SOLUTION BLUEPRINT
Intel® Core™ Processors
McAfee* Security Solutions
Industrial and Energy Industry

Increasing Situational Awareness and Multi-zone Protection of Industrial and Utility Infrastructure

A comprehensive end-to-end security solution based on leading Intel and McAfee* technologies

Protecting critical infrastructure is about a comprehensive solution – not a single product

The complexity and diversity of equipment used in factory automation and electric power delivery systems makes protecting against cyber attacks ever more difficult. Industrial and utility infrastructure comprises a diverse set of networks that cannot be effectively secured by simply "bolting on" technologies designed for enterprise IT. Aging assets, such as programmable logic controllers (PLCs), power meters and digital relays, predate the Internet revolution, and therefore are particularly vulnerable to attack and unable to report malicious activity up the chain. Hackers have grown more sophisticated and dangerous, increasing the need to improve the situational awareness of industrial IT and utility control centers, so they can more quickly detect and defuse zero-day attacks.

A comprehensive solution requires multiple products to create layers of security that operate together without introducing great complexity, degrading performance or impacting availability. This can be accomplished with Intel® vPro™ technology-based solutions and McAfee* software that deliver greater situational awareness, seamless multi-zone protection, native supervisory control and data acquisition (SCADA) support, and remote device management. The solution integrates a number of McAfee cyber-security products relevant in industrial automation and energy designed to protect embedded devices against malicious attacks. Moreover, device management is enhanced through the use of Intel® Active Management Technology (Intel® AMT)[1], which enables network operators to gain full control of an attacked device regardless of its hardware or software state. Intel® Virtualization Technology (Intel® VT)[2] provides a layer of separation between applications running on the processor, thus helping to keep rogue software from infiltrating safety-critical applications.

Cyber-Security Challenges Facing Critical Infrastructure

Developing an end-to-end security solution is complicated by the diversity and scale of industrial and utility networks and equipment. Adding another level of difficulty to the task, some companies are simultaneously merging their information technology (IT) and operations technology (OT) infrastructures that have been mostly independent over many years.

Managing different network environments

Organizations faced with securing factory automation and electric power delivery systems have an enormous task. There are multiple zones that must be addressed, including corporate IT, SCADA and device networks, and each zone has unique technical challenges. The composition of these zones is illustrated by the 3 x 3 matrix in Figure 1, which also represents typical host, network and system environments for each.

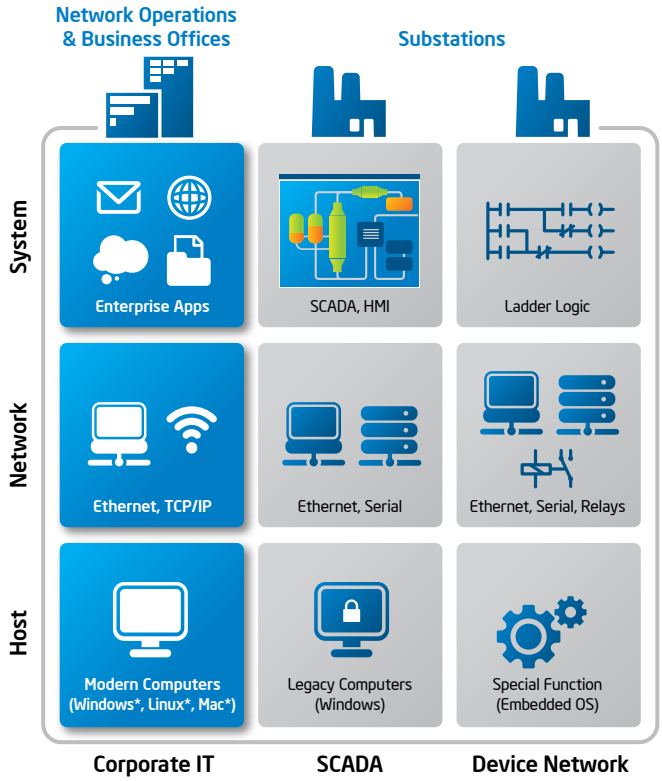


Figure 1. Utility Infrastructure Represented in a 3 x 3 Matrix

Some of the key challenges by zone include:

- **Corporate IT** – A significant amount of effort is required to deploy and manage a broad combination of security products (e.g., firewall, IPS/IDS, VPN, anti-virus, anti-spam and content filtering) needed to protect wireless and wired networks.
- **SCADA** – Control and management software runs on modern operating systems and networks. However, their high-availability requirements and long lifecycles can make it difficult to update and patch these systems because of the necessary downtime and fewer security fixes as the operating system becomes obsolete.
- **Device networks** – Control devices, like PLCs and remote access controllers, require real-time embedded operating systems and run specialized software to execute automation logic. The myriad of controllers, sensors and intelligent electronic devices that make up an automated system are largely unsecured, complicating efforts to enforce consistent security policies and detect an attack. Devices, in general, are becoming more connected.

Coping with data overload

Security devices on the network are producing an incredibly large numbers of logs, overwhelming IT departments. Some of the information, like content-based data from deep packet inspection, is sometimes kept around for a year. This big data problem requires a big data solution.

Simplifying endpoint manageability and improving visibility

Endpoints are often out-of-site and out-of-mind, especially when they lack the ability to communicate a security breach. When a device fails, a costly "truck roll" response may be needed to fix the issue, unless the system can be managed remotely.

Providing the right security context for the grid

Standard IT products can't see what's happening within an industrial or utility infrastructure, and if they can, they still don't understand the unique lexicon of that infrastructure, making it difficult to apply traditional IT security measures within a control system environment.

Intel® vPro™ Technology for Device Management and Improved Virtualization

Intel vPro technology on select Intel® Core™ i5 and i7 processor-based platforms offers a more robust remote management solution and a more secure virtualization environment compared to software-only solutions.

Increasing System Availability with Remote Management

When a piece of equipment on the power grid goes down, a service interruption usually occurs, and a technician is dispatched to find, isolate and fix the problem. On-site repairs are especially costly for the energy industry because of geographically dispersed equipment, such as meters located at every customer site, buried underground or mounted on top of utility poles. On the factory floor, equipment failures can stop the production line.

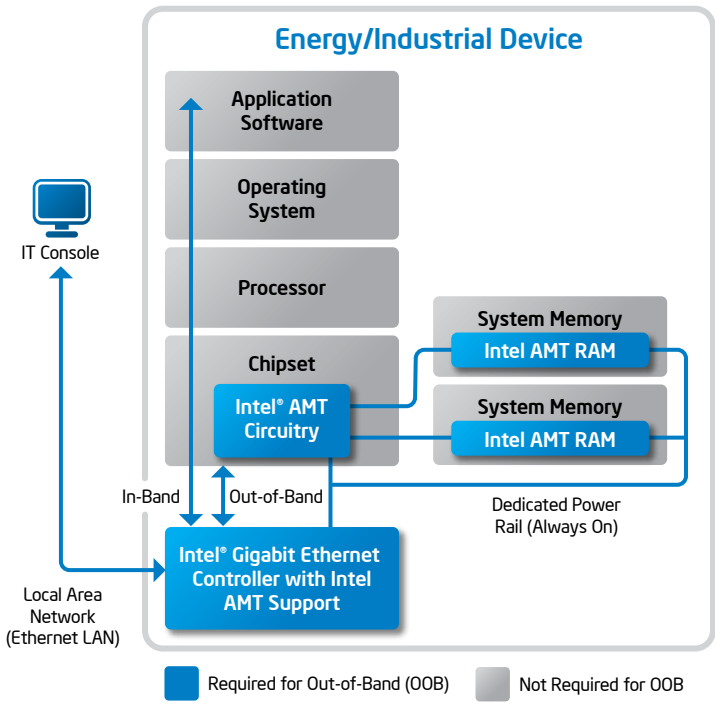


Figure 2. Intel® Active Management Technology Components

Alternatively, utilities and factories are turning to remote management solutions to diagnose, repair and get equipment online faster at lower cost. Today, almost every power system is connected to a data network in order to share power monitoring and switching information between utility operators, consumers and power networks. The data network can also provide the communications link for remote management terminals used for many IT support tasks, such as updating software, repairing systems and collecting inventory information. When communicating with remote management systems, many power systems use the same networking functionality (e.g., Ethernet NICs, CPU, operating system, protocol stacks) for both standard LAN and remote management communications. When equipment fails, this "in-band" approach has the drawback of relying on the continued operation of many equipment components: CPU, operating system, hard disk drive and system memory. In other words, if the system is not functioning, the only option may be to send a crew.

Providing a significant remote management breakthrough, Intel Active Management technology (Intel AMT) implements a special circuit in the Intel vPro technology-enabled chipset that can access and control the system, even when the system is powered off or the software is corrupted. This circuit establishes an "out-of-band" link so the system communicates with a management console without relying on the system's standard networking functionality, as illustrated in Figure 2. Intel AMT is a key component of McAfee* ePO Deep Command, which is used to manage endpoints and is discussed later.

Cutting IT Support Costs

By employing Intel AMT technology-based management solutions, utility operators can remotely fix a wide assortment of system defects, track inventory – including warranty and software license information – and track intermittent failures, as described in Table 1. This capability reduces cost and saves time by supporting devices without requiring hands on intervention.

Improving Security with Application Isolation

Securing applications and data is essential for energy and industrial systems, and this includes providing protection between known software components as well as malware that may have infiltrated the device. Using hardware-assisted virtualization, applications can be isolated in secure virtual machines (VM), whose memory space is protected by hardware features in Intel® processors and Intel VT. This means software running in a VM only has access to its own code and data regions, unable to page outside its memory boundaries.

Capabilities	Results
Fix Hung Systems	Restore systems by cycling power, reloading software or booting from a 'gold' hard drive over the network.
Track Intermittent Failure Modes	Access error log and event records from FLASH, accessible at all times to the remote console.
Protect Against Infected Devices	Quarantine at-risk systems by cutting off their in-band network connection, effectively isolating the virus.

Table 1. A Subset of Intel® AMT Technology Capabilities and Results

KVM (Keyboard-Video-Mouse)

Intel AMT on 2nd generation Intel Core processors has been enhanced with a feature called KVM redirection over Internet Protocol (IP), permitting the keyboard-video-mouse (KVM) for an IT console to control and display the graphical user interface (GUI) of an embedded device in the field. As a result, technicians can manage the remote device as if they were sitting right in front of it using normal input devices and not only through command line instructions. To resolve issues, it's possible to reboot the device, observe errors, launch tools for analyzing failure data and guide the OS to fix the error. Even in the case that a technician would have to physically go to the computer to repair it, there would be a need to connect a keyboard and mouse to the computer, which typically doesn't have these input devices permanently connected. An important benefit of this implementation is the KVM is separated from computational blocks of the system, which is a key requirement for use in substations.

Virtualization provides the ability to run multiple virtual machines (VMs), containing an OS and its associated applications, on the same physical board by abstracting the underlying processing cores, memory and devices. This is achieved by adding a new software layer, called a virtual machine monitor (VMM), which manages the execution of 'guest OSes' in much the same way that OSes manage the execution of applications. Systems can run real-time operating systems (RTOS) and general-purpose operating systems simultaneously, as depicted in Figure 3, which provides both fast response for time-critical code and many standard features for application development. If the guest OS running the GUI crashes, the RTOS and the time-critical functions will continue to run deterministically because they are isolated and protected.

Virtualization has been around for many years, most notably used in data centers where many applications are consolidated onto a single server. The added benefit from using Intel VT is it speeds up the transfer of platform control between the VMM and guest OSes by using hardware-assist to trap and execute certain instructions on behalf of guest OSes, relieving the VMM of such duties. These commonly used virtualization operations are very secure because they are performed in hardware and thus unalterable by hackers.

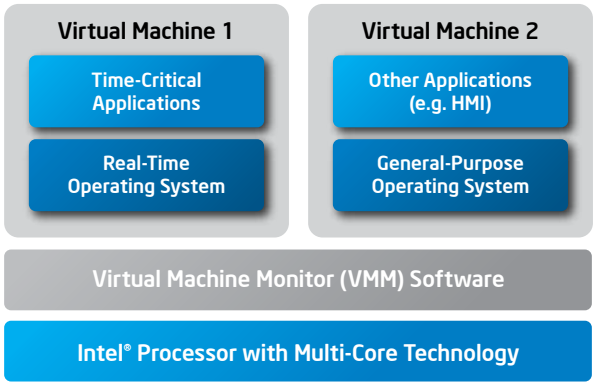


Figure 3. Virtualization Isolates Mission-Critical Code

Security Solutions for Industrial and Utility Infrastructure

Operations technology (OT) departments need products that protect against both zero-day and known attacks in a manageable way. Intel and McAfee address this with a select group of products and technologies that are highly applicable to critical utility infrastructures.

Situational awareness

In order to stop zero-day attacks, OT departments need actionable intelligence, not just security data. This is the role of the McAfee* Enterprise Security Manager, which incorporates security information and event management (SIEM) for processing logs from all the organization's sources and organizing them in a central place in near real-time. The SIEM parses valuable information from the logs, normalizes the data and correlates the information into a common taxonomy that is understandable to humans. The result is a contextual view that helps identify and isolate attacks produced by unknown malware.

The SIEM stitches the distinct events together, looking for patterns in order to answer questions such as: Is there a threat? What and how big is the threat? Where is it coming from? What is my exposure? How can I best react to this threat? This is called situational awareness.

For example, when the SIEM examines an IP address in a log file, it parses the host name or true location: internal or external source. Moreover, information about the user is inferred, such as her/his role in the company, entitlements, locations, cubicle and manager name. With this type of information, the SIEM can detect and report anomalies, like someone from the loading dock (e.g., warehouse employee) accessing the configuration file for an embedded controller. In another case, the SIEM knows many failed login attempts are frequently followed by successful logins from the same source, indicating a possible brute force attack.

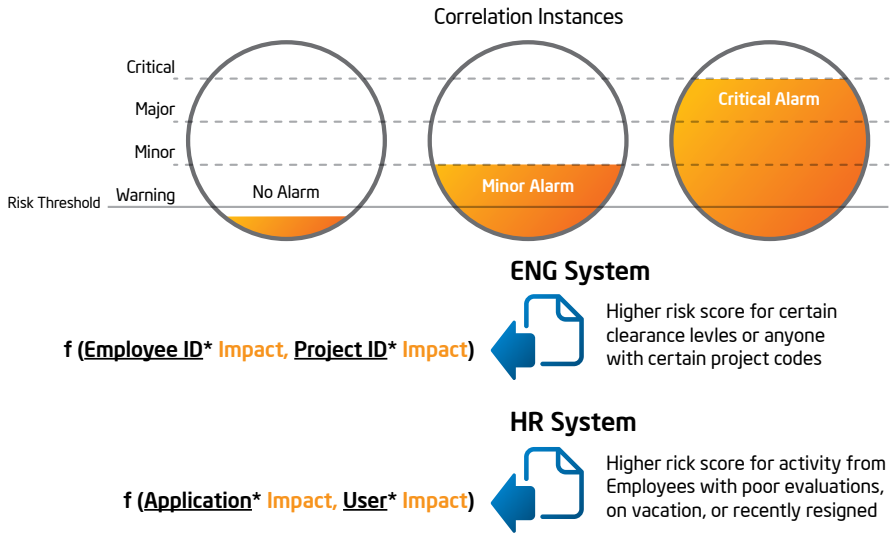


Figure 4. Scoring Models that Pair Employees with Critical Applications

The McAfee Enterprise Security Manager can tap the network for more information that may not be in logs, but is nonetheless instrumental in protecting critical systems. The SIEM provides traditional monitoring of computing infrastructure and risk, along with the modeling of business operations and processes that generates several levels of alarms.

Examples of scoring models are shown in Figure 4, where the SIEM assesses the risk of individual users who are accessing critical systems. For instance, the IT department may create a function that checks the clearance of users accessing applications for a classified project and assigns higher risk scores for office administrators or for users in foreign locations. Similarly, a function may look for unusual behavior by monitoring activity of employees who are on vacation, recently resigned or faired poorly on their last performance evaluation.

Protecting Against Stuxnet-class Threats

Stuxnet, a sophisticated cyber weapon that targeted and sabotaged automated uranium enrichment facilities in Iran, changed the scope and context of control system cyber security forever. Stuxnet raised the bar—by combining stolen certificates and multiple zero day exploits to deliver a payload that was designed to find and disrupt a specific industrial control process. That payload was also unique, in that it targeted programmable logic controllers (PLCs) used within the automation system, assets that were thought to be untouchable due to their isolation, obscurity and specialized functions. With the knowledge that these systems are vulnerable, improved cyber security measures are required to deter the threat of additional "Stuxnet-class" cyber incidents.

How to Defend Against Stuxnet

Because Stuxnet is an adaptive and sophisticated threat, defending against it requires improved protection at three levels: better network protection to secure the initial attack vectors of the worm; better host security to block the worm's ability to infect SCADA systems and the PLCs that those systems control; and better situational awareness, to detect any incidents that do occur.

Network protection: Network protection that supports industrial control protocols, such as Modbus, Profinet, Ethernet/IP, OPC, ICCP, etc., is needed so these protocols cannot be exploited. McAfee* Network Protection secures the native communications of SCADA and control systems; thus, the initial infection vectors of a Stuxnet-class attack are minimized.

Endpoint protection: All assets used to monitor, manage or control an industrial system require strong endpoint protection to safeguard against Stuxnet-class payloads, which are designed to take advantage of the inherent command-and-control capabilities of these systems. McAfee* Application Control, which allows only whitelisted applications to be used, can lock down both SCADA servers and PLCs to ensure the control environment is not compromised.

Situational Awareness: To protect against blended attacks that infiltrate across zones, security monitoring must function across zones as well. By extending the centralized policy and threat management capabilities of McAfee* ePolicy Ochestrator and Mcfee* Enteprise Security manager in the industrial control environment, Stuxnet-class threats can be detected, assessed, analyzed and mitigated.

Real-World Deployment

While Stuxnet targeted a particular SCADA system, it proved to be a use case that puts all industrial control systems at risk. To address this risk, McAfee* is working with leading control system vendors—including Siemens, Schweitzer Electric Corporation, Invensys, Emerson, Rockwell Automation, ABB, Yokogawa and others—to validate key security technologies and develop a cohesive control system cyber-security solution.

Unified, multi-zone protection

McAfee* ePolicy Orchestrator (McAfee* ePO) software, the foundation of the McAfee* Security Management solution, unifies management of endpoints, networks, data, and compliance solutions. The software enables utility IT organizations or substation network operation centers (NOCs) to centrally manage security and achieve dramatic efficiencies. Used on nearly 60 million nodes, the software increases overall visibility across security management activities, thereby improving protection. In addition to being the most advanced security management software available, McAfee ePO has special capabilities that better secure industrial and energy assets:

- **Application whitelisting** – Particularly effective against zero-day attacks, whitelisting is well-suited for fixed-function devices running only known, trusted software. Permitted code – registered on a carefully controlled list – is allowed to execute, while unknown software is prevented from running. When untrusted software attempts to run and gets blocked, the whitelisting application alerts McAfee ePO, prompting potential corrective action. Whitelisting is a "light" approach, using far less CPU and memory resources than blacklisting products such as anti-virus software. Moreover, blacklisting solutions are difficult to keep current in these environments, as in working with outdated signature files that impair the ability of anti-virus solutions to detect and remediate malware, thus minimizing the overall effectiveness and value proposition.

- **McAfee ePO Deep Command** – Lowering the cost to service endpoints, this solution minimizes expensive onsite visits to address security incidents or fix equipment. Security administrators can remotely deploy, manage and update security and device software on disabled or powered-off endpoints. This is possible because McAfee ePO Deep Command employs Intel AMT, which establishes an out-of-band (OOB) connection to the endpoint that allows utility IT departments to take control of the device regardless of the hardware or software state – even, potentially, a rogue device. Using Intel AMT, the device can be taken offline and replaced by a redundant, failover device, thus minimizing downtime. Subsequently, the infected device is cleansed remotely by reloading its software image and then brought back online.

Malware copied to computing assets

For those concerned about malware on a USB drive infecting the factory floor or energy assets, McAfee* Device Control helps protect critical data and devices by controlling the use of removable media. It provides tools to monitor and specify permitted data transfers between assets and USB drives, CDs and DVDs, among others. Integration with McAfee ePO facilitates gathering of details such as device, time stamp, and data evidence for prompt and proper audits. IT organizations can specify in detail which devices can be connected and what content can and cannot be transferred with removable storage.

Intrusion prevention

The McAfee* IPS is an intrusion prevention appliance that actively detects, analyzes and protects the network from an array of security attacks, including viruses, worms, spyware and Denial-of-Service (DoS) attacks. Utilizing a patented relational data management engine, the IPS identifies and neutralizes threats and detects anomalies in real time, before they disrupt the network.

Database protection

McAfee* Database Activity Monitoring automatically finds databases on the network and protects them with a set of preconfigured defenses or policies customized for a particular utility environment. This is particularly valuable when a database hasn't seen a patch in a long time, perhaps because the software vendor doesn't have access to the system. The solution protects data from all threats by monitoring activity on each database server and by alerting or terminating malicious behavior.

Continuous Compliance

Organizations responsible for critical utility infrastructure are forced to comply with a number of regulatory mandates, including the North American Electric Reliability Corporation's (NERC) CIP (Critical Infrastructure Protection) standard. This is a slow and costly manual effort. McAfee helps by automating the process of reporting and demonstrating compliance with multiple regulatory mandates across enterprise IT, SCADA and device networks. Because McAfee offers situational awareness across these zones; implements controls across endpoint, network and data; and supports native SCADA, the solution provides continuous compliance in a fast, automated and easy-to-use fashion that addresses auditor requirements in minutes instead of hours or days.

The NERC CIP standard requires a KVM interface that is located in a separate room from the host; today, expensive, tethered KVM extenders are typically used. This requirement can be satisfied more cost-effectively with the Intel AMT KVM feature because additional KVM hardware components are not needed, as previously mentioned.

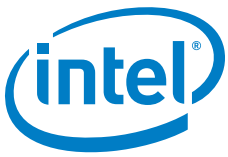
A Comprehensive Solution for the Automation and Energy Industries

Protecting utility and industrial infrastructure is challenging for many reasons, including its network diversity, data overload, complex endpoint management and tools that lack the right security context for the grid. Using Intel Core processor-based platforms with Intel vPro technology in combination with McAfee security solutions is unique in that it unifies situational awareness and multi-zone protection using purpose-built, compliance-oriented solutions that prevent malicious attacks in real time. This end-to-end security solution features advanced remote management using Intel AMT, with out-of-band capabilities that are more robust than in-band software solutions. The end result is a comprehensive solution for securing critical infrastructure – designed to protect against malicious attacks, increase equipment uptime and lower the cost to service endpoints.

For more information about Intel solutions for industrial applications, visit www.intel.com/go/industrial

For more information about Intel solutions for the energy industry, visit www.intel.com/go/energy

For more information about McAfee security solutions, visit www.mcafee.com



[1] Intel® Active Management Technology (Intel® AMT) requires the platform to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. With regards to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see http://www.intel.com/p/en_US/embedded/hwsw/technology/amt.

[2] Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM), and for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

Printed in USA 0412/VS/SD/PDF ♻ Please Recycle 327215-001US