

Technical White Paper

# ICS CYBER SECURITY

Protecting Industrial Control Systems:  
An Integrated Approach



1010 Market Street, Suite 550  
St. Louis, MO 63101



info@rkneal.com



+1 314 754 8814

The purpose of this white paper is to present a novel cyber security framework for deploying and managing best-in-breed cyber threat management products across multiple OEM vendors.

## ABOUT RKNEAL

**Founded:**  
1994

**Ownership:**  
Privately held

**Expertise:**  
Industrial control system (ICS)  
cyber security

**Global Headquarters:**  
St. Louis, MO

## PROTECTING INDUSTRIAL CONTROL SYSTEMS: AN INTEGRATED APPROACH

Hackers have infiltrated credit card companies, retailers, health care providers and other consumer industries over the past several years. The hackers are utilizing the very technologies we all use to make life easier – Internet connectivity to bank accounts, health records, etc. – to gain access to our private information and financial accounts. As a result, innovative cyber security providers are constantly improving their defense technologies to keep up with the ever-changing threat landscape. Companies are also increasing their investments in these technologies to protect this critical information.

Recently, however, a much larger threat has emerged – one that threatens the physical assets of our critical infrastructure. This is the cyber threat to industrial control systems (ICS). These systems control our electricity, water, manufacturing plants, refineries and transportation systems. Historically, these systems have faced less of a threat simply because they were often isolated from business networks and utilized proprietary technologies. More and more, however, companies are seeking to gain the efficiency of remote access or utilize the Internet of Things (IoT) to improve performance. Furthermore, newer ICS systems are employing open standard communication protocols. As a result, these systems have become major targets for cyber attacks.

Although industry-specific regulations (e.g., NERC CIP and CFATS) have started requiring increased protection, potential defense solutions still lack many of the critical elements required for a cohesive and efficient defense mechanism. ICS OEM vendors are not experts in cyber security nor have they built their products with cyber security in mind. Each site will likely have multiple DCS, PLC and SCADA vendors present, and solutions that work in enterprise IT environments need to be tailored to the unique requirements of operation technology (OT) environments before being deployed in an around-the-clock, mission critical environment.

## INTENDED AUDIENCE

This white paper covers details specific to ICS systems and primarily focuses on the power generation industry. Readers of this document should be familiar with general ICS components and design, cyber security concepts and communication protocols. The intended audience includes: control engineers, information technology (IT) professionals who secure ICS systems and engineering and/or compliance managers.

## ICSTHREATSAREREAL:PROGRESSBREEDSRISK

Make no mistake, the cyber threat to the world's critical infrastructure is real. The ICS systems that generate, distribute and transmit our electricity, operate our water systems, refine our chemicals and control our transportation systems are under threat for several reasons.

First, the potential impact of the attack is significant and our enemies understand this. A notable disruption to our infrastructure can cause significant economic harm, but can also threaten health, safety and lives. Although the focus of public discussion has been on threats to our financial records or privacy, the potential disruption to critical infrastructure is much greater.

Second, the control systems in operation today are complex webs of old and new technology provided by a range of OEM vendors. Historically, the use of proprietary technologies and isolation protected these systems from the Internet-based attacks so prevalent in our IP-oriented communication technologies. As we look to the future, however, operators seek to leverage the efficiency provided by these new communication technologies and are connecting these older systems to new systems.

Third, we have growing evidence that hackers are in fact targeting these systems. Enterprise Strategy Group, a leading consulting firm, published results of its 2015 survey for critical infrastructure providers that showed dramatic increases in the number of attacks. Sixty-eight percent claimed that they experienced one or several cyber security incidents over the past two years; thirty-six percent said cyber security incidents led to a disruption of operations; and two-thirds of cyber security experts at critical infrastructure providers believe that the threat landscape is more dangerous today than it was two years ago.



**Critical infrastructure providers are under attack,** with 36% of firms experiencing at least one operational disruption in the past two years.



Protecting against cyber threats challenges the traditional paradigm of disconnected, siloed industrial control systems managed individually by OEM vendors.

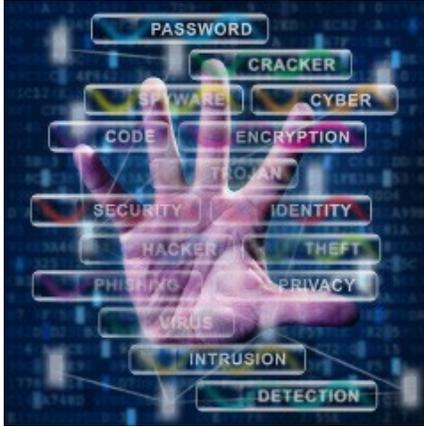


## TECHNOLOGICAL IMPACTS ON INDUSTRIAL CONTROL SYSTEMS

According to the National Institute of Standards and Technology (NIST), ICS is a general term applied to several types of control systems designed to support industrial processes. This includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS) and programmable logic controllers (PLC). While the dissimilarities between the aforementioned systems are diminishing with the advancement of technology, there are still differences worth noting. SCADA systems are generally used to control assets that are geographically dispersed over large areas and are specifically designed to handle long-distance communication challenges. DCS systems were developed to replace PID controllers and are used primarily to control production systems within the same geographic location (power plant, factory, etc.). PLCs are typically used to control specific applications and/or standalone equipment and can be used in both SCADA and DCS systems. A typical ICS system is built using a range of network protocols and contains an array of instrumentation, controllers, human interfaces and support tools.

Since control system upgrades are costly and typically require production loss, they often occur in phases and may not apply to all aspects of a plant (meaning, boiler controls may be upgraded to a next generation DCS but coal handling equipment may still use older PLC technology). Different units/areas within the same plant might also deploy different control systems. The end result often equates to several different types of ICS platforms and vintages that have to be maintained, supported and secured.

The rise and evolution of ICS systems can be directly linked to the introduction of IT capabilities. As previously mentioned, early ICS systems had very little similarity to traditional IT environments since they used proprietary technologies and were isolated from corporate environments. But over the past couple of decades, these older, proprietary technologies have been replaced with cheaper and more available Internet Protocol (IP) devices. The introduction of Ethernet into industrial networking allowed corporate networks and control systems to be more easily connected. It also allowed interested parties to retrieve and leverage process data. While this integration creates a more streamlined process for operations, introducing IT capabilities brings with it complex security implications and makes ICS systems vulnerable to cyberattacks.



## Current solutions have four problems

- 1) Not integrated across OEM vendors
- 2) Not keeping pace with ever-changing threat landscape
- 3) Not built with ICS systems in mind
- 4) Too complicated

## CURRENT ICS CYBER SECURITY SOLUTIONS OFFER PIECEMEAL, STATIC AND LABOR INTENSIVE APPROACHES

Through our work with critical infrastructure operators we have studied a significant number of security solutions offered to meet both the minimum regulatory requirements as well as the more stringent security requirements of industry-leading companies. We did not find a solution that was comprehensive or offered the defense-in-depth strategy necessary for adequate protection.

Furthermore, these systems are complicated webs of proprietary protocols, interfaces and custom software that make standardized tools difficult to develop. As a result, ICS owners have had to patch together piecemeal solutions using manual processes or leverage home-grown technologies.

We saw four fundamental problems with the available solutions:

- 1 They do not offer an integrated defense-in-depth solution that support multiple OEM systems in a given plant or across plants;
- 2 They do not keep up with the ever-changing threat landscape, in part because they do not leverage the investments being made by enterprise IT;
- 3 They are not built to take into account the unique requirements of ICS networks, thereby potentially causing more harm than good; and/or
- 4 The products are too complicated.

### 1. Not integrated across OEM vendors

One of the biggest challenges facing critical infrastructure operators is the fact most facilities do not possess a single ICS system. Instead, there are multiple versions of PLCs and DCS systems (or a combination of the two) at a typical site. Most OEM vendors do not develop leading cyber security products. If they do, they typically only protect their specific ICS platform. This forces asset owners to purchase multiple (often different) cyber security products, all of which have to be managed, monitored and updated.

Some non-OEM vendors have built cross-vendor solutions. But in most cases those solutions are focused on only one or two elements of the threat matrix, such as change management, asset management, or application whitelisting. Furthermore, most of these products only offer monitoring capabilities to inform the operator of issues, but rarely provide tools for remediation purposes (an example would be a product that tells operators patches are outdated, but will not perform that actual patch). What is needed is a solution that can bring together as many of the critical elements of cyber security as possible - both those required by regulatory structures as well as those in critical areas not covered by regulatory requirements.

## 2. Not keeping pace with the ever-changing threat landscape

Total investment in cyber security across the IT landscape was over \$100B in 2015. Leading companies such as McAfee, HP, Tripwire, Symantec and IBM, as well as thousands of startups are investing billions in R&D to stop the next innovative hacker. Every year when Gartner releases their Magic Quadrants, not only are there new players appearing in the upper corners, there are completely new sectors being created for solutions that didn't exist a year or two prior. To compete with an ever-changing threat landscape, customers need to continually improve their defenses.

Unfortunately, ICS cyber security pales in comparison to the total investment made on the IT side. Part of this is due to the sheer number of end points, but part of this is also due to the level of sophistication of these threats. Cyber security vendors only focusing on ICS do not have the resources to invest in the IT side. More importantly, no single vendor can update their proprietary software fast enough due to the daily innovations occurring within the threat landscape. ICS only offerings will find it difficult to keep their customers protected over time. In addition, third party companies that do not leverage best-of-breed IT solutions will struggle to keep up with the large R&D budgets. Eventually, their products will become stale.

## 3. Not built with ICS systems in mind

Although the lines between ICS systems and IT have softened, the fundamental difference between the two remains – ICS systems are connected to physical equipment and are used to control some type of industrial process – whereas IT manages data. This difference brings unique performance requirements and impacts. Some of these impacts include equipment damage, negative environmental issues, production loss and even the health and safety of human lives.

Additionally, most industrial processes controlled by ICS systems are continuous in nature. This means control systems typically cannot be interrupted during production, and must run around-the-clock. Disruptions in the production environment can mean lost revenue, damage to major capital equipment, or even worse, injury to humans or loss of life.

One other difference worth noting is the speed at which these industrial processes and equipment operate. ICS systems must function in real time. IT environments usually do not have the same requirements and if they do, they are usually in the area of seconds rather than milliseconds.

For example, a company that has installed an Intrusion Detection System (IDS) in corporate IT environments may not properly configure their IDS for an ICS system. The amount of network traffic, alarm settings, and protocol alerts can be completely different. Interfering with the operator interface (HMI) can have a harmful impact if the HMI becomes inoperable due to CPU and/or bandwidth constraints. Furthermore, many ICS systems have obsolete hardware and OS's that often generate spurious IDS alerts.

Therefore, off-the-shelf enterprise IT cyber security solutions often fail the "first, do no harm" test. Because of the unique nature of ICS systems, IT solutions can be ineffective or, at worst, bring down the very critical infrastructure they are trying to protect. Vulnerability scanners, network mapping tools, antivirus scans and other cyber security tools required for defense-in-depth strategies must carefully be tuned and tested to ensure there is no impact to the operations environment.

#### 4. Too complicated

**Over the past decade, hackers have expanded the attack vector. Innovative companies have responded with better protection. Unfortunately, the result is often a maze of different alternatives - too complex for ICS managers to understand or support effectively. In many cases, the security protection is so complex it is not used appropriately, which results in a false sense of confidence. In addition, regulatory requirements for compliance reporting makes the job even more complicated. During conversations with our customers, they have often expressed the need for a solution that would simplify their lives and reduce labor costs.**

To succeed in protecting our world's critical infrastructure, operators will need solutions that integrate across OEM vendors, draw on the progressive thinking of the IT cyber security world, and are designed to operate within the constraints of ICS environments.

## A NEW & BETTER MODEL: AN ORCHESTRATED SECURITY CENTER

---

Over the past 8 to 10 years more and more IT security products are being deployed into OT environments. Some of them fit quite well and others are only used sparingly or for small subsets of their product portfolio. However a deep dive into these various tools illustrates that there is value in adopting many of these best in breed tools into OT if done correctly and from an ICS engineer's perspective.

The ICS perspective is the key here. The truly successful adaptations of IT tools into OT environments are always architected, tested, deployed and often also supported by people and organizations with deep roots in process control engineering. Too often a security tool will fail to execute and the only way to properly troubleshoot is to bring in a process control skill set. Making sure your IT tools fit multiple systems is, therefore, heavily reliant upon a co-operative approach between OT and IT.

Extending this co-operation to the selection and deployments of specific tools we find that an integrated approach is the most likely to succeed. The integrated approach must consider the following in its design: 1) in tuning the best IT solutions to operate in ICS environments, 2) a vendor agnostic solution that allows for one, fully converged, defense-in-depth solution, and 3) a simple, user-friendly interface that allows the user to manage the full suite of security products from a single pane of glass. Simply installing multiple security tools with a myriad of logins, screens, reporting and interfaces misses the opportunity to 'orchestrate' your program across those specific tool sets.

And by layering a portal on top of best in class tools your viewpoint is always adaptable and up to date as your underlying technologies and their vendors spend their time and money to keep their components up to date and current. This gives the end user tremendous flexibility and often allows them to leverage their current infrastructure. Integration with multiple antivirus, change management, backup management, etc. vendors has already occurred in some platforms. And as new and better technologies are developed and released, the intention of these platforms is to integrate to them as well.

**Authors:**

Robert K Bevis – CTO

John Livingston – CEO

Rick Kaun – Lead Application  
Engineering

In summary the best possible solution for installing a scalable, operational, affordable cyber security system into an OT environment is to leverage an orchestrated platform. The platform should integrate best in class IT security tools, should be built/installed/tested/supported by ICS engineers and should work across multiple OEM platforms. The platform then rolls up your data and required actions across your specific tools and provides reporting and tracking capabilities. This type of platform is starting to emerge in the market today and the sooner it is embraced by Operational groups the more effective and valuable your security investment will be.

# RKNEAL, INC.

---

FOR MORE INFORMATION:

---



1010 Market Street  
Suite 550  
St. Louis, MO 63101



[info@rkneal.com](mailto:info@rkneal.com)



+1 314 754 8814