Summary
This document provides an understanding of the security challenges faced by manufacturers in the plant networks and at a high level discusses various ways of protecting them.

Author: Deepak Rai Sharma
Company: SAP Labs India Pvt. Ltd.
Created on: 02 November 2009

Author Bio
Deepak Rai Sharma is Solution Manager - Manufacturing at SAP Labs, Bangalore. He has experience in design, development and product management for ERP and Manufacturing applications. He specializes in various logistics and manufacturing modules of SAP ERP and an expert in SAP MII. His current focus is on Enterprise Service Enablement and Adoption of SAP Manufacturing processes and next generation Manufacturing Connectivity and Intelligence initiatives.
# Table of Contents

Executive Summary ................................................................................................................. 3

Security Challenges for Plant Networks .................................................................................. 3

Understanding the Plant Networks ........................................................................................ 3

Ways to Protect Plant Systems ............................................................................................... 4
  - Network Topology ........................................................................................................... 5
  - Transport Layer Security ................................................................................................. 7
  - Secure Software Programming ......................................................................................... 8

Conclusion .............................................................................................................................. 8

Related Content ....................................................................................................................... 9

Copyright ................................................................................................................................. 10
Executive Summary

Cyber security means confidentiality, integrity and availability of computers, applications and digital-based data and process systems. Traditionally, the Plant systems have been working in disjunction with the local MRP and other centralized business applications. With the growing demand of Lean Operations and demand driven supply chains, as well as business intelligence reaching the plants through Enterprise Manufacturing Intelligence (EMI) applications, the need for integrated functioning of both Business systems and Plant Systems has become more important than ever. However, these enterprise integration strategies coupled with the increased exposure of company LAN/WAN infrastructures to Internet attacks, can put plant automation and production management systems vulnerable to cyber attacks. How do manufacturers deal with this problem?

Through a combination of advanced infrastructure, progressive software, and pervasive policies, companies can protect their plant infrastructure as well as their corporate financial and strategy systems. This document provides an understanding of the security challenges faced in plant networks and at a high level discusses various ways of protecting them.

Security Challenges for Plant Networks

Plant Systems are designed for performance and reliability. In the past, Plant Systems have been working as silos without much interaction with high level business systems. But now, with increased emphasis on operational excellence, it has become very important that the global planning systems work closely with the plant operational applications. This means the plant systems need to expose data and functionality to business systems and vice-versa.

With today’s interconnected architectures, company WANs are potentially vulnerable to attack. Attacks could be the result of cyber criminals, corporate espionage, or even potential terrorists. The evolution of plant automation and infrastructure has made the plant floor another hub on the corporate WAN. Enterprise Integration Strategies without due consideration of security could leave plant systems vulnerable to attack. There are several risks associated with IT threats to industrial control systems. The most consequential risks are those associated with the health and safety of human lives. Cyber attacks on energy production and distribution systems including electric, oil, and gas, water treatment and distribution systems as well as on chemical plants containing potentially hazardous substances could endanger public health and safety as well as invoke serious damage to the environment. Attacks on any industry could result in serious financial implications including loss of production, generation or distribution of a product, compromising of proprietary information, loss of intellectual property around plant processes and recipes, loss of information that could compromise competitiveness, and creation of liability issues.

Understanding the Plant Networks

The control systems used in Plant Applications are designed quite differently to transactional business systems. The Plant control systems need to have high-availability and sub-second response time for any requests or events. The Plant Networks are generally on a separate network segment, with the control system landscape separated via switches and/or firewalls from the corporate IT landscape. As shown in Fig.1, the key basic building blocks of the Plant Systems consist of controlling computers [often Programmable Logic Controllers (PLC) and Distributed Control Systems (DCS)], standalone controllers for simple process loops, Human-machine Interface (HMI) and Supervisory Control and Data Acquisition (SCADA) systems, Data Collectors such as Data Historians, and Remote diagnostics and maintenance utilities. The business applications access the plant systems via the LAN or WAN. The plant has an internal LAN which processes all operations. This LAN would provide access to various databases, Application Servers and other Workstations. Generally there is one central business LAN but there can be multiple plant networks. The plant networks are generally isolated in some fashion from the business LAN at the site.
Ways to Protect Plant Systems

Addressing cyber security between plant production and business systems is a complex task, made more difficult because of the differences between plant automation systems and typical business applications. Corporate IT may not be familiar with complex industrial systems and any errors can adversely affect production. From the perspective of industrial automation, rather than be challenged with IT security, some automation systems are run autonomously, leaving a communication gap between the business applications and the plant systems. Vulnerabilities are dependent on the existing network architectures, IT policies and risks associated with a particular industrial process control system. The major aspects where the security concerns need to be addressed are providing a secure network architecture, designing pervasive corporate and plant policies, and providing a framework for secure software programming.

SAP MII (Manufacturing Integration and Intelligence) is an application framework which is deployed at the plant site to provide integration between the manufacturing/process systems and the business systems. MII is used to build composite applications using the information available from both business and plant systems. Appropriate deployment architecture, after taking into consideration the security threats mentioned above, is the key to a successful and secure implementation.
Network Topology

Your network infrastructure must be designed keeping security in mind, and should be closely monitored for any threat. A well-defined network topology can eliminate many security threats based on software flaws (at both the operating system and application level) or network attacks such as eavesdropping. If users cannot log on to application or database servers at the operating system or database layer, then it is more difficult for intruders to compromise the machines and gain access to the SAP System database or files. Additionally, if users are not able to connect to the server LAN, they cannot exploit well-known bugs and security holes in network services on the server machines. The network can be made very secure and robust by using already available technologies, such as Firewalls, VPN and Segmenting the LAN into several IP Subnets.

All external access to the plant systems should be authorized through a firewall which allows communications only for designated services. A firewall can be setup between the intranet and Internet so that only designated services can pass through it, blocking all non-authorized protocols. A firewall will also allow communication only via designated ports, blocking all others. Firewalls at multiple levels in plant network can drastically reduce the vulnerability of the plant systems. Firewalls are typically one of two types. The first is a setup to filter packets on the router itself based on type of service request. For example, this implementation of a firewall could route the http and ftp service request packets to the http and ftp proxies but block any unwanted protocols, such as telnet service requests. The second type of firewall is at the application level which can filter the packets based on the content. The application level gateways provide a wide range of filter criteria like content, user authentication, source network zone, source address etc. SAProuter and SAP Web Dispatcher are the application level gateways that filter network traffic.

There are several possibilities to consider when organizing your network topology. The topology can vary from a single LAN segment to multiple IP subnets. It is recommended that you install your application server and central database server on separate machines and place them in an access controlled subnet as indicated in the graphic below. It should be noted that not all systems have the same level of security requirements. These security requirements should be analyzed and grouped into several subnets based on the requirements of the solutions being implemented.
The topology described in the figure below is recommended as a starting point for designing your specific solution. The firewalls protect the network from undesired access from persons or resources outside of the designated area. The application gateway or proxy server in the DMZ makes sure that requests are not directly passed through to the desired resource, but are handled by the gateway or proxy server's own cache. Not only does this buffer zone reduce network load, it also allows you to filter requests from the external to internal networks through the multiple firewalls. Application servers, database servers, and the user management systems have increased protection and are only accessible by authorized users or resources. In this way, you can provide for optimal protection.


**Transport Layer Security**

SAP MII provides transport layer security features like support for the internet standard protocol secure socket layer (SSL, also known as HTTPS) for runtime and design time secure communications. MII also supports the SAP proprietary interface called Secure Network Communication (SNC) for SAP Protocols. Either of these can be used based on the underlying protocols. For example SSL is used to secure Internet protocols like HTTP, LDAP etc. SNC is used for SAP Protocols like Dialog and RFC. Both these transport layer security mechanism provide protection for Authentication, Data Integrity and Data Privacy.

Another secure data transfer option between two networks is Tunneling or Virtual Private Network (VPN). This can be utilized when the plant data is needed to be made available outside the plant network, especially if data and analytics need to be shared with customers and suppliers through an extranet. A VPN provides secure access to the plant network from outside. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols. Secure tunneling can be done using a SAP Router in conjunction with SNC. Tunneling technology can also make use of port restriction, user authentication, and data-stream encryption to overcome a variety of security issues.
Secure Software Programming

However, even if the network protocols and topologies are taken care of, the plant systems could still be vulnerable in absence of secure software programming. Many aspects like authorizations, cryptography, usage of user and system logon credentials, and abstraction of actual data help in making the plant data secure.

In SAP MII, all the plant systems that need to be integrated are maintained as a data server, which is an alias for a set of connection data, and works as an abstraction layer providing secured access to the data from the application. All credentials, such as the technical user credentials required for data access, are encrypted in a credential store with the highest encryption security available on the MII server.

Users and roles for SAP MII are all stored and managed by the SAP NetWeaver User Management Engine (UME). For more information on UME, see http://help.sap.com/saphelp_nw04s/helpdata/en/5b/5d2706ebc04e4d98036f2e1dcfd47d/frameset.htm

The Virtual Server feature available in SAP MII can be used for secure and firewall-friendly communication in a multi-node environment. In SAP MII, "virtual servers" are used for peer to peer communication between MII nodes. This allows one MII node to access data, with proper authentication and authorization, to access data via another SAP MII server. This is helpful in environment where communication between several plants or between plant and corporate is required. The advantages of using virtual servers is that the data is sent in binary format, making WAN communication efficient, and the data is sent on the HTTP/HTTPS port, so no firewall exceptions need to be implemented. The MII to MII communication using virtual server is secured as there is no direct access to the data source, and data transfer between the MII servers can be encrypted via SSL.

All security relevant changes in SAP MII are logged using a separate category in the standard SAP User Management Engine (UME) logging file. Security permissions for data servers and services are written to the security log with the MII Security category. The data includes the previous value and the value to which the security permission was changed. Security permissions for MII content objects are also written to the same log.

In addition to securing the network and software programs, pervasive corporate and plant policy management is also required to orchestrate access to complicated and disparate plant landscapes. Well defined policies help in answering questions such as which systems and information are allowed to be accessed from outside the plant network and how; Should it be allowed to only read the data or even write back; How are the changes in the IT landscape effect the control systems etc.

Conclusion

While manufacturers have long realized that plant floor information is business imperative for successfully implementing lean supply chain concepts, the technology and applications to make this simpler to implement and govern are now available. But an organization must be careful when exposing plant systems to networks outside the local environment. Exposing plant systems without taking due security measures could jeopardize the functioning of process control systems, causing both physical and financial damages. But this doesn't mean that plant networks should be completely cut off from any external integration. Close scrutiny of plant networks, leading to segregation of plant systems into several subnets based on security requirements along with appropriate usage of technology can make this a manageable process without overly driving up the total cost of ownership. Firewalls, VPN tunneling and technologies provided by SAP such as SAProuter, SAP Web Dispatcher, SSL and SNC reduce the vulnerability of plant systems drastically. SAP MII, which works on the high security SAP Netweaver platform, leverages many security standards and methodologies to provide safe access to plant information. Secure Programming, Identity Management and appropriate corporate and plant policies can also further help strengthen cyber security within your corporate landscape. And of course, SAP consulting is happy to provide expert analysis and implementation advice for your particular needs.
Related Content
For more information, visit the Manufacturing homepage.
For more information, visit the Business Process Expert homepage.