



Industrial Defender, Inc.  
16 Chestnut Street · Suite 300  
Foxborough · MA · USA · 02035  
T: +1-508-718-6700  
F: +1-508-718-6701

# An IT Perspective of Control Systems Security

## Abstract

Enterprises with industrial operations typically utilize at least two types of computer networks – Information Technology (IT) - a network that supports enterprise information system functions like finance, HR, order entry, planning, email and document creation; and Operational Technology (OT) - a network that controls operations in real-time. This second type of network supports real-time or control system products, generally referred to as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), Energy Management Systems (EMS) or Manufacturing Execution Systems (MES), depending on the industry.

There has been much discussion and debate around the convergence between Information Technology (IT) and Operational Technology (OT). In an effort to provide better visibility and information flow between revenue generating OT assets and enterprise applications, these systems have often been interconnected, in many cases without properly securing the control systems from cyber attack first. If the IT and OT networks are interconnected, yet not properly secured, a breach to one network can easily transverse to the other, leaving the entire computing infrastructure at risk.

At first glance, interconnected IT and OT networks appear to share similar technologies and so a common approach to cyber-security might be indicated. However, upon deeper inspection, many important differences in IT and OT networks will be revealed. The unique characteristics of OT systems and networks preclude many traditional IT enterprise security products from operating safely without impairing operations, and when introduced, can provide significant disruption and downtime to these real-time, revenue generating assets.

This paper is intended to educate IT professionals on the unique requirements of operational technology and what is required to properly secure these networks from cyber attack, so that organizations can assure security, reliability and safety of information and revenue generating assets.

Andrew Ginter, ISP, CIPS, CISSP  
Chief Security Officer  
Industrial Defender, Inc.

October 2009

## Introduction

Security of a company's critical information (IT) and operational (OT) infrastructure is a key concern in today's world of viruses, hackers, criminals and terrorists. A breach to IT information systems can provide significant economic and social consequences; therefore, organizations have invested heavily to protect computing assets that manage information by deploying firewalls, antivirus, intrusion detection and monitoring solutions. In fact, spending on enterprise security information and event monitoring alone surpassed \$1 Billion in 2008 (Gartner Group, Research ID: G00167782, May 2009). What are companies spending to secure the critical revenue-generating OT assets where the risk of a cyber-security breach has not only significant economic and social impact but potentially physical, life-threatening impact as well? What do enterprise IT and security professionals need to know about this environment to work with the operations staff to properly secure and defend against these threats?

Enterprise IT and security personnel have done extensive work to secure the perimeter, the networks and the hosts on the information side of the business, and are increasingly being asked to extend the corporate IT strategy to address security of operational technology as well. Although it seems logical to deploy the same products on the OT infrastructure as on the IT infrastructure, in fact, due to the unique nature of OT infrastructure, this approach may wreak havoc on daily operations where availability and uptime are the number one priorities.

## Why Control Systems are Different

Control networks and control systems (OT) exist to supervise the operation of large, complex and potentially dangerous physical processes. While some of what you find on operations networks is specialized software running on conventional computers, much of what you find is very different. Some of the oldest control systems still use custom-built computers with custom operating systems or real-time kernels. You may also find devices like Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs) – devices with conventional microprocessors at their core, but with nothing like a general purpose operating system running on them. These devices exist to interact directly with a huge variety of physical sensors and actuators. PLCs especially often play an important safety role as well – they sample every input every few milliseconds, calculate and push new outputs at the same rate, and if any input ever exceeds a safety limit, a PLC can trigger an automatic emergency shutdown of the entire process, or, of the affected part of the physical process.

Securing operational technology networks requires a different paradigm than what Corporate IT professionals have traditionally focused on: "CIA": Confidentiality, Integrity, Availability - in that order. In order to assure confidentiality, no matter what, protect the most sensitive information from loss or disclosure. An outage of a web server, email server or desktop PC can be tolerated for short periods of time; availability may be compromised to repair the affected system, patch it, and prevent access until confidentiality can be assured.

Control systems (OT), on the other hand, and the personnel that run them, have always had a different set of priorities. Industrial operations may be measured on the availability or productivity of the physical process, but that measurement is always in this context: "AIC" – Availability, Integrity and lastly, Confidentiality. The process that is being controlled by these computers is

gathering and disseminating data in real time. It may involve potentially dangerous situations if the equipment is not running properly. Batch processes could run and be collecting data for days, a single batch could be worth thousands or millions of dollars. These OT revenue generating assets must be operational 24 hours a day, 7 days a week, without interruption.

Integrity of the data that is gathered automatically from sensors is often transitory in nature and could be replaced by another measurement on the next scan. The primary requirement is to ensure the accuracy and validity as it travels, therefore many networks address transmission over slow speed serial links. Although the information in an OT system or network can be confidential, protecting the confidentiality of the information is a lower priority than assuring that the real time system is up and running and that the data has integrity.

The biggest difference between IT systems and OT systems is that OT systems are often directly connected to pipelines, electrical grids, water supplies, process equipment, chemical processes, etc. A security breach can have severe consequences including loss of revenue, environmental damage, power outages and even loss of life. Therefore, in high risk industries, such as oil and gas or chemical, a new paradigm of security is emerging: "SAC": - Safety first and foremost, then Availability and lastly Integrity and Confidentiality.

### Security Challenges Abound in Control Systems Networks

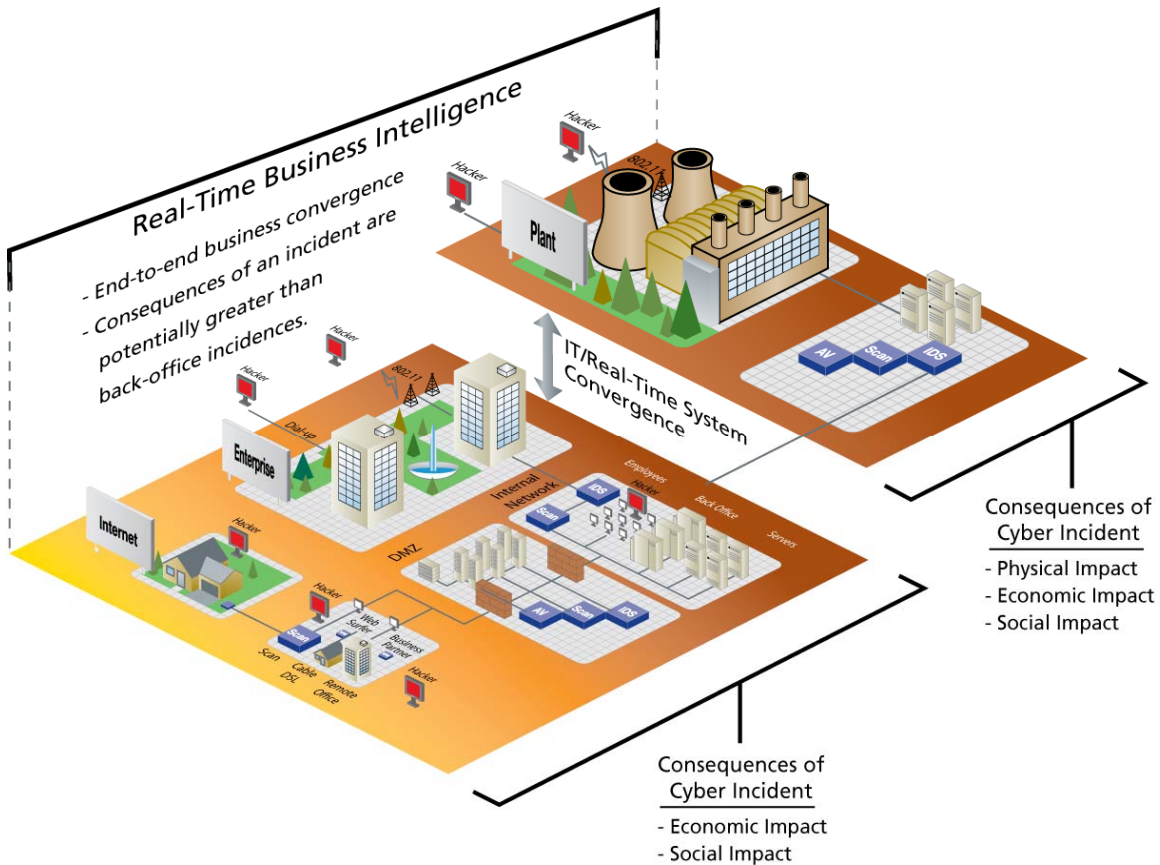
When IT investigates security for OT networks, they may be surprised by what they might find.

- Old hardware and older, un-patched software and operating systems. Often, almost none of the components in a control system are anywhere near the latest vendor patch level. The operations facility cannot afford to test new patches as quickly as they come out, to ensure the continued safe operation of the control system. Patches, if they are applied at all, are applied slowly and very carefully. For example, a test bed system might first be patched and tested. Then for each computer in the operational control system, a patch may be applied on one system in a redundant set, and that system watched closely for a period of time. If it behaves within specification across a wide range of operational conditions, the patch may be applied to other systems in the redundant set. The process is not nearly fast enough to keep up with weekly or daily security patch releases, but over time may be enough to keep most of the control system within several months of current patch levels.
- No anti-virus running. Most control system vendors do not support their software on equipment with conventional antivirus software running. Currently, a very small set of vendors do support anti-virus, often for a small subset of their product line, but most do not. And for many operational systems, applying anti-virus after the fact, without the support of the vendor, can result in the malfunction of the control system.
- Plain-text, unauthenticated communications protocols. Only the newest control systems applications use SSL routinely. It is common to see non-TCP and even non-IP protocols in use. Control system components are specialized and focused on real-time response fast enough to keep a fast-changing physical process stable.

- Vendor-default passwords. Passwords are often not changed so that in an emergency, an engineer, operator or technician can remember the password to the critical component that could avert catastrophe.

### Connecting These Two Networks Introduces Real Risk on Both Sides

There was a time when IT and OT networks were completely isolated from each other and used different equipment, operating systems and communication protocols. While that is still true to some extent, many OT networks have adopted IT technologies because of their cost advantages. Furthermore, companies have realized that there is a wealth of valuable information contained in their SCADA, DCS, EMS or MES computers so they have integrated the two networks to make detailed production, inventory and other operational data readily accessible throughout the corporation.



If the IT and OT systems and networks are not properly secured, and the networks are interconnected, a breach to the OT side can easily transverse to the IT side and vice versa. Who should be responsible for addressing this risk?

Operations staffs and plant engineers are generally aware of this risk and clearly have an interest in securing their control systems networks to ensure their safety, but such security cannot be at the expense of assuring safety, productivity or availability/uptime. The mission of operations staff is to assure safe, productive and reliable operation of the physical processes. Any threat to the

control system is a threat to the safe operation of the physical processes. In some cases, the fact that these systems have been interconnected may not be realized by either side.

IT security staff get involved with OT security generally because enterprise IT staff are given responsibility for security “enterprise wide”, because they are consulted by operations when operations considers a security technology purchase, or when enterprise security staff learn that an operation is planning to install an OT or control system security product.

Unless the IT team includes someone experienced with OT control systems, the first reaction is to look at the problem as an extension of the enterprise security problem. Due to the scale and complexity of the networks they manage, IT departments generally select a few vendors, qualify their products and then apply them as corporate standards. Why not just deploy the same solutions that enterprise IT has used for years and be done?

### A Different Line of Defense is required

Corporate standards selected for enterprise IT networks do not meet the needs of OT networks. IT can have a tendency to look at control systems as just another computer, but treating the two types of systems as equivalents can lead to unexpected and perhaps even catastrophic results. The truth of the matter is that the unique characteristics of OT systems and networks mean that many conventional best of breed enterprise IT security solutions not only do not work on control networks, they may impair the operation of the system or stop it from operating completely.

For example, initiating a port scan on an OT network can have the same impact as a denial-of-service (DOS) attack. Installing the latest patch to fix a security hole may cause the control application to fail and force a line to shut down. When an anti-virus application checks for updates, it may impair the timing of responses to system health/heartbeat messages, which impairment is interpreted by the control system as evidence of a control system malfunction, triggering a safety shutdown. OT Control systems and supporting networks have unique protocols and traffic patterns; conventional IT security components seeing unrecognized traffic may cause unnecessary false alarms or frequent alerts.

A specific case was reported in the NERC Jan-June 2009 Disturbance Reports whereby a disturbance resulted in the loss of the utilities Energy Management System functions including SCADA, AGC, Network Applications and ICCP. The disturbance was caused by the implementation of a device locking security tool which caused the select hard drives to become unavailable resulting in the loss of the above functionality. The tool was being implemented in response to the Critical Infrastructure Protection (CIP) standards. The disturbance remediation consisted of uninstalling the device locking tool and restarting the impacted systems. To prevent the recurrence of this incident in the future, comprehensive testing will be performed to insure that the tool operating characteristics are in accordance with expectations.  
(<http://www.nerc.com/files/disturb09-January-June.pdf>)

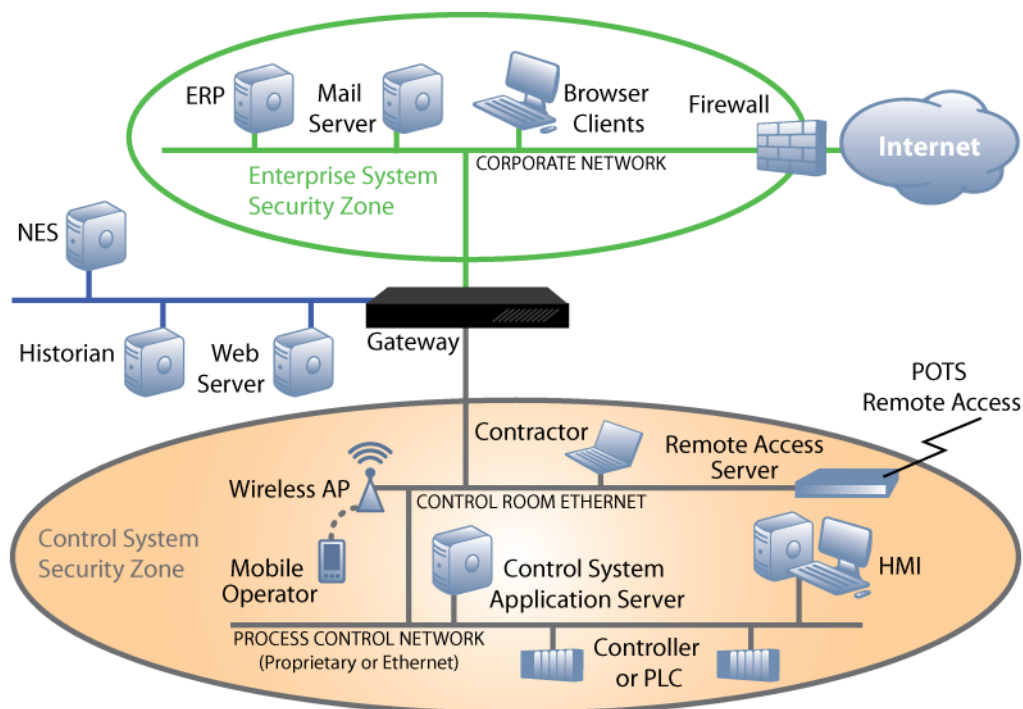
Any new technology, procedure or other change deployed on OT networks must be reviewed to ensure that the change results in continued safe and correct operation of the physical process. This cannot be over-emphasized: operations staff and control engineers are the experts on the safety and availability of the control system and the physical process – they must be involved in

specifying technology requirements and in reviewing, testing and certifying the safety of new technologies and processes before deployment.

### Securing Critical Infrastructure While Assuring Availability and Safety

Securing OT infrastructure from cyber threat can be achieved with many similar policies, approaches, and best practices as for the enterprise, but the products deployed must be designed and optimized to work within the unique requirements of control networks. Some of these unique constraints include:

- Recognition of the unique protocols related to network traffic so as not to cause unnecessary alerting.
- Configuration of control system intrusion sensors to detect the known, good traffic and alarm on anything else.
- Careful design in adding intrusion detection sensors so that they consume minimal CPU and network bandwidth to avoid disrupting time-critical operations.
- Support for access control for remote devices such as PLCs, RTUs and distributed controllers.



Enterprise and Control System Security Zones

As with the enterprise, the solution often deployed first is an “electronic security perimeter” (ESP) for the OT network: IT and operations should jointly define a demarcation boundary between the enterprise network and the OT network. This boundary protects the enterprise network from

vulnerabilities in the control system devices without requiring the imposition of strict IT security policies that are inappropriate for OT networks, and protects the operations network from threats that arise on the enterprise network. The operations network should have no routine access to electronic mail or the internet. Operations personnel need such access, but workstations with such access should be on the enterprise network side of the ESP.

Ideally, the interface between the enterprise IT security zone and OT control system security zone should be a firewall or more modern “Unified Threat Management” (UTM) device that is used at the edge of the control network to dynamically regulate traffic to and from critical OT systems, to block viruses and intrusion attempts, and to provide secure connections to authorized external users. The device should be able to be configured for a variety of pre-planned lock-down responses based on current threat levels or routine maintenance.

The second level of defense often deployed as part of a “defense-in-depth” strategy is intrusion detection, or, beyond securing the perimeter, providing the capability of watching closely, and reporting on, what is inside the perimeter for any suspicious behaviors. These intrusion detection measures must be passive with tight resource controls and must be carefully introduced so as not to consume CPU, memory, network, disk or other resources to impair system performance.

Network intrusion detection sensors must be able to passively monitor all network traffic within the security perimeter, enabling detection of any suspicious activity, including internally generated attacks, as well as any that may have circumvented the perimeter defenses. The network sensors must be able to recognize the de facto protocols used by process control systems (Modbus TCP, DNP3, ODVA Ethernet/IP, ICCP, etc.) and generate alarms for logging and diagnosis.

Host intrusion detection sensors which reside in and secure the critical process control host systems such as DCS workstations, SCADA servers, historians, substation routers, etc. must be able to be customized for the control applications running on a specific control system and should be designed for minimal impact on older SCADA and DCS workstations which are often resource constrained.

To be most effective in managing the security environment, operations personnel need access to a central console that monitors and protects control systems from threats and vulnerabilities by collecting all of the event logs generated by devices within the plant, including the perimeter protection devices. A Security Event Manager is a critical component that provides IT-like visibility to control system networks, archives event logs, processes logs in real time and generates alerts when suspicious patterns of behavior are observed.

### Conclusion and Recommendations

As organizations increasingly merge their Information Technology and Operational Technology systems to support business requirements, the responsibility for securing all of these important assets from cyber attack can converge as well. Companies can benefit from having an enterprise view across all security systems, but the products in the control world need to be optimized for the unique needs of this environment.



On the OT side of the boundary, select technologies that are designed or certified for use on industrial networks. Select technologies that are passive – the control system needs no new points of failure. Data collection within the control system must not impair the behavior or performance of the control system. Select technologies that are simple - corporate network administrators and call center personnel are not going to understand the unique and complex systems on OT networks in an enterprise, but each site's operations personnel maintaining their network do understand their networks. Give those engineers tools they will understand, and that help them understand their unique systems. Or consider outsourced managed security services to provide in depth expertise and 24x7 coverage to assure uptime and availability of OT networks.

IT and OT personnel responsible for security should work together to devise the appropriate Defense in Depth strategy to protect all systems from cyber attack.

Finally, it's important that IT and control system engineers establish a dialogue about security and safety issues. Both sides have a lot to learn from each other. Security is an on-going process because threats and vulnerabilities are constantly evolving. Working together is the best way to ensure the safety, reliability and security of mission-critical OT networks.

###



### About the Author

Andrew Ginter is Chief Security Officer of Industrial Defender, Inc. Andrew is responsible for technology direction, product architecture and corporate IT for the company. Ginter has more than 25 years in security systems and software development, and brings critical technical leadership to Industrial Defender. He previously held various technical management roles at Agilent and Hewlett-Packard. A central theme in Ginter's career has been the development of high quality, reliable, and secure systems software - including compilers, real-time operating systems, network software, industrial control systems, message-passing middleware and alert management systems. Ginter holds a B.Sc. in Applied Mathematics and a M.Sc. in Computer Science from the University of Calgary. His professional background also includes an Information Systems Professional (ISP) accreditation from the Canadian Information Processing Society (CIPS), and a Certified Information Systems Security Professional (CISSP) from the International Information Systems Security Certification Consortium (ISC2).

### About Industrial Defender

Industrial Defender, Inc., the global leader in Cyber Risk Protection™, is the first company to offer a completely integrated cyber security solution designed to protect the real-time process control and SCADA environment in a flexible and cost effective platform. This comprehensive Cyber Risk Protection™ Lifecycle solution enables the efficient assessment, mitigation and management of cyber security risk within the critical infrastructure network domain. Industrial Defender is a privately held company with over 18 years of real-time process control and SCADA industry experience and more than 7 years of industrial cyber security experience. Industrial Defender has completed more than 100 process control / SCADA cyber security assessments, more than 10,000 global technology deployments in securing critical infrastructure systems, more than 3,000 mission critical SCADA deployments and provides managed security services for 170 process control plants in 21 countries.