

Cisco Ethernet to the Factory Solution: Securing Today's Global Networks in Industrial Environments

As global manufacturing increasingly bases its industrial automation and control systems on open networking standards, manufacturers have been able to operate more efficiently and effectively. This new ability to integrate industrial and enterprise data enables real-time information sharing across the value chain, which increases data visibility, makes systems more available, assists rapid resolution of problems, and reduces operational and support costs.

Such powerful connectivity throughout the company and to outside partners has become indispensable for success. But it also creates an environment where security threats are a far greater concern. Because of the critical nature of industrial systems and the risks associated with them, it is more important than ever for manufacturers to implement a comprehensive network security strategy that protects while it enables access and integration to achieve efficiencies and complete visibility.

Working closely with Rockwell Automation, Cisco® has created the Ethernet to the Factory (ETTF) solution to address these needs by providing highly secure Ethernet-based connectivity throughout the manufacturing plant and enterprise. By relying on the combined knowledge base and expertise of these two companies, factory and business managers at any location can access critical real-time information on demand, from process performance, work-in-process inventory, and asset utilization to financial reports, distribution schedules, and internal memos, to optimize production while helping to ensure complete security.

Over the years, Cisco has invested significantly in security to develop a wide range of powerful product offerings. The Cisco ETTF solution takes advantage of a family of industry-leading security technologies to help ensure the availability and integrity of the industrial network, while evolving to keep pace with the ever-changing nature of security threats. Cisco and its partners provide detailed, ongoing design guidance to make sure that manufacturing capabilities continue to protect critical automation and IT networks in the long term.

The Cisco ETTF solution helps manufacturers moving to industrial automation systems based on standard Ethernet to connect, integrate, and secure their systems to help ensure consistent and reliable performance. Cisco's recommended security model enables successful deployment of complex technologies in a manufacturing environment, meeting the needs of the factory floor and automated systems as well as enterprise business applications.

The Security Challenges of Manufacturing Environments

The potential impact of security-related incidents to manufacturing can be devastating; resulting in system downtime, loss of critical data, and other potential consequences. Even outages and performance degradation are unacceptable in these real-time, on-demand environments. Manufacturing business success depends on continuous, ongoing factory production, and downtime is incredibly expensive.

Today's movement toward commercial off-the-shelf (COTS) technologies, such as the Microsoft Windows operating system, Distributed Component Object Model, Ethernet and TCP/IP, and Internet-based applications, increases the risk. Open, standards-based functionality provides great benefits in terms of visibility, efficiency, and cost-effectiveness, but it also exposes the manufacturer to a wider range of security threats, ranging from malicious code and attacks by hackers to performance issues due to unexpected traffic, network scans, or similar activities. Then too, as hackers become increasingly aggressive and sophisticated, and as disclosure of vulnerabilities occurs in real time, the time between the discovery and the exploitation of a COTS vulnerability is rapidly decreasing. While most security issues have been effectively managed in IT networks for several years, security has not typically been the focus of engineers who design, deploy, and manage production control networks.

The requirements of industrial automation and control systems compound the challenge of securing industrial environments. To ensure consistent uptime and performance, these systems demand very low levels of latency, predictable performance, and high availability. At the same time, they often have technology limitations (memory, processing power, old operating systems, etc.), patching limitations, and specialized network management considerations. Also, it is often important to provide guest and remote access to production systems and have visibility and integration of data between enterprise business and manufacturing applications. All these factors increase vulnerability and can affect the security tools that can be deployed.

Although it is tempting to conclude that plant networks protected by a corporate firewall must be safe, and therefore immune to attacks on corporate mail and web servers, the situation is not that simple. Small security failures, an improperly secured wireless access point or a forgotten dial-up modem attached to a programmable automation controller for automated systems, a personal computer, or even a remote access server directly connected to the plant network, can provide easy access for a determined attacker. Intranet connections with business partners, suppliers, system integrators, or vendors within the plant can also provide ample opportunity for attackers to gain access without having to breach the Internet firewall or the firewall between the enterprise and plant networks. Even control systems on their own separate network are at risk if users can access them. And once access is gained, attackers can find many familiar and largely vulnerable targets (namely, Windows-based workstations and servers) that can be compromised using existing tools and techniques.

While no specific log currently exists of security incidents in manufacturing control systems, the data that does exist indicates that these systems face the same challenges and threats as traditional IT environments. According to the British Columbia Institute of Technology (BCIT) Industrial Security Incident Database (ISID), there has been a sharp increase in manufacturing security incidents since 2001. As of mid-2006, approximately 119 incidents had been reported to the BCIT. When you consider that only a small percentage of such incidents are reported (an estimated 2–10 percent)¹, those statistics become more alarming. Given the severe implications of failure in a manufacturing environment, such a trend should raise great concern.

¹ Based on traditional industry databases and Cisco estimates

These trends and issues are not unique to manufacturing. Organizations across many industries face similar challenges, particularly as hackers find new ways to exploit systems for financial gain. Manufacturing environments, like other embedded control systems, are especially at risk of attack since the cost of downtime is so high. As a result, the number of extortion attacks is increasing to the point where some manufacturers have found it easier to pay ransoms to regain access to a lost system or stolen or encrypted data. This type of extortion is also being seen in healthcare, finance, and critical infrastructures (such as traffic-control systems).

Manufacturing Security Requirements and Priorities

The first step in developing a manufacturing network security approach is to define the secure environment's fundamental priorities, which will vary depending on the environment. This approach should be used for each security zone² (such as a manufacturing control network or a plant site IT network) across the enterprise to determine system needs and the best solution to support basic business requirements. These business necessities typically are availability, confidentiality, and integrity.

- **Availability:** The ability to preserve operational continuity. Information, data, services, networks, applications, and resources should be accessible in a timely manner when needed. It's essential to protect the availability of these assets from intentional or unintentional impact. Additionally, security services cannot impact the operational continuity as they execute.
- **Integrity:** The ability to preserve the authenticity of information, data, service, and configurations and to help ensure no unauthorized clients unexpectedly or covertly modifies any of these aspects.
- **Confidentiality:** The ability to maintain the privacy and confidential nature of potentially private or sensitive information, and to help ensure that only authorized entities have access to it. This applies both to data at rest and data in transit during communication.

A compromise in any of these three requirements carries the potential of serious impact or loss to a system or physical assets. It is important, however, to understand the relative priorities between the requirements to make sure the security solution supports business demands. In a typical industrial automation and control system, availability is the highest priority, followed by integrity of data, with confidentiality as the lowest priority. This may vary with the specific environment (if, for example, there are significant regulatory requirements), but confidentiality is rarely considered more important than availability or integrity. This differs from a manufacturing company's traditional IT environment, in which confidentiality is often the highest priority (to protect customer information, batch recipes, or intellectual property), followed by integrity and availability.

System designs need to take into account these relative priorities to help ensure the appropriate security capabilities are implemented and aligned with policy. For example, if confidentiality is a priority, the network may have very stringent access requirements or may incorporate security solutions that shut down access to the system when it detects unusual activity. Depending on how they are configured, these solutions can have a negative impact on availability and might not be appropriate in a manufacturing environment. Business priorities also help to define the appropriate architecture for network services, such as Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and other critical network services.

² A security zone is defined as a logical grouping of physical, information, and application assets sharing common security requirements. The concept of security zones is described in more detail below.

The manufacturing architecture should also be designed for a worst-case scenario to make sure systems remain available during unusual events, such as during alarms and notifications. If the network is not designed to maintain high levels of performance, or if it shuts down access or reacts unpredictably to unusual activity, it will not achieve high availability and the security program will not have supported the objectives.

The security tools implemented to support the above-mentioned high-level requirements must meet secure usability and manageability requirements:

- **Low end-user or end-device impact/High end-user transparency:** The measures used to protect the network environment should be chosen, designed, and deployed so as to minimize impact to automation and control devices and systems, achieving a balance between security and end-device impact. Increased end-user impact and complexity also has the potential to affect the overall effectiveness of a security design, as it is human nature to try to avoid complexity.
- **Manageability:** A major aspect of delivering security services relies on increasing the overall visibility of the network and its transactions. It is imperative that manageability be considered when creating a security design, especially since online security is not typically an expertise found in production environments. Manageability includes being able to properly configure policy, rules, and parameters for the security system, but also involves key issues such as monitoring, feedback mechanisms, and telemetry data gathering.
- **Low performance impact:** The implementation of security measures in a network must take into account the underlying performance requirements to avoid affecting the overall performance of the system. Most industrial automation and control networks have unique performance considerations, including low latency and jitter, and technology limitations (processing power, memory, operating system, etc.) on many devices.
- **Authentication, authorization, and accounting (AAA):** The network solution should provide the ability to implement security services that provide the necessary control mechanisms to limit access to systems, applications, and network devices, as well as accounting mechanisms to track access, changes, and events.

Other security objectives that need to be considered when designing the architecture relate to the functional capabilities and access desired. The most important considerations include:

- **Remote access via a trusted connection:** The ability to access industrial automation and control systems remotely to provide quick and efficient support.
- **Guest access inside the facility:** Providing a mechanism for guests to access control systems and the Internet for third-party support personnel.
- **Device access (protocols):** The ability to communicate with all networking equipment and suitably equipped devices using standard networking protocols (SNMP, HTTP, etc.) instead of only industrial protocols (CIP, ProfiNet, Modbus, etc.) to achieve visibility and efficiency gains. (Industrial protocols are also critical, but remaining limited to industrial protocols limits efficiency and management.)
- **Shared access to data:** Allowing access to manufacturing data for efficient implementation in business systems and visibility of operational status.
- **Secure access from control systems to Internet and intranet:** Implementing systems that enable secure access to specific Websites and Web-based applications required for business operations (these capabilities must be carefully implemented, and open access is not recommended).

The architectural design of Cisco Ethernet to the Factory accomplishes these objectives in a manner consistent with these critical priorities and requirements. This highly secure, integrated network platform enables all these capabilities to be efficiently deployed as the need arises.

Securing Manufacturing Assets

The next step in developing a security design is to identify the assets at risk or being targeted. The Cisco approach is to identify the standard high-profile assets of potential value to an attacker or likely to have a significant impact on production operations in the event of an incident. The value typically associated with these assets is either direct (such as sensitive information) or indirect (such as resulting fear, media coverage of a theft, revenue loss from an outage). They include:

- **Endpoints:** The devices or systems terminating an IP communications path and handing the data to the application layer. Endpoints may be interactive or standalone devices (laptops, desktops, servers, etc.). Endpoints considered include all the devices in levels 0–3 (see Figure 2) and in the demilitarized zone (DMZ) that is created as part of the architecture for the Ethernet to the Factory solution (see below).
- **Applications and services:** The higher-level processes relying on and using data being communicated or stored. Typically, the application or service uses network communications (and consequently the network infrastructure) to communicate with other applications or services residing on another endpoint.
- **Data in transit:** Data that is traversing the network infrastructure and is in transit between endpoints. Typically, active IP communications may use any subprotocol (UDP, TCP, RTP, etc.) to communicate information between applications on the endpoints. Of primary concern for protection of data in transit are industrial protocols, such as CIP.
- **Stored data:** Information or data at rest in storage on an endpoint. The architecture designed to protect network access to endpoint systems should include protecting the stored data on those devices (e.g., Historian Server).
- **Infrastructure:** The network elements that make up the transport structure moving communications between endpoints (switches, routers, security appliances, etc.).

Protecting physical, non-network items such as material, products, resources, and people is also important to any overall security program. Protecting the networked assets noted above will help safeguard these items, but additional services may be needed to further defend physical assets. Capabilities such as physical security and location tracking are often important components of an overall security program. Many of these capabilities can be implemented using intelligent networking technologies, such as integrated physical and virtual security and wireless location-based services. It is also important to include the appropriate policies, procedures, and training to protect all vital assets in a manufacturing facility.

Threats to Manufacturing Networks

After identifying priorities, basic requirements, and assets that need to be protected, the next step is to identify specific threats and attack vectors. As industrial automation and control systems move to more common computing and networking platforms, and become connected to enterprise systems, business partners, and the Internet, they are increasingly exposed to the same types of threats as traditional IT networks. These security threats include:

- **Malicious code (malware):** The broad range of software designed to infiltrate or damage computing systems without user knowledge or consent. The most well-known forms of malware include:
 - *Viruses* manipulate legitimate users into bypassing authentication and access control mechanisms in order to execute malicious code. Virus attacks are often untargeted and can spread rapidly between vulnerable systems and users. They can damage systems and data, or decrease the availability of infected systems by consuming excessive processing power or network bandwidth.
 - A *worm* is a self-replicating program that uses the network to send copies of itself to other nodes without any involvement from a user. Worm infections are untargeted and often create availability problems for affected systems. They may also carry a malicious code to launch a distributed attack from all infected hosts.
 - The *Trojan horse* is a virus in which the malicious code is hidden behind a functionality desired by the end users. Trojan horse programs circumvent confidentiality or control objectives and can be used to gain remote access to systems, gather sensitive data, or damage systems and data.
- **Distributed denial of service (DDoS) attack:** A common type of attack used by network saboteurs. DDoS attacks have become notorious over the past few years by flooding the network resources (such as critical servers or routers) of several major retail websites, with the goal of consuming resources or obstructing communication to decrease the availability of critical systems. A similar attack can easily be mounted on a targeted control system, making it unusable for a critical period of time.
- **Eavesdropping attacks:** Used to violate the confidentiality of the communication by sniffing packets on the LAN or by intercepting wireless transmissions. Advanced eavesdropping attacks, also known as man-in-the-middle or path insertion attacks, are typically leveraged by an attacker as a follow-up to a network probe or protocol violation attack.
- **Collateral damage:** An unforeseen or unplanned side effect of techniques being used for the primary attack. An example is the impact that bulk scanning or probing traffic may have on link and bandwidth availability. Manufacturing control systems are especially sensitive to network latency and dropped packets. If a network is not properly configured, unintended traffic such as large downloads, streaming video, or penetration tests can consume excessive bandwidth and result in slowed performance and unacceptable levels of network jitter.
- **Unauthorized access attacks:** Attempts to access assets that the attacker is not privileged or authorized to use. This implies that the attacker has some form of limited or unlimited control over the asset.

- **Unauthorized use of assets, resources, or information:** Use of an asset, service, or data by someone authorized to use that particular asset, but not in the manner attempted.
- **Reconnaissance attacks:** Probing that enables the first stage of the attack lifecycle. This serves to provide a more focused attack cycle and improve the attacker's chances for success.

It's also important to understand where threats are coming from (threat vectors) when developing a security approach. As noted, security data related to industrial automation systems is limited, but you can see some consistent trends if you look at the data that does exist and traditional IT security issues.

According to the BCIT, the primary sources of attacks against control systems are the corporate WAN and business network, the Internet³, and trusted third-party connections (including guest laptops). While internal threats are still significant and one of the top areas of concern for production managers, the data suggests that the threats increasingly originate from external sources. Prior to 2001, by contrast, the majority of attacks originated from internal sources. This mirrors the trend in traditional IT systems, where the threats have increasingly originated externally.

Internal threats can come from a number of sources, including attacks by disgruntled employees and contractors. Current or former employees and contractors often have detailed knowledge of target systems and can cause considerable damage. The IDC Security Survey of 2004 indicated that 31 percent of responding companies across multiple industries had terminated employees or contractors for violating their security policies. Therefore, it is important that security solutions and policies protect against potential insider attacks

An internal threat can also be a device accessing the network without the latest protection and unknowingly spreading a virus or attack. In addition to targeted threats, user error and unintentional incidents pose a significant risk and cause failure in manufacturing environments. A local or remote user might access the wrong systems and make changes, IT personnel can perform a network penetration test that degrades performance or renders systems inoperable, or a user may download or send large files over the network and impair control traffic performance. All these scenarios drive the need for comprehensive, multilayer security solutions and policies and should be considered when developing the system architecture.

External threats to information and automation systems are many and varied. They include accidental infection by a guest laptop; attacks by hackers seeking a thrill, fame, or money; corporate espionage; and even intrusion by terrorist organizations and foreign governments. Hackers use many of the techniques noted above and are an increasing source of threats to manufacturing systems. Today's hackers generally focus less on making trouble and more on making a profit, with groups looking for opportunities for extortion or theft that provide a quick payoff. Probably as a result, the number of attacks targeting specific organizations increased exponentially from 2005 to 2006. Such targeted intrusions are increasingly difficult to detect, which is a key reason for requiring complete visibility across the infrastructure. The faster a threat can be recognized, the more quickly it can be dealt with. Preventing the *behavior* of the attacks and intrusions once the hacker is inside is the key to security.

³ Studies indicate that 80 percent of companies report employees abusing Internet privileges. Providing direct access to the Internet from manufacturing systems can significantly increase risks due to malicious code downloads, or may affect network performance due to the downloading of large files, videos, etc.

Hackers are developing new ways of penetrating a network every day, and their increasing sophistication has made it virtually impossible to prevent damage by traditional means. Numerous examples exist of means of attack that combine software vulnerability with human psychology. For example, a hacker may infect several USB keys with a Trojan horse designed to attack an internal system, setting them out in a parking lot in the hopes that an insider will use one and trigger the collection of a ransom. Cisco has identified this and hundreds of other innovative techniques that hackers use to bypass traditional security controls.

Software vendors regularly release patches to correct the vulnerabilities that hackers and viruses exploit. But a patch, by definition, is a response to an identified problem, not a proactive fix. Most patches are released three to six months after a vendor has identified a vulnerability, but large-scale outbreaks may occur just hours or days following a vendor announcement and continue causing incalculable damage until the patch is widely deployed. For example, in 2005 Microsoft identified and announced vulnerability in its Universal Plug and Play service and issued a patch. Within seven days, before most companies could validate and deploy the patch, the Zotob worm struck, bringing down production for several manufacturers, including a number of large automakers and industrial equipment manufacturing plants⁴.

Further complicating these issues are the difficulties in deploying patches and effectively implementing and maintaining antivirus protection on many systems in a production control network. Patches typically need to be carefully qualified, sometimes by the automation vendor, and deployed during scheduled downtime. This increases the period of exposure to vulnerabilities and makes patch management a significant challenge for many manufacturers.

There are many other back doors and potential weak links in manufacturing networks, including incorrectly configured devices, undocumented connections, wireless networks without proper security configurations, and open ports on the manufacturing floor. These weak links are vulnerable to a variety of threats and must be addressed as a part of any manufacturing security architecture.

The Impact of Security Incidents in Manufacturing Environments

Once the requirements, priorities, and threats have been identified, it is important to estimate the impact of a security incident to establish the relative importance of protecting against various attacks. The implications of security incidents are often severe in production environments, as attacks may interrupt production and result in costly downtime and process startup time. According to a recent MetaGroup study, manufacturers earn an average of US\$1.6 million per hour in revenue; so any downtime or overtime required to fill production quotas clearly has significant financial impact. A study done by Infonetics in 2005 indicates that the manufacturing industry sustains the highest cost in terms of system downtime (calculated by revenue loss and productivity impact of both outages and degradations of service), estimated at \$201,000 per hour for North American manufacturing enterprises.

Security incidents can also result in the loss of critical data. Due to increasingly regulated production requirements, data from the manufacturing process usually needs to be gathered, stored, and integrated with business applications to maintain a detailed and accessible history of the production cycle. A related cost impact is the loss of proprietary information related to the production process, and contained in the industrial automation systems and associated applications.

⁴ *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, National Institute of Standards and Technology, special publication (SP) 800-82.

Attacks can have safety and environmental impacts, as well, caused by system availability concerns or deliberate attacks meant to sabotage systems. A well-known example is the Maroochy Shire sewage spill in Queensland, Australia. In March and April 2000, a disgruntled employee remotely hacked into the controls of a sewage treatment plant and caused malfunctions that ultimately resulted in 264,000 gallons of raw sewage being dumped into nearby rivers.

Any one of these incidents may not only have a large, direct financial impact, but also can result in noncompliance penalties, a loss of customer satisfaction, and a decline in corporate image and public confidence. According to ISID estimates, half the incidents in which a financial impact was reported cost the manufacturer more than \$1 million.

Given the potentially significant impact of security incidents in manufacturing environments, a strong, adaptable security approach is highly recommended. Cisco designed the architecture of its Ethernet to the Factory solution to address the significant implications of system failure and to minimize the risk of incidents while still meeting business objectives. With effective security solutions and procedures in place, many of the security incidents and associated losses described above are, in fact, preventable.

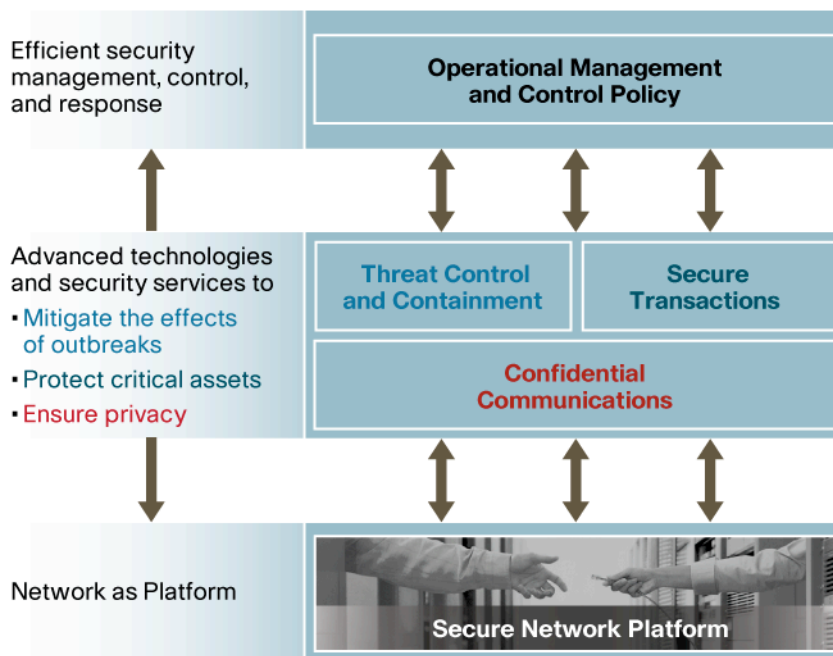
Identify the Specific Security Services and Capabilities Required

The next step is to identify the security services required to protect your assets while supporting your overall security objectives and priorities. The architecture for the Cisco Ethernet to the Factory solution is designed with the appropriate security services, given the assets to protect, threats to mitigate, and implications of failure. In order to deal with network-borne attacks on assets, a combination of techniques and technologies must be used. The first step is to identify the broad categories of defensive behavior. These include:

- **Prevention:** Preventive technologies are used to proactively reduce the probability of an attack that is known to be possible and/or likely to happen. Prevention is typically accomplished using preprovisioning or preconfiguration.
- **Detection:** Detection technologies discover the presence or existence of an active attack or violation of policy being executed.
- **Mitigation:** Mitigation technologies invoke the actions needed to render the effects of an attack less severe.

Prevention is the first step to network security. Proper planning, asset identification, threat assessment, and security design should allow the corresponding measured deployment of preventive technologies or features to address anticipated attacks. While prevention can reduce the probability of an attack progressing through its lifecycle, it cannot be 100 percent effective. As a result, any security architecture should also incorporate detection and mitigation mechanisms. This is particularly true in addressing unknown or unexpected attacks.

The Cisco Self-Defending Network is a strategic systems approach that uses the underlying network foundation to prevent, detect, and mitigate threats from internal and external sources. Rather than relying on add-on point solutions, the Self-Defending Network framework integrates security directly into all aspects of the network, creates and protects collaboration between the various security and network components, and evolves intelligently to disarm new threats as they arise, adapting to the changing nature of threats. The Cisco Ethernet to the Factory solution incorporates the appropriate elements from the Self-Defending Network framework and applies them to achieve the objectives and requirements of both manufacturing automation and control networks, as well as traditional IT networks.

Figure 1. The Cisco Self-Defending Network Framework

The three components of the Cisco Self-Defending Network that are most critical to securing factory networks are:

- **Secure network platform:** The secure network platform provides a scalable, flexible base from which to build the Self-Defending Network. Security does not reside in multiple point solutions; rather, it is integrated into the very fabric of the network. Its building blocks include Cisco adaptive security appliances, Cisco Catalyst[®] switching products, and Cisco integrated services routers. Based on this foundation, the self-defending network enables efficient management, a fully integrated platform, and ongoing deployment of advanced integrated security capabilities.
- **Threat control and containment:** Threat control and containment go beyond defending against threats to proactively and collaboratively control and contain them. Key components of this advanced technology include host- and network-based intrusion prevention and detection systems, network-based antivirus, and DDoS attack mitigation. These functionalities are built on top of the secure network platform and provide an integrated, multilayer security architecture that can be managed more effectively and efficiently than multiple-point solutions.
- **Operational management and policy control:** It is especially important to have the proper tools to monitor, analyze, and respond to changing security conditions. A set of integrated adaptive security management tools provides this capability, giving you an efficient means of managing and configuring network security to adjust to changing policies, network configurations, and security threats.

These elements enable the efficient identification, prevention, and mitigation of threats in a manufacturing environment.

An Integrated Security Architecture for Manufacturing

To achieve the three fundamental aspects of the self-defending network, the integrated architecture for the Cisco Ethernet to the Factory solution is designed specifically for industrial environments and lab-tested to offer proven capability. Manufacturing environments differ so much that it is vital to select a security strategy that can adapt to meet unique performance and technology requirements. Unlike the many multibox security solutions on the market today, Cisco's solution offers mature, proven, cost-effective security that unites multiple layers of functionality into a powerful and robust whole.

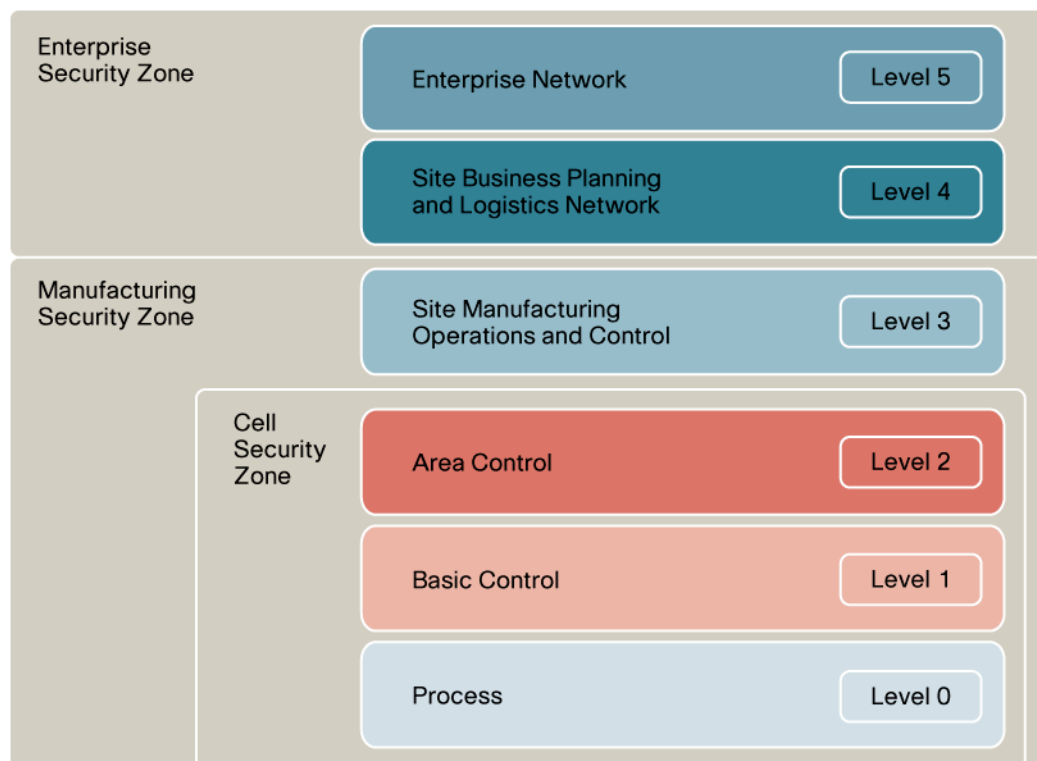
The Cisco ETTF solution is aligned with emerging guidelines and standards such as ISA-SP99 and NIST SP 800-82, which advocate multiple zones and multiple layers of defense to ensure system and data integrity and availability. Its security framework is based on the well-known Purdue Model referenced in standards such as ISA-SP99, S95, and NIST SP 800-82.

Like most existing and emerging standards for manufacturing security, the Cisco Ethernet to the Factory solution specifies separate protective zones for manufacturing systems and for the rest of the enterprise. A *zone* is defined as an aggregation of resources with similar access requirements, potential vulnerabilities, change management processes, and provision for the same consequences of security incidents. The concept of well-defined zones is especially important to help ensure that appropriate policies and capabilities are applied and security and performance requirements met in these two very different areas. The architecture is based on the principle that security must not compromise operations of the manufacturing control zone or the performance required by control I/O and real-time traffic. Zones typically encompass compatible content and frequent, clearly defined communication patterns.

There are three zones in the factory model used in ISA-SP99. The two primary zones are the enterprise zone and the manufacturing zone. The cell, or area, zone is considered a subzone within the manufacturing zone

- The *enterprise zone* comprises the site (plant) and enterprise IT environments, and includes corporate data centers, general access LANs and WANs, e-mail systems, and business applications.
- The *manufacturing zone* consists of the different cells within a specific site and the application, systems, and services required for ongoing manufacturing operations.
- The *cell/area zone*, a subzone within the manufacturing zone, typically consists of systems that need to interoperate and communicate on a frequent or real-time basis. A cell/area zone may consist of multiple programmable automation controllers (PAC), robotic devices, and the human-machine interfaces (HMI; either standalone or distributed) associated with related or interdependent steps in the manufacturing process.

Each of the two primary zones has security requirements that are quite different from each other.

Figure 2. Six-Level Plant Framework Based on ISA-SP99

In the manufacturing zone, the key priorities are availability of manufacturing control systems and applications, followed by integrity of data and confidentiality. (The cell/area zone has policies, priorities, and considerations similar to those of the overall manufacturing zone.) Systems in the manufacturing zone often require very low levels of latency and jitter across the network to achieve very high levels of reliability. At the same time, the challenges associated with patch management, the inherent technology limitations of the devices, and the skill sets of the individuals responsible for maintaining these systems all affect the types of tools that can be implemented in this zone. The fundamental requirement is that security should not impair the performance of manufacturing systems.

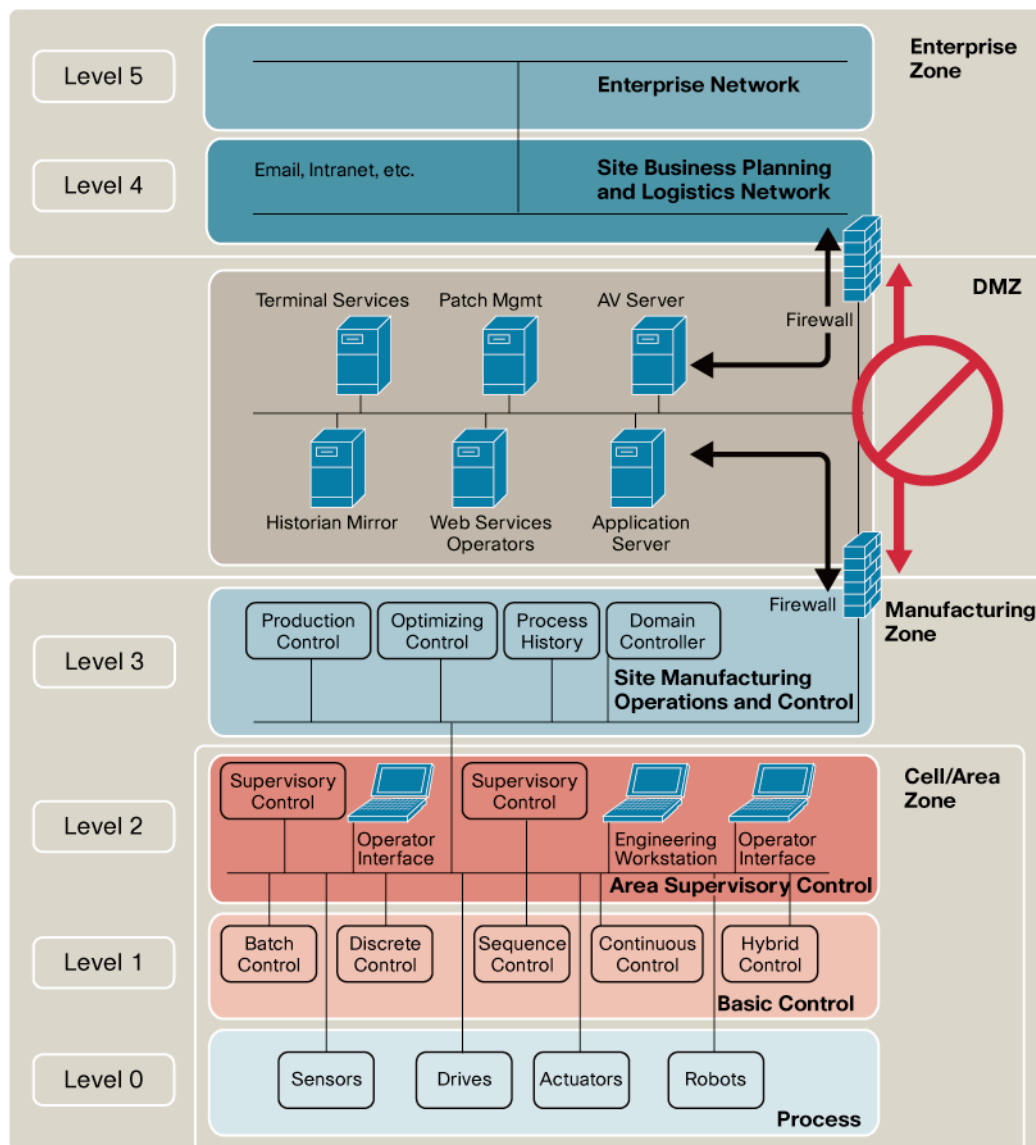
Therefore, some of the key security components in this zone include VLANs to limit access of individuals and traffic to specific devices and ports. Different cells in Levels 0-2 (see Figure 2) can be grouped into different VLANs and then integrated at Level 3 in the manufacturing zone to enable communication between cells. Access control lists (ACLs) prevent unauthorized users and traffic types from gaining access, while port security prevents users from plugging in unauthorized devices. Solutions to protect vulnerable endpoints and help mitigate patching issues are also important here, as are management and monitoring. For network devices maintained by production personnel, these features need to be combined with easy-to-use network device functionality to ensure consistent and effective deployment.

Maintaining proper policies is important in the manufacturing zone, to help ensure that zone-allowed systems conform to security policies and have not been accidentally or deliberately infected, potentially compromising the zone. Important best practices include implementing programs to check guest laptops or provide validated loaners while on site, disconnecting modems on automation systems that can create a vulnerable back door, and designing systems to help ensure that critical services are highly available. Limiting access to the manufacturing zone is especially important and will typically consist of only a small group, not the overall plant IT environment.

In the enterprise zone (as in the manufacturing zone), the same solutions and management tools are used to establish a strong security architecture, but different priorities and policies apply with regard to authorized access, number of users allowed, and traffic types. Applications and data related to batch recipes, product configurations, and enterprise-wide business reside in this zone, so protecting the confidentiality and integrity of information takes priority over availability of systems. Additional capabilities to provide guest access and more stringent network admission control can be deployed to help secure the overall network.

Given that the enterprise zone and the manufacturing zone have different requirements, priorities, policies, and implications of incidents, and that it's desirable that they be able to share data and access systems and applications, the solution introduces a fourth zone into the Ethernet to the Factory architecture to provide insulation. This is the demilitarized zone. Systems and data that need to be accessed by both manufacturing and enterprise business systems reside in the DMZ, protecting information and accommodating the different security requirements of these major zones. As a best practice, all traffic should terminate in the DMZ, eliminating direct traffic flow between the enterprise zone and the manufacturing zone.

Figure 3. Six Level Plant Framework with DMZ



The DMZ can also host patch management servers, proxy servers, and terminal services, enabling highly secure access to and from the zones and the Internet while accommodating the potentially unique patching policies of the manufacturing zone. This architecture enables highly secure remote access to production control systems, which allows remote employees and contractors to view and control the manufacturing systems they are authorized to access without directly connecting to the enterprise zone. It is important for remote access to connect only through the DMZ to maintain the appropriate levels of security.

Strict policies in the DMZ help to prevent cross-layer communication and infection, and include signature identification and intrusion protection through the deployment of intrusion prevention systems (IPS) to inspect and secure traffic coming from the enterprise and external networks. The DMZ can be split into functional subzones, divided by a firewall and an IPS (logically partitioned) to limit access to authorized individuals and traffic types.

Some manufacturers may be concerned about additional complexity with a DMZ. Given the critical nature and vulnerabilities of production control systems, however, a DMZ is an important part of the overall security architecture. The DMZ can be deployed using paired firewalls or a “three-legged firewall,” depending on the requirements of the specific environment, and it provides a significant increase in security for industrial automation systems without a significant increase in complexity over a traditional security configuration. The DMZ provides a highly important buffer between the manufacturing and enterprise zones, permitting highly secure shared access to data and systems.

Cisco Features Supporting the Factory Architecture

The specific security components of the Cisco Self-Defending Network framework implemented in the Ethernet to the Factory solution include:

- **Adaptive security appliances:** The use of Cisco adaptive security appliances (ASA), either as standalone appliances or integrated with Cisco switching and routing platforms, provides a key component of a perimeter defense, including defining and protecting the DMZ. The firewall can perform stateful inspection and can incorporate advanced functionality, such as intrusion detection and prevention and VPN capabilities. Implementing a strong perimeter defense with adaptive and multifunctional firewalls is an important step to achieving prevention objectives. Additionally, the ASA will perform application and protocol inspection to help ensure proper protocol behavior.
- **Secure infrastructure:** A secure network platform supports the consistent use of integrated security features important to both the manufacturing zone and the enterprise zone, such as VLANs, ACLs, port security features, and network foundation protection features.
- **Behavior-based intelligence to detect and mitigate attacks, and assist with patch management:** Deploying patches and antivirus applications in a manufacturing environment presents special challenges, as they may disrupt production, degrade processor performance, or otherwise affect time-sensitive applications or processes. The answer is behavior-based security that does not require signatures, providing day-zero protection to critical systems without continuous updates. Cisco Security Agent is a behavior-based software agent that can be used to protect endpoints and secure either applications that are based on standard operating systems or hardening servers located in the DMZ, making it a critical component of the Ethernet to the Factory solution.
- **Integrated security for converged wired and wireless networks:** The use of integrated wired/wireless networks is increasingly significant in manufacturing and provides much-needed productivity gains. If wireless networks are not properly secured, however, they can become another source of threats to the industrial automation network. Integrating security into the Cisco converged network supports consistent safety functionalities and management.
- **Intrusion prevention systems:** Deployed between the enterprise and manufacturing networks, IPSs can detect and block attacks, including worms, viruses, and other malware, through inline intrusion prevention, innovative technology, and identification of malicious network activity. This stops threats before they reach industrial automation and control systems, helping to ensure availability and integrity of manufacturing data and equipment.

- **Monitoring, analysis, and response:** With multiple layers of security in place, it is important for manufacturers to be able to take advantage of an integrated view and analysis of the status and performance of security tools, as it helps to ensure optimal protection and faster response. Cisco Security MARS provides security monitoring for network security devices and host applications made by Cisco and other providers. Cisco Security MARS monitors various systems and devices, correlates events, and uses this information to identify and respond to security threats.
- **Security Management:** The Cisco Security Management suite consists of a framework of products and technologies designed for policy administration and enforcement. This integrated capability provides functions that simplify and automate the tasks associated with security management operations, including configuration, monitoring, analysis, and mitigation.

These capabilities are built on a secure network platform that provides a scalable foundation to efficiently deploy additional security solutions over time. For example, network-based physical security designs allow the integration of multiple video surveillance systems onto a single converged network. If you integrate physical and network security services, an intruder who does not properly access the plant by scanning a valid ID badge, for instance, will not be able to access the network. In another example, Cisco Network Admission Control can be set up to recognize multiple, non-PC type devices, supporting properly secured guest network access in a manufacturing plant.

The combination of these powerful security features provides the multiple layers of defense needed to protect against the many different threats and attack vectors that can affect a manufacturing network. Founded on a secured network foundation, these capabilities are integrated, adaptable, and scalable to meet changing business needs, and can be consistently and efficiently monitored. The low-impact, manageable Cisco ETTF solution helps manufacturers optimize their investment to efficiently achieve reliable, effective security.

Managing the Security Lifecycle: The Importance of Policies and Procedures

Security policies and procedures are a key element of achieving a secure manufacturing environment. Even the most powerful network security tools and technologies can be misused or incorrectly configured for their circumstances. Incorrect network configuration is, in fact, one of the chief causes of performance degradation. Establishing and following a precise set of security policies throughout the network, with procedures that allow for constantly evolving security threats, will help to minimize incidents and maintain the integrity of the industrial environment. Well-designed policies and procedures also help to reduce operating costs by getting the best performance out of the security implementation.

Manufacturers have traditionally maintained different priorities and technologies for security, as their control systems were markedly dissimilar from those of enterprise IT networks. But as technologies increasingly converge, many manufacturers find they lack the experience to plan, implement, and manage complete, cross-functional security solutions. Security for control systems is often the responsibility of manufacturing controls engineers, yet a recent ARC Research survey found that 79 percent of manufacturing organizations have no training program for control systems security.

To assist manufacturers, the Ethernet to the Factory solution is supported by Cisco's advanced services consulting team. This group of manufacturing industry experts provides practical experience, knowledge of the latest network technology, and proven tools and methodology to help plan, design, and implement network security by:

- Mitigating security threats to networks, systems, and information
- Deploying powerful security policy and procedures
- Setting up ongoing management and maintenance
- Shortening implementation time

The proper policies, procedures, and training are critical parts of any effective security program. By educating users and operators about the types of risks, threats, policies, and tools, manufacturers help ensure that the proper implementation and use of their security program. This also ensures that the security program aligns with and helps the enterprise to achieve overall business objectives. This training should become a continual process, informing all personnel of the latest policies and procedures, and keeping them aware of evolving security risks and capabilities. The overall security program should also include policies to regularly reassess threats, vulnerabilities, assets, business objectives, and available technologies.

Laying the Foundation for Manufacturing Security with Cisco

By definition, IT security is a continuously evolving process, one that must adapt as risks and technology capabilities change. According to a 2007 ARC survey, less than half of all manufacturers, only 41 percent, feel that their systems are more secure than five years ago. This, even with the greatly increased industry focus on security in recent years. To remain competitive today, it's becoming imperative to integrate manufacturing and enterprise data throughout the supply chain. Yet many manufacturers cannot keep up with the changing nature and frequency of internal and external threats. Point solutions are helpful, but they don't provide the intelligent, ongoing security that manufacturers need.

The Cisco Ethernet to the Factory solution provides a multilayered architecture that uses tried and tested security capabilities, and is designed specifically to protect critical industrial operations and information in factory environments. Cisco best practices help manufacturers to implement and maintain a powerful networking foundation that unites business and industrial automation systems while protecting them from today's ever-proliferating security threats.

Deploying integrated, adaptable security functionalities that evolve over time is the only answer to ensuring complete availability, integrity, and confidentiality of manufacturing systems. The Cisco Ethernet to the Factory solution provides investment protection through a scalable network foundation that remains robust, flexible, and manageable through business change and expansion. Based on the Cisco Self-Defending Network, it enables manufacturers to continually take advantage of advanced security technologies, helping to secure their organization's value chain today and into the future.

**Americas Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912

www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands

www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)