience of critical network systems have been identified as chief concerns for the energy industry [1]. Key security breaches are considered probable and "most information security professionals believe that the US' critical infrastructure will be breached by a cyberattack within the next two years [2]." Such a breach would affect all aspects of the organizational risk portfolio, including

- **Operational impact**
  Systems go down and are not resilient enough for quick recovery
- **Organizational brand impact**
  The organization's reputation is tarnished.
- **Financial Impact**
  Cost of remediation is more than $1.2 Trillion per year.[3]
- **Regulatory Impact**
  Fines and sanctions can cost up to 1 million dollars per day.

The risk of a critical breach is great, and the impact is well understood. The potential damage to critical assets and infrastructure could shift our current threat-state level from "normal" to "critical" in the near future.

CURRENT STATE APPROACH TO THE DEFINED PROBLEMS

Energy Sector

Industrial organizations currently address the problem statements with outdated and vulnerable mechanisms. For example, Legacy Networks were designed for an air-gapped environment with no integrated security. Perimeter (North-South) security tools have been "bolted-on" to the limited SPAN ports of these networks, providing incomplete protection and leaving large security gaps. Integrated (East-West) systems to detect and mitigate breaches before they result in catastrophic failures are often missing. Many organizations lack a fundamental understanding of their legacy system baselines. Many firms lack the cybersecurity expertise to monitor, track, identify, and quickly mitigate intrusions and other security issues within their legacy systems. Monitoring regulatory reporting guidelines often requires implementation of updated technology and outsourcing work or hiring vendors to complete compliance tasks. These obligations can be expensive and time-consuming for responsible entities. It is difficult to stay abreast of rapidly evolving cybersecurity risks and the threats to large and complex electric delivery systems.

[1] NERC Reliability Issues Steering Committee (RISC) 2017 Reliability Risk Priorities Report
[2] Portrait of an Imminent Cyberthreat, 2017 Black Hat Attendee Survey
[3] Cyber Security in the ERA of Industrial IOT, Frost and Sullivan Report

Regulatory Sector

One way to manage this emerging issue and reduce the risk to the Bulk Electric System (BES) is to implement regulatory standards that set minimum industry guidelines for creating and implementing cybersecurity policy and practices. The North American Electric Reliability Corporation (NERC) portfolio of Reliability Standards includes a distinct set of security standards that address Critical Infrastructure Protection (CIP). These standards are designed to help identify, manage, and mitigate risks in the energy sector.

Compliance with the CIP Standards can be particularly challenging for registered entities subject to NERC regulation. The CIP Standards can be ambiguous and guidelines for their use have been controversial. This can result in differing interpretations by responsible entities and auditors. Finally, the CIP Standards have been in a state of flux for the past several years while NERC has been revising them in response to Federal Energy Regulatory Commission (FERC) regulations for cybersecurity and physical security. Many responsible entities are continually drafting and implementing new procedures to meet the new requirements. Failure to comply with the standards creates potentially costly risks for companies involved in the generation, transmission, and distribution of electricity.

The CIP Standards continue to be ranked as the regulated energy industry's most often violated NERC Standards. Confusion in the industry is illustrated by the frequency of requests for clarity and guidance on CIP issues relative to analogous requests concerning operational and planning standards.

Most Violated Standards Discovered in 2016

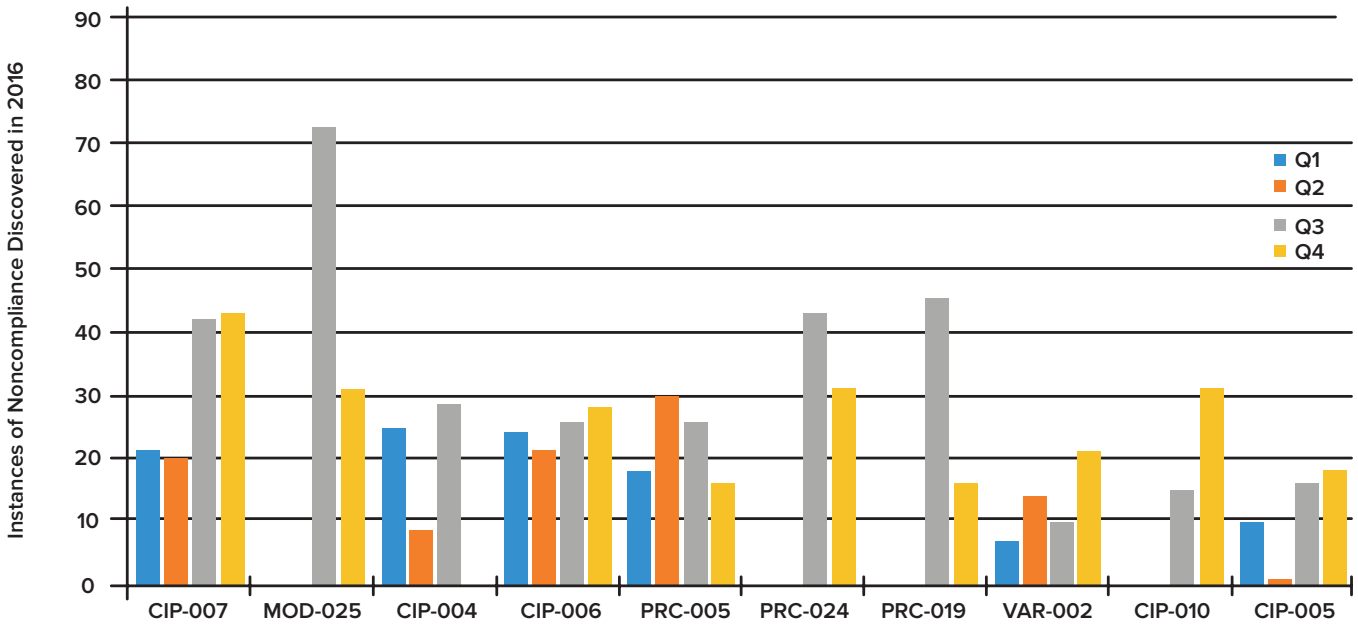


Figure A.11: Most Violated Reliability Standards Discovered in 2016 by Quarter

In addition to having the highest rate of noncompliance in 2016, CIP-004, CIP-005, CIP-006, and CIP-007 are among the most violated historically. NERC has concluded that the industry exhibits "a lack of commitment to compliance with the CIP standards [4]." This statement shows an obvious disconnect between the regulators and the energy sector they oversee. NERC is finding it increasingly difficult to maintain the desired compliance because of the complexity of the CIP standards and the regulated industry's struggle to increase the performance and visibility of legacy systems.

Another important factor is the historical trend of violations of new NERC standards—regulated entities often find it hard to keep pace with evolving standards and comply when the new standards require the implementation of new technology. The following chart reflects this continuing trend.

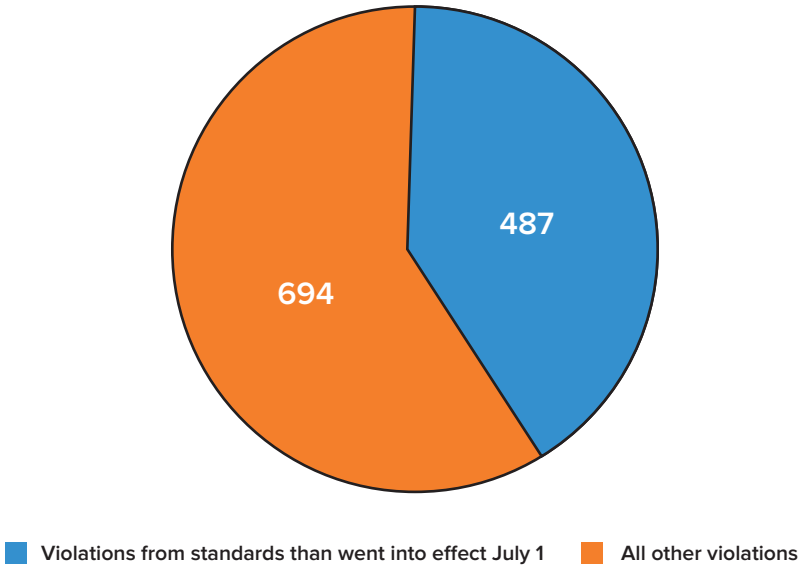


Figure A.4: Percentage of 2016 Newly Discovered Noncompliance with July 1, 2016, Enforceable Date

CIP standards are necessary; however, they only lead to minimal cyber competency—regulations will always lag evolving threats and cybercriminal technology.

LOOKING TO EMERGING TECHNOLOGY FOR SOLUTIONS

The energy sector must adapt layered cybersecurity programs based on industry standard frameworks and best practices, which should be executed by staff that understand baseline operations. The implementation of technology that can respond quickly and reliably to anomalous cyber activity must reduce any lingering "dwell time." Embracing technology that is adaptable to legacy systems (rather than "bolted-on") and provides visibility and security at the network level is essential to comprehensively addressing the defined problem statements. Technological solutions should at a minimum include

Centralized Orchestration

A software platform that allows centralized orchestration of network flows, configuration, and security with distributed execution at the network switch. The console should provide a single view of the health and status of the ICS network as well as security zones and posture. A platform that is a "deny-by-default" network that moves beyond detecting and alerting cyber events to a resilient network that reduces the attack surface by design. With this comprehensive approach, cybersecurity experts and analysts will have a centralized platform for planning and executing responses to an attack. All forensic investigation and recovery can be visualized, monitored, managed, and controlled from one place to avoid missteps and to accelerate the triage and recovery process.

[4]ERO 2016 Annual CMEP Report, Feb 2017

Situational Awareness

A platform that provides 100% visibility of connected devices, their identities, functional roles, and the communication between them. One which enables passive asset discovery and characterization with graphical networked device management. The solution must deliver a simple visual network representation with intuitive tools that identify communication trends and possible issues.

Industrial Network Resiliency

A system that utilizes a pre-defined policy for each defined threat or operational state on the basis of the control system's communication needs. When a threat or operational state changes, the pre-designated policy is executed. This policy-based approach provides comprehensive remediation.

Threat Based Security Policy

A graphical interface that includes drag-and-drop configuration that simplifies the creation and management of security zones and network segmentation. Operators can visually define security policy on the basis of predetermined threat levels, which ensure the security of ICS assets.

Cyber Defense In-Depth

An interface that includes coordinated layers of North, South, East, and West protection. This approach addresses external and internal attackers. Traditional firewalls protect systems from external intrusion; failure to recognize internal intrusions results in a single point of failure.

Automation

Software that allows an organization to address limited resources with automation, minimizing and/or eliminating many resource-intensive activities normally addressed by security personnel.

CONCLUSION

It's time for the energy industry to think differently and embrace a new security paradigm. An approach to decades-old network infrastructure that is rooted in "bolted-on" solutions has proven ineffective for minimizing threats; in fact, this approach often creates security problems. A proactive risk management approach that includes emerging technology will help the energy industry to achieve 100% visibility of critical industrial assets and secure those assets.

ABOUT EARL SHOCKLEY

Earl Shockley is the President and Founder of inPOWERd LLC and is a strategic advisor for Veracity Industrial Networks. Earl has over 40 years in the energy industry and is a former regulator and senior executive with the North American Electric Reliability Corporation (NERC). Earl was instrumental in NERC's shift from the "zero-defect" compliance and enforcement approach to one that focuses on a company's inherent risk and ability to manage reliability and security risk with associated internal risk control programs. Earl also led investigations of major system blackouts including the FERC/NERC Inquiry & Investigation of the September 8, 2011, Arizona-California Blackout, the joint FERC/NERC Compliance Investigation of the February 2008 Florida Blackout, and the FERC/NERC inquiry of the February 2011 Southwest Cold Snap event. Earl is a sought after public speaker and expert witness on complex issues involving regulatory compliance, risk management, internal risk control systems, and event causal analysis.

To learn more, please contact:
info@veracity.io | www.veracity.io

VERACITY INDUSTRIAL NETWORKS™