SIEMENS

SIMATIC

Security concept PCS 7 and WinCC - Basic document

Whitepaper

04/2008
A5E02128732-01

Safety instructions

This manual contains instructions intended to ensure personal safety, as well as to protect equipment against damage. Instructions relating to your personal safety are indicated by a warning triangle, which does not appear with instructions solely relating to material damage. Warning notices appear as shown below, in descending order of hazard priority.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

with a warning triangle indicates that minor personal injury may result if proper precautions are not taken.

CAUTION

without a warning triangle indicates that property damage may result if proper precautions are not taken.

NOTICE

indicates that an unwanted result or state may occur if the relevant instruction is not observed.

If several hazard levels are applicable, the warning notice corresponding to the highest level is always used. If a warning notice with a warning triangle relates to the risk of personal injury, a warning relating to material damage may also be added to that same warning notice.

Qualified Personnel

The equipment/system to which this documentation applies must always be set up and operated in accordance with this manual. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Qualified personnel, as used in the safety-related information in this documentation, is defined as persons who are authorized to commission, to ground, and to tag equipment, systems and circuits in accordance with established safety practices and standards.

Correct Usage

Note the following:

⚠ WARNING

The equipment may only be used for the applications described in the catalog and the technical description, and only in conjunction with equipment or components from other manufacturers which have been approved or recommended by Siemens. This product can only function correctly and safely if it is transported, stored, assembled, and installed correctly, and operated and maintained as recommended.

Trademarks

All product names marked with the ® copyright symbol are trademarks of Siemens AG. Other product names in this document may be trademarks and third parties using these names for their own purposes may infringe upon the rights of the trademark owners.

Disclaimer of Liability

We have checked the content of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. The information in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.

Siemens AG
Automation and Drives
P.O. Box 48 48
90327 NUREMBERG
GERMANY

Document order number: A5E02128732-01
℗ 04/2008

Contents

1 Preface

1.1 Validity

"Security Concept PCS 7 and WinCC" incrementally replaces prior documents and recommendations "Security Concept PCS 7" und "Security Concept WinCC", both in Version 1, and is valid as of WinCC V6.2 and PCS 7 V7.0 or later.

"Security Concept PCS 7 and WinCC" should be considered a set of recommendations and is intended to support SIMATIC customers in creating a secure network for production plants. The recommendations are based on the latest technology, current standards and the features of the employed products.

1.2 Structure and organization of the document

"Security Concept PCS 7 and WinCC" is a document collection of requirements and recommendations consisting of several parts:

- The basic document is a central guide and provides an overview of the document collection.

This document is the basic document. It describes the general principles of the security concept and potential approaches for solutions. The basic document should be considered a single entity. All additional detail documents assume the reader has read the basic document. The following list shows the structure of the basic document:

- Sections 1-4: Required information for understanding the security concept
- Section 5: Security strategies and their basic principles
- Section 6: Implementation of the security strategies for security solutions and references to specialized detail documents
- The detail documents explore specific solutions and their recommended configuration in detailed form, always focusing on a particular topic or product.

In the detail documents you can find detailed recommendations on important security topics, which should facilitate the implementation of the principles and solution approaches presented in the basic document.

These detail documents are supplemented, updated and published separately to ensure they are always up to date.

You can find information on the "Security Concept PCS 7 and WinCC" document collection in the Internet at the following address:http://support.automation.siemens.com/WW/view/de/28580051
http://support.automation.siemens.com/WW/view/en/28580051

1.3 Required knowledge

This document collection is aimed at anyone involved in configuring, commissioning and operating automated systems based on Siemens SIMATIC PCS 7 and SIMATIC WinCC.

The basic document can also be used as an overview for decision makers or as an introduction to the topic.

The following knowledge is required for the implementation of the detail documents:

- Management of IT typical in the office environment
- Configuration of the employed SIMATIC products
- Configuration of the employed products from third parties.

1.4 Employed products

The following products, product versions and add-ons are used in the solution approaches described in this document collection:

- "Microsoft® Windows Server 2003" (with SP1 or later) as the basic operating system for server functions such as: Process control stations (e.g. OS server), operator control and monitoring stations (e.g. WinCC server), Terminal Service, Active Directory domain controller, name services (e.g. DNS, WINS), network services (e.g. Virtual Private Networks, Routing and Remote Access, Radius, Firewall), infrastructure services (e.g. certification bodies, Windows Software Update Services), and Web services.
- "Microsoft® Windows XP" (with SP2 or later) as the basic operating system for client functions such as: Process control stations (e.g. OS client), operator control and monitoring stations (e.g. WinCC client), Terminal Service client, VPN client, Web client and firewall client.
- "Microsoft® Internet Security and Acceleration (MS ISA) Server 2006" as the main firewall system and access point to the production networks from office or intranet networks.
- "Siemens SIMATIC PCS 7 V7.0" (and later) as a special hardened process control system and "Siemens SIMATIC WinCC V6.2" (and later) as a special hardened process visualization system (operator control & monitoring system), both installed on the above-mentioned Microsoft® Windows Server 2003 or Microsoft® Windows XP operating systems.
- "Siemens SIMATIC Logon Service" in a Windows domain environment as a combination secure authentication, fail-safe centralized logon and centralized user and operator management or as logon server in Windows workgroups for combining centralized logon and centralized user and operator management.
- "SIMATIC PCS 7 OS Web Server und Client", "SIMATIC WinCC Webnavigator Server and Client" and "SIMATIC DataMonitor Server und Clients", each used as a dedicated Web server, offer secure publishing via the MS ISA server as access point.
- "SIMATIC SCALANCE S" and "SIMATIC SCALANCE X" product families as security modules and network peripherals for robust Industrial Ethernet with increased availability, especially suited for use in industrial environments.

Additional products, product versions and options may also be used, as explained in the individual detail reports.

The selection of the "Microsoft® Internet Security and Acceleration (MS ISA) Server 2006" as the main firewall system and access point for the production networks is in part based on the long-term, close and successful cooperation between Microsoft und Siemens in software development.

The Microsoft Corp. has also been positioned in the Gardner Inc. report, "Visionaries of the SSL VPN Magic Quadrant®". This report evaluates Microsoft's Internet Security and Acceleration Server (ISA Server) and the Microsoft developed Virtual Private Network, which is based on the Secure Sockets Layer Protocol (Microsoft: secure sockets layer virtual private network (SSL VPN))" server, both summarized in the "Intelligent Application Gateway (IAG)".

Microsoft's ISA Server offers a centralized and consolidated appliance for network perimeter defense, remote access, endpoint security and application-layer protection.

2 Aim of the security concept

The highest priority in automation is the unconditional maintenance of control over production and process by the operating personnel, even in the event of security threats. Preventing or limiting the spread of a security threat for plants and networks should occur while maintaining full operator control and monitoring of production and process.

The "Security Concept PCS 7 and WinCC" is intended to ensure that only authenticated users can perform authorized (permitted) operations through operating option assigned to them for authenticated devices. These operations should only be performed via defined and planned access routes to ensure safe production or coordination of a job without danger to humans, the environment, product, goods to be coordinated and the business of the enterprise.

The "Security Concept PCS 7 and WinCC" therefore recommends the use of the latest available security mechanisms. This means selecting all solutions and configurations so that the plant manager uses all currently available security mechanisms and technologies, as well as products from Siemens and third parties if they are required to achieve the highest possible security of his plant. Depending on the security needs of the plant manager, the responsibilities involved or existing implemented security mechanisms, the configurations presented here can be implemented and scaled as shown or in adapted form. However, this should be carefully planned in each individual case by all involved technicians, specialists, administrators and officers. To achieve the highest possible security, adapted configurations should never contradict the basic principles of this security concept.

This document collection is intended to facilitate the cooperation of network administrators of company networks (IT administrators) and automation networks (automation engineers), allowing the exploitation of the advantages provided by the networking of process control technology and the data processing of other production levels without increasing security risks at either end.

This document collection should be considered a set of recommendations and is intended to support SIMATIC customers in creating a secure network for production plants. The recommendations are based on the latest technology, current standards and the features of the employed products.

3 References

The following internationally recognized norms and standards are observed to ensure that this document collection is future-proof and includes third parties and their products in the security concept:

ISA - Instrumentation, Systems, and Automation Society

- ISA-95 "Enterprise – Control System Integration"
  - Part 1: "Models and Terminology"
  - Part 2: "Object Model Attributes"
  - Part 3: "Models of Manufacturing Operations Management "

- ISA-99 "Security Guidelines and User Resources for Industrial Automation and Control Systems"
  - Part 1: "Concepts, Terminology and Models"
  - Part 2: "Establishing an Industrial Automation and Control Systems Security Program"
  - Part 3: "Operating an Industrial Automation and Control System Security Program"
  - Part 4: "Specific Security Requirements for Industrial Automation and Control Systems"
  - TR-99.00.01-2004 "Security Technologies for Manufacturing and Control Systems"
  - TR-99.00.02-2004 "Integrating Electronic Security into the Manufacturing and Control Systems Environment"

ISO/IEC - International Organization for Standardization / International Engineering Consortium

- 15408 "Information Technology – Security-Techniques – Common Criteria for Information Technology Security Evaluation"
- 17799 "Code of practice for information security management"
- 27001 "Information security management systems – Requirements"
- 62443 "Security for Industrial Process Measurement and Control – Network and System"
- 61784-4 "Profile for Secure Data Communication in Industrial Networks"

NAMUR - International User Association of Automation Technology in Process Industries

- NA 67 "Information Protection for Process Control Systems (PCS)"
- NA 103 "Usage of Internet Technologies in Process Automation"
- NA 115 "IT-Security for Industrial Automation Systems:"

FDA - Food Drug Administration

- FDA 21 CFR 11 "Electronic Records; Electronic Signatures"

Additional future-proof measures are:

- Close consultation on the security needs of customers and plant managers (for example, through the PCS User Club or selected security-critical references plants and reference customers)
- Cooperation with independent institutions and organizations (for example, OPC Foundation, ISA, ISCI, ARC, OMAC, MsMUG, PCSF, PCSRF)
- Close interaction with other manufacturers and suppliers (Microsoft, for example).

4 Definitions

This section defines designations, terms and abbreviations as they are used in this document collection.

Some terms from previous documents require updating due to work in the field of standardization and the need to present SIMATIC customers this document collection with a uniform, internationally recognized terminology and set of concepts.

Most designations, terms and abbreviations are taken from internationally recognized standards (e.g. ISA-95, ISA-99) or the latest documentation of the respective manufactures (see source information).

4.1 Designations, terms and abbreviations

Plant, automation plant

A production or manufacturing system (including all distributed I/O, sensors, actuators, drives, network and software components, buildings, control cabinets, cabling, operating and administration personnel) consisting of networked process control, process visualization, automation and engineering systems

Plant PC, plant computer

A computer located in the plant manager's area of responsibility and managed there.

Plant administrator

A plant administrator is a user in a network who manages the plant PCs in the plant manager's area of responsibility. The plant administrator is not necessarily an operator.

User:

(ISA-99): "A person or part of an organization or automatic process accessing a system with or without access permission."

A real or virtual person who is logged on (for example, the user logged on to the desktop of the respective operating system or an automatic desktop logon).

Operator, plant operator

An operator (or plant operator) is a real person logged on to the automation plant. This person is trained and authorized to operate this plant (for example, the operator logged on in PCS 7).

Computer name

The computer name is one way of identifying a computer in the network. It corresponds to the host part of the FQDN (Fully Qualified Domain Name), if a DNS assignment has been made (DNS suffix assignment). The computer name may match the NetBIOS name of the computer, if the computer name does not exceed 15 characters and both names have not been intentionally selected to differ.

DCS, distributed control system

(ISA-99): "A type of control system in which the system elements are distributed but operated as coupled. In general, the time constants of the coupling are substantially less than those for SCADA systems.
Note:
Distributed process control systems are usually used in the context of continuous processes, such as the generation of electrical energy, refining of oil and gas, production of chemicals or pharmaceuticals and manufacture of paper; they are also used in discrete processes such as manufacturing, packaging and warehousing of automobiles and other goods."

Domain

(ISA-99): "Environment or context which is defined by a security policy, security model or security architecture and includes a group of system resources as well as the corresponding group of system entities that have permission to access these resources."

(Windows): Logical group of computers on which a version of the Microsoft Windows operating system is run and which uses a central, common directory database (referred to as Active Directory as of Windows 2000). The Active Directory contains the user accounts and security information for the resources in this domain. Each person who uses the computers within a domain is assigned a unique user account or unique user name. This account can be assigned access permissions to resources within the domain.

(Windows): A model for managing local Windows networks, corresponds to a local security zone with centralized management of resources and represents an administrative border.

Domain controller (DC)

(Windows): A domain contains the directory of computers that are configured as "domain controllers". A domain controller is a server that manages all security-related aspects of the individual users and domain interactions. The security services and administration services are centrally managed on this server.

(Windows): A domain controller is a server for centralized authentication and authorization of computers and users in a computer network.

Firewall

(ISA-99): "Belongs to the connection between networks and restricts data traffic between connected networks.

Note:
A firewall can be either an application, which is installed for general purposes on an appropriate computer, or a dedicated platform (appliance), which forwards or discards packets in a network. The firewall typically serves to define zone borders. A firewall usually works with restriction rules, which allow only specific ports to be opened."

Firewall types

Serve to better distinguish tasks and application locations in this document collection:

- Front-end firewall

  A front-end firewall protects the perimeter. Only uniquely identified, real persons have access via verifiable communication (application filter). Uniquely identified and trusted devices may be permitted access (e.g. via IPSec) by declaring exceptions.

- Back-end firewall

  A back-end firewall protects the PCN production network from the perimeter and other trusted networks (e.g. MON). The back-end firewall must be realized as a performance-based solution for uniquely identified, trusted devices.

- Three-homed firewall

  A three-homed firewall is a combination front-end and back-end firewall, with a separate "minimal perimeter" for scalable security solutions.

- Access point firewall

  (Special case) An access point firewall is exclusively used for maintenance tasks, permitting access to a security cell, which otherwise would require no connection (e.g. to MES).

Control center;

(ISA-99): "Central location at which a group of resources are operated.

Note:
In an industrial infrastructure, one or more control centers usually serve to monitor and coordinate operating procedures. These are usually connected via a WAN (Wide Area Network) in complex plants with several control centers, for example, a fail-safe control center at another location. A control center contains the SCADA host computer and associated display device for operators, as well as supporting information systems, such as an archive server."

Network names

Network names facilitate the assignment of groups of networked systems with similar areas of application in this document collection, e.g.:

- ECN - Enterprise Control (Systems) Networks
  Designation for a network as component of a security cell or security zone, which contains the ERP (Enterprise Resource Planning) system. This is usually the same network cloud as the so-called office network.
- MON – Manufacturing Operations Network
  Designation for a network as component of a security cell or security zone, which contains the MES (Manufacturing Execution Systems). This is usually the same network cloud as the so-called office network or a special network or part of a production control network (PCN). The service personnel also use this network in many cases.
- PCN – Process Control (Systems) Network
  Designation for a network as component of a security cell or security zone of the plant, which contains the PCS (Process Control Systems), DCS (Distributed Control Systems) or SCADA (Supervisory Control and Data Acquisition) systems. This is always a so-called plant, terminal or HMI network. This should be a special and separate network. The service personnel also use this network in many cases.
- CSN – Control Systems Network
  Designation for a network as component of a security cell or security zone of the plant, which contains the automation systems. The PCS or DCS or SCADA server systems are also connected to the CSN to be able to establish contact to the automation systems. CSN involves the so-called plant network or the so-called plant bus. It should be a special and separate network that is not used for data communication between computers and whose bandwidth and availability are reserved for the automation systems.
- FDN – Field Device Network
  Designation for a network as component of a security cell or security zone of the plant in which only automation systems and field devices are connected to one another.
- Perimeter – perimeter network
  Designation for a separate and firewall-protected network used for policy-based data communication by means of perimeter techniques.

Perimeter network, perimeter, demilitarized zone (DMZ)

(ISA-99): "Segment of the perimeter network, which is logically located between internal and external networks"
Note:
The purpose of the so-called demilitarized zone on the one hand is to enforce the policy of the internal network for information exchange to the outside world as well as to restrict access of non-trusted external sources to public information only, and, on the other hand, thereby shield the internal network from attack from the outside world.
Note: In the context of industrial automation and control systems, "internal network" usually means the network or segment on which the protective mechanisms primarily concentrate. For example a process control network is considered an "internal network" if it is connected to an "external" enterprise network."

Process control network (general)

(ISA-99): "Networks which are normally connected to time-critical equipment for controlling physical processes (see "Secure network").

NOTE: The process control network can be divided into zones and there may be several separate process control networks within a company or location".

Process control equipment (general)

(ISA-99):" A category that includes distributed process control systems, programmable logic controllers, SCADA systems, dedicated consoles for HMI interfaces, as well as sensor equipment and control instruments in the field or managing and controlling the process.
Note: The term also encompasses Fieldbus networks, in which control logic and control algorithms are executed on intelligent electronic devices that coordinate their actions".

Industrial automation and control systems (IACS) (general)

(ISA-99): "The term encompasses control systems for use in manufacturing and industrial process plants and facilities, in building automation, in plants with geographical distributed operating procedures and those of utility companies (i.e. electricity, gas and water companies), in production and distribution plants such as pipelines for crude oil as well as other industrial branches, for example, traffic networks in which processes are automated or remotely controlled.

(ISA-99): "A combination of personnel, hardware and software, which affects the physical ("Security") and the information technological ("security") secure and reliable performance of an industrial process or is capable of influencing this performance. These systems include:

- Industrial process control systems, e.g. distributed process control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, SCADA systems (Supervisory Control and Data Acquisition), networked electronic sensor, control systems, as well as monitoring and diagnostic systems.
  In this context, process control systems demonstrate, regardless if they are physically separate or in integrated form, basic functions of process control systems as well as safety-instrumented systems (SIS).
- Assigned information systems, for example, systems for advanced or variable controlling, online optimizer, monitors for permanently installed devices, graphic user interfaces, process history, MES (Manufacturing Execution Systems) as well as plant information management systems.
- Assigned internal interfaces, network interfaces, machine interfaces or user interfaces that provide functions for controlling, safety and manufacturing operations for continuous and batch processes, discrete and other processes".

Remote access

(ISA-99): "Form of access control based on determination of identity, in which the system entities, identified and subjected to access control, represent function-related positions in an organization or a process".

Remote client

(ISA-99): "Resource outside the process control network, which is temporarily or continuously linked to a host computer in the process control network via a communication connection in order to directly or indirectly access part of the control equipment in the process control network".

Role-based access control

(ISA-99): "Form of access control based on determination of identity, in which the system entities, identified and subjected to access control, represent function-related positions in an organization or a process".

Support PC / PG

Separate mobile support PC of a support employee (e.g. support programming device, support laptop)

Support station

Stationary support PC, which is either physically located in the plant as an ES in the PCN and is therefore part of the plant or a remote ES located in a perimeter network / MON and therefore a trusted, remote plant PC.

Defense in depth

(ISA-99): "Security architecture, which assumes that each point representing a security measure can be overcome and probably will be overcome.

NOTICE: The concept of defense in depth encompasses a staged or layered structure of security and identification measures and mechanisms (even on the level of single station systems). It has the following features:

- Attackers must expect to be detected when attempting to penetrate or circumvent the individual layers.
- A vulnerability in one layer of this architecture can be compensated by defense measures in other layers.
- The system security for its own layer structure within the overall hierarchical structure of the network security".

4.2 Name conventions in figures and examples

Names, designations and symbols are used in the figures and examples to facilitate the use of this document.

Designations for networks in this document collection

Until now, the bus designation of the individual manufacturer, the name of the employed medium or a special system feature was typically used to name individual networks. However, this is no longer sufficient to describe the security cell or automation cell, the area of responsibility or the security layer / security zone in which this network is available. To meet the resulting current demands for a uniform naming convention for a variety of networks, the following network designations are used in this security concept and the figures it contains.

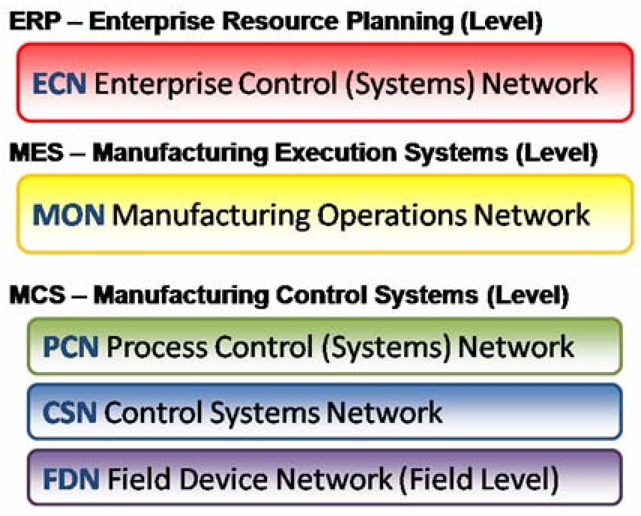
ERP – Enterprise Resource Planning (Level)
ECN Enterprise Control (Systems) Network
MES – Manufacturing Execution Systems (Level)
MON Manufacturing Operations Network
MCS – Manufacturing Control Systems (Level)
PCN Process Control (Systems) Network
CSN Control Systems Network
FDN Field Device Network (Field Level)

Figure 4-1

The network designations and the basic colors used (red, yellow, green) in Figure 4-1, identify the networks, production levels (according to ISA-95) and their security zone (according to ISA-99). The automation levels (MCS according to ISA-95) in this security concept are divided into further networks for specific tasks (green, blue, violet). This division is required by the various requirements for bandwidth, availability, reaction capability and climatic resistance and safety.

Bus designations such as: Plant bus (for CSN), terminal bus (for PCN), H1 bus, field device bus, I/O bus etc., as well as previously used network / security level designations such as ERP network, MES network, DCS network, office network etc., continue to be valid to describe the medium, the application type or topology.

Demo plant of the examples in this document collection

A concrete demo production plant including a complete network topology (IP addresses, computer names), associated DNS name spaces and a domain management is described in the following examples to provide a clear overview. The following designations are used in the figures as placeholders:

- "plant" or "plant1A", "plant1B" are placeholders for specific customer plant names.
- "enterprise", "business-unit1", "department2" etc. are placeholders for company names and the organizational departments and corresponding production areas.

An appendix of this document provides a network overview of the complete plant, the DNS name space and the domain management forest.

The following division of the DNS name space of the plant facilitates assignment and simultaneously represents a basic recommendation. The real DNS name space may deviate from this depending on the number and size of plants and the existing DNS / Active Directory domain forest. You should always use the following structure when designing networks:

- enterprise.com→ Complete **external** name space of the company for remote access and Web publishing in the Internet
- enterprise.local→ Complete **internal** name space of the company (Intranet)
- department1.enterprise.local→Intranet name space for the **enterprise layer** (office network) of department 1 responsible for production area 1
- manufacturing-execution1.production1.enterprise.local→ Internal name space of the **manufacturing control** of plant 1
- production1.enterprise.local→ Complete internal name space of the **process control** of plant 1
- plant1A.production1.enterprise.local or plant1B. production1.enterprise.local→ Internal name space of the **process control unit 1A** (basically, plant1B for unit 1B etc.)
- perimeter1.production1.enterprise.local → Internal name space of the **perimeter network** of plant 1 (is also used in this way for publishing in the Intranet)
- production1.enterprise.com→**External** (e.g. in Internet) **published** name space of the perimeter network of plant 1

5 Strategies of the security concept

Targeted protection against each and every current or future threat or method of attack from the inside or outside is not possible. With that said, this security concept deals with general defense strategies designed to protect against the following threats:

1. Denial of service
2. Circumvention of specific security mechanisms (such as "Man in the middle")
3. Intentional maloperation through permitted actions (such as password theft)
4. Maloperation through non-configured user rights
5. Data spying (e.g. of recipes and business secrets or operational plans for plants and their security mechanisms)
6. Manipulation of data (e.g. to downplay the importance of alarms)
7. Deletion of data (e.g. log files to cover up attack activities)

The following defense strategies serve as an overall approach to supplement the required and desired access types and operator control options with the majority of available security mechanisms in a multi-level defense (defense in depth) with numerous security layers. The table provides an overview of the important goals and strategies that are described in the following sections.

Goals and strategies	Section in Security concept
Comprehensive protection against security threats through access-based, multi-level defense.	Defense in depth
Increased availability and proliferation prevention of security threats through division into task-based security cells.	Division into security cells
Preventing the misuse of role-based access control for users, software components and devices.	Role-based access control
Reaction to current and future security threats with centralized maintenance, servicing, updating and distributed security of the employed products with defined distribution routes.	Role-based grouping and management, central and local data storage and configuration

Individual security measures (e.g. IP Security or VPN) can be used several times or simultaneously fulfill various requirements. These security measures are described once for all situations in common and noted for the given security solution with references to the command description.

The various security measures and strategies may influence one another for better or worse. Each case requires that a correct balance be found for availability, security, comfort and performance. If there is a conflict in this regard in one of the described security solutions, it will be noted.

The main aim of the following descriptions for the individual security strategies and their implementation in a system is to support the plant designer and operator in assembling the latest security measures so that future security measures can be specifically and efficiently supplemented.

5.1 Defense in depth

From the point of view of the plant manager, secure access to the components of his plant should allow him to perform regularly occurring tasks. This access is realized through a variety of components and mechanism of process control and process visualization. The risks associated with such access differ. These access actions are classified more exactly as "access types" from the customer's point of view in the following.

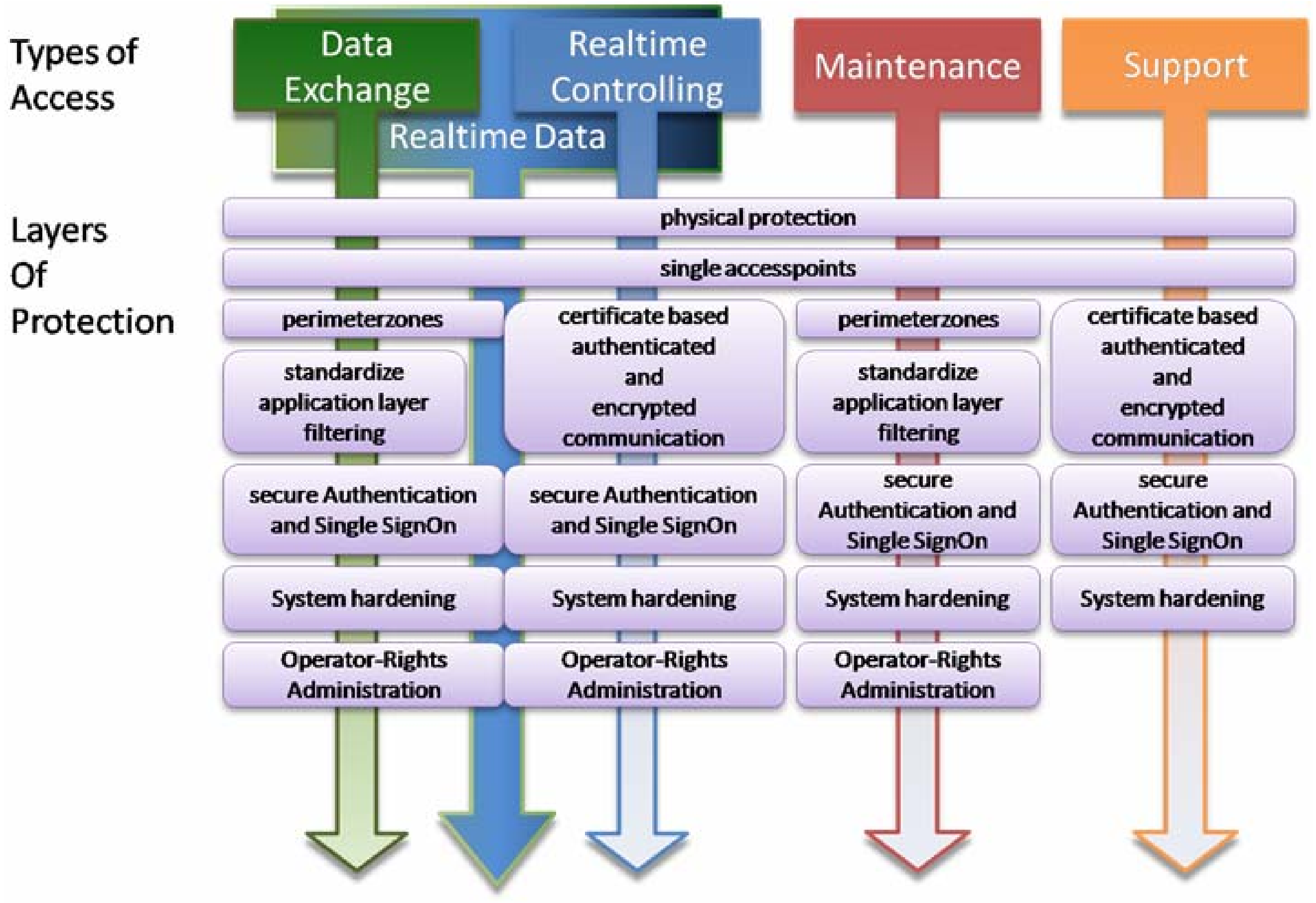
Types of Access
Data Exchange
Realtime Controlling
Realtime Data
Maintenance
Support
Layers Of Protection
physical protection
single accesspoints
perimeterzones
certificate based authenticated and encrypted communication
perimeterzones
certificate based authenticated and encrypted communication
standardize application layer filtering
standardize application layer filtering
secure Authentication and Single SignOn
secure Authentication and Single SignOn
secure Authentication and Single SignOn
secure Authentication and Single SignOn
System hardening
System hardening
System hardening
System hardening
Operator-Rights Administration
Operator-Rights Administration
Operator-Rights Administration

Figure 5-1

The defense in depth strategy in this documentation is not a simple list of the security measures used in process control engineering, for example, encryption, authentication, authorization etc.; it is a description of practical application of these security measures in the various "layers of protection", exactly adapted to the "types of access" from the customer's point of view and shown in overview in Figure 5-1.

Access is only allowed from specifically authenticated network devices and by authorized users. "**Data exchange**" and "**realtime controlling**" in this overview represent the IT connection among the Enterprise Resource Planning (ERP) systems on the business layer, the Manufacturing Execution Systems (MES) for manufacturing control and the Manufacturing Control System (MCS) of the automation layer. Servicing and upkeep of the various systems is summarized as "maintenance", for example, regular installation of security updates or the collection and analysis of diagnostics and log files. "**Support**" represents required remote access for updating, upgrading or trouble-shooting the employed systems.

Examples of access types

- **Data exchange** / information exchange: Data and information exchange between various production levels, neighboring plants, onshore/offshore components, automation and security cells.
- **Realtime controlling** / remote controlling: Control or remote support of onshore to offshore or different plants or between the remote control center and the plant.
- **Maintenance**: Normal monitoring and archiving of diagnostic information, data backups, updates or fine tuning of configurations).
- **Support**: All engineering activities, upgrades or changes of the process control system, as well as error diagnostics and correction.

The overview of Figure 5-1 refers to a "**realtime data**" access type, which represents a combination of "**data exchange**" and "**realtime controlling**". This combination access type usually results from the employed access method or the bundling of several functions by the plant manager. **From a security point of view, however, this mixed access type should be avoided, since the security measures used are too different and compromise solutions often mean increased risk.**

Planning the plant or plant migration involves consulting with the plant manager and, based on the required access types, deciding which of the following security mechanisms and security layers need to be implemented:

1. **Physical protection** (i.e. control of the physical access to spatial areas, building, individual rooms, cabinets, devices, resources, cables and wiring) -> must be aimed at security cells and responsible persons. It is also important to realize physical protection at remote single station systems.
2. **Single access point** to each security cell (should be a firewall system) for the authentication of users, employed devices and applications, for the direction-based access control and the assignment of access permissions as well as for detection of break-in attempts. -> Functions as a main access point to the network of a security cell und serves as the first point of a control for access rights to networks levels.
3. **Perimeter zone techniques** should be used. This means in this case the use of data that is exported and not directly intended for process control, available on a system (data medium, database) located between the main access point for data (the so-called front-end firewall) and the deeply embedded access point for data (the so-called back-end firewall) or in the third network segment of a three-homed (located in three networks) firewall.

4. **Standard application layer filtering techniques** should be used (i.e. an access mechanism that allows each and every command to be checked on the highest level of analysis for available access rights as well as for malicious or criminal intent (usually realized for standard Web servers, published by the front-end firewall), and does not hinder the control of the process if failure occurs).

   - **Scanning of incoming viruses** (generally corresponding to this technique or part of this technique) means that all files and readable data entering any systems of the plant are scanned by the first system, which allows access to the file/data and reading of the file/data.

5. **Certificate-based authenticated and encrypted communication** should always be used when the perimeter zone technique or standard application layer filtering technique are not available. This can take place using tunneling protocols such as PPTP (Point-To-Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol) or IPSec (IP Security) filtering or even via channels that are also secured by server-based certificates, for example RDP (Remote Desktop Protocol), a Windows Server 2003 terminal server securely published via HTTPS or Windows Server 2003 Web server via the firewall using SSL (Secure Sockets Layer) technology.

6. **Secure authentication and single sign-on** should only be used when an Active Directory domain under Windows provides an advanced function for delegating the authentication instead of formula-based authentication, for example NTLM V2, Kerberos or a SecurID card. This provides the network administrator with centralized, time-based and role-based password policies as well as group-based access right management and a standardized audit trail. System hardening means firewall protection against access from any location outside the own security cell, careful prior configuration of access control lists (ACL) and their access control entries (ACE) to protect all objects accessible via remote access, for example files, registry entries and applications (DCOM), in addition to restricting all systems to tasks specifically assigned to them.

7. **Security updates** (generally corresponding to this technique or part of this technique) means that system security updates and virus signature updates need to be available and installed as quickly as possible. Some procedures described in section "Patch management and security updates" need to be followed to prevent the security update from interfering in currently running processes.

8. Management of operator control permissions for each Siemens application when necessary. This is the "last line of defense", also referred to as "**role-based access control**". It should be realized or practiced by the plant manager and his operating personnel. An extreme example for this is the use of the write-protected "PCS 7 Webnavigator" clients or write-protected "WinCC Webnavigator" clients, in which it is hard-wired that no change can be made to the data of the process control system and which therefore make them suited for presentation purposes or write-protected information systems.

5.2 Division into security cells

The strategy for dividing plants and connected plants into security cells increases the availability of the overall system. Failures or security threats that result in failure can thereby be restricted to the immediate vicinity.
During the planning of the security cells, the plant is first divided into process cells and then into security cells based on the security measures.

Process cells and security cells

Process cells represent specific production-related zones, sections, sub-areas or units and must fulfill the following conditions:

- A process cell must be an autonomous "operational plant or unit", which can run for a certain period of time without connection to the rest of the plant or plant units, i.e. a process cell must be and remain independently operational for a time.
- All elements that belong to a process cell must be connected directly to one another (e.g. not via leased lines). Technically, this is a LAN (Local Area Network).
- Plant units that cause high network and computer load, e.g. if they have to be connected from the outside via expensive security mechanisms, should always be integrated directly in the process cell.

One or more process cells become a security cell when the following conditions are met:

- Only trusted and authorized persons with appropriate instruction are given access to a security cell. The following accesses must be strictly controlled:
  - Physical access to the production areas and process control rooms
  - Operation of the process control system and manual production sections
  - Access to file system and configuration of the process control stations
  - Access to computer and control networks, their power supplies and infrastructures (e.g. network services, domain controllers)
- Legitimacy of all access to a security cell must be checked beforehand. This means persons and devices must be authenticated and authorized, for example.
- Every access must be recorded or monitored by an authorized person, e.g. bodily access, file access, support work etc.

Summary

The planning of security cells is based on actual areas of responsibility, the separable process cells, the physical access possibilities and the resulting network design and access protection.

Operation of individual security cells or segments is enabled by temporary loss of units in the infrastructure (e.g. network shown in red in Figure 5-2).

This means information and services which is generated on the outside and required within the security cell must be buffered or substituted within the respective security cell using suitable measured (e.g.: recipes and material data, network services such as name resolution, IP address assignment, user authentication).

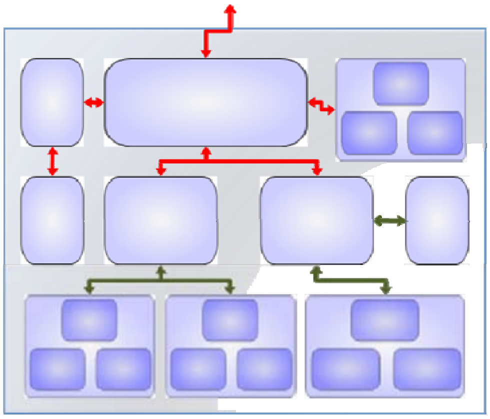

Figure 5-2

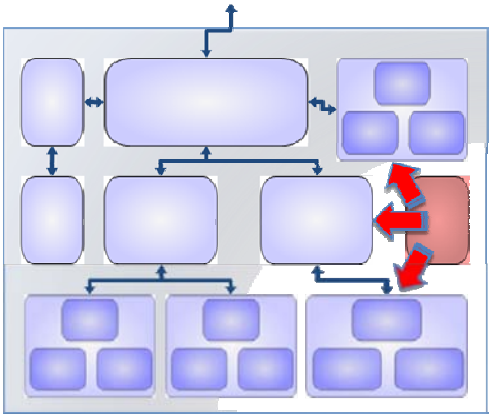

Figure 5-3

The entire system is protected if a security threat occurs within a security cell (e.g. a virus as shown in red in Figure 5-3). The security threat has no influence on other security cells or their members. The overall system can continue to be operated while the security threat is being eliminated.

5.3 Role-based access control

The strategy of role-based access control includes restriction to minimally required rights and functions for users, operators, devices, network and software components.
Close consultation on the following aspects is required to achieve effective protection with this strategy without restricting normal activities:

- Access control for the respective plant and its area protection
- Intended use of individual devices and software components
- Organization of the production and its areas of responsibility and thereby for the plant manager
- Administration of the plant
- Responsibilities of the operator

This consultation can be based on the production levels and the production process, and this is described below.

Note: In certain branches (such as oil & gas) or in small plants, the only division to be made is for local and remote access to a plant, in other words, there is no MES / ERP connection. Security for simple remote access is described in the section "Secure access techniques".

The organization of the production process (see Figure 5-4) is in many ways based on the three layers ERP, MES and MCS, which are defined by ISA-95.

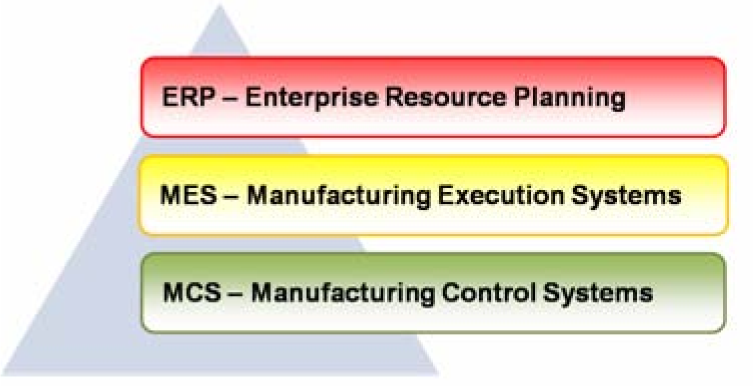
ERP – Enterprise Resource Planning
MES – Manufacturing Execution Systems
MCS – Manufacturing Control Systems

Figure 5-4

The areas of responsibilities for resources (e.g. personnel, material, plants) within a company is based on the production process and must reflect the relationship to the respective structures and plant components:

- Rights management for users and computer (e.g. using domain management)
- Assignments of the plant operator (e.g. through user management in the software of the process control systems)
- Software components (e.g. through local access rights of the software on the computer)
- Device
- Network (e.g. including the administration of the network and the network access)

In general, there is already an administration for the IT infrastructure and the office computer (labeled as "**Responsible ERP administrator**" in Figure 5-5). The separate, specialized administration for the automation devices and process control plants (labeled as "**Responsible MCS administrator**" in Figure 5-5) must also take on the administration of the production-related computer systems, since the responsibility for the entire production level) belongs to the production manager and his staff.

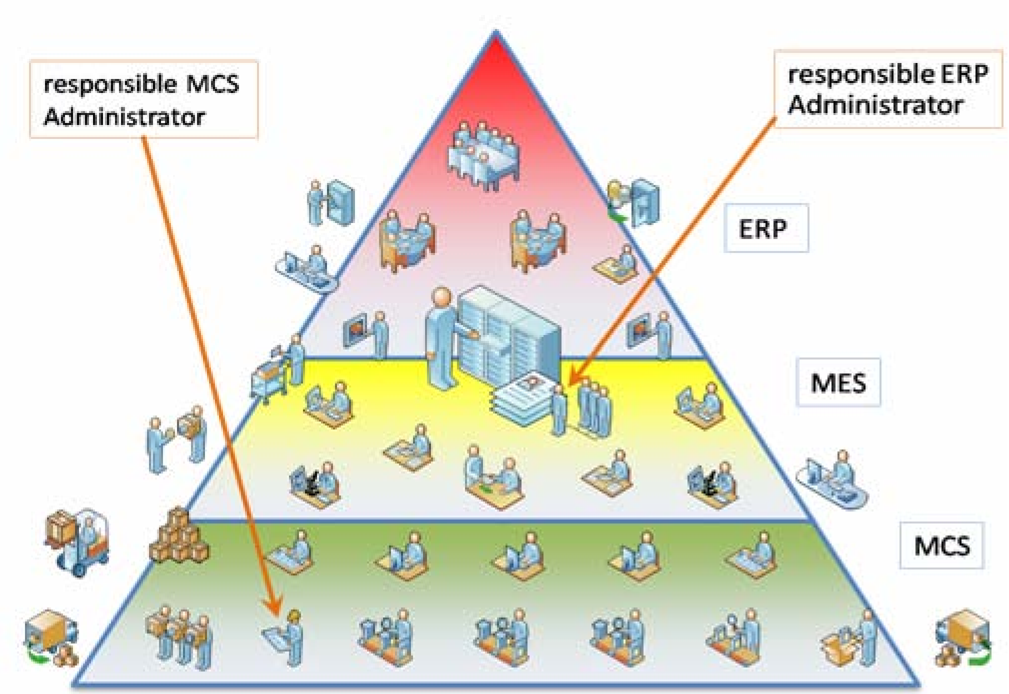

Figure 5-5

To prevent security gaps, the areas of responsibilities need to be exactly delineated, including the network and administration levels, in consultation with the other production levels.

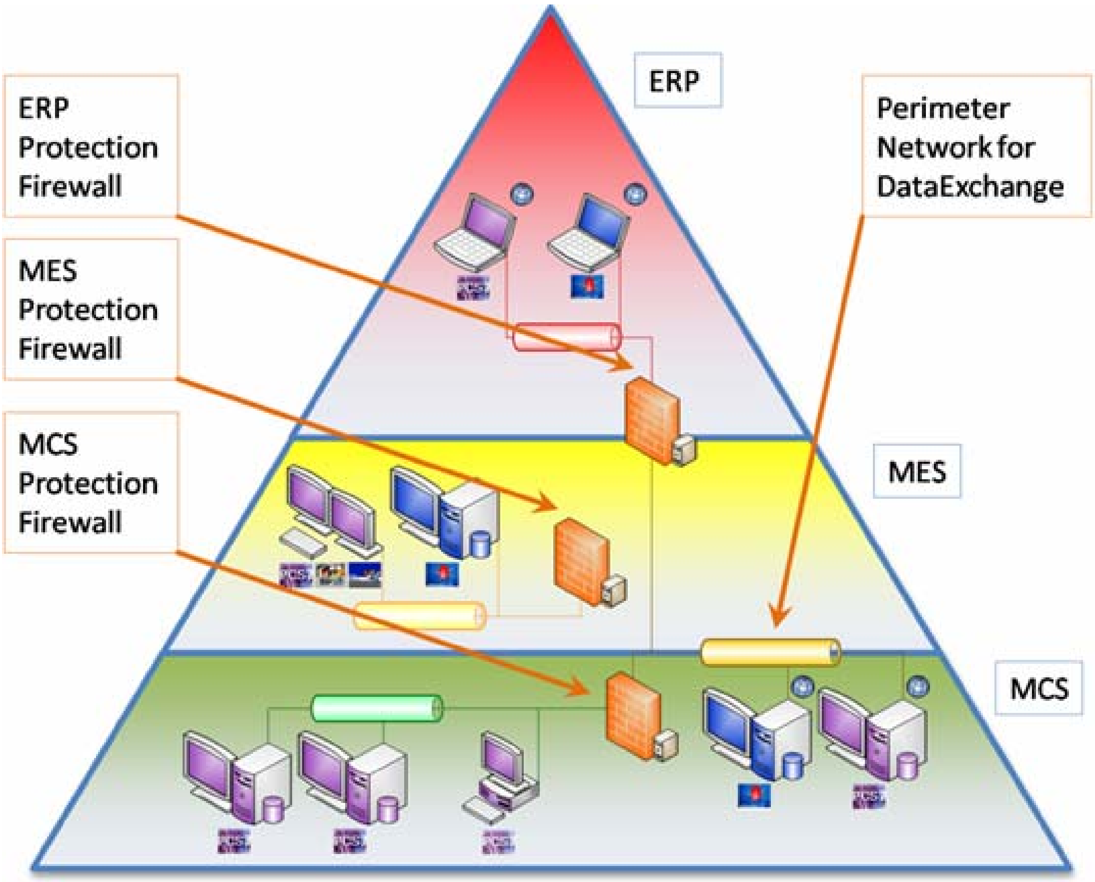

Figure 5-6

To realize the area of responsibilities, the network design and the technical options for controlling the network traffic for the individual networks (shown for example in Figure 5-6 with firewalls and perimeter) must correspond to these areas of responsibilities.

The administration of users and computers in domains must be adapted to these areas of responsibilities. Figure 5-7 provides an example of the connection through different types of trust relationships between administration domains (Windows) of the office IT (ERP layer) and the production IT (MCS layer). In the figure, the manufacturing control area (MES layer) does not have its own IT administration; it is managed by either the office IT or production IT area, depending on where the involved users and computers of a company spend the most time.

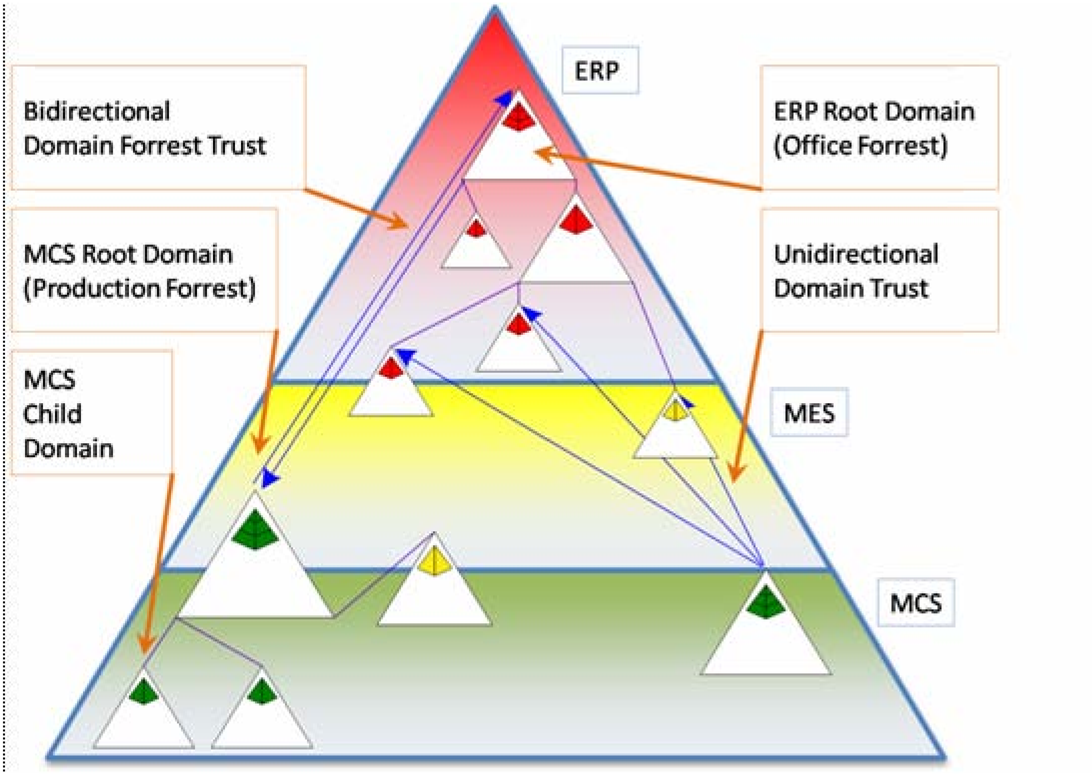
ERP
Bidirectional Domain Forrest Trust
ERP Root Domain (Office Forrest)
MCS Root Domain (Production Forrest)
Unidirectional Domain Trust
MCS Child Domain
MES
MCS

Figure 5-7

The trust relationships between domains facilitate secure, mutual identification of users in these domains. The trusted users can be given access to the other domains.

The plant manager (production manager) is responsible for the practical restriction of the process operator control permissions for the individual plant operators. The settings are made in the process control system or process visualization applications (e.g. via SIMATIC Logon).

Note

A unauthorized user can change settings of the administrative rights if the plant operator are set incorrectly on the operating system level.

Each process control station, software component or network hardware should only be able to perform the tasks locally or in the network as stipulated by the manufacturer. This restriction reduces the potential for damage due to an "assumed security credential" of a user or device.

5.4 Role-based grouping and management, central and local data storage and configuration

This section describes administrative tasks for servicing, maintenance and updating of a plant, which need to be specifically planned and ensured due to their strategic importance. The requirements for servicing, maintenance and updating of a plant are very similar in regard to the security solutions.

Requirements

- All tasks should be always realized and managed from a central location (e.g. backup server, Windows Update Service server etc.).
- All tasks must use the distribution and security routes configured in the given plant (e.g. network connections, firewall connections etc.).
- The grouping of systems with the same settings or functions (e.g. in the Windows Software Update Service) reduces the susceptibility to error from individual local configurations.
- Critical plant units must be defined and grouped in such a way that these groups can be edited independent of one another without having to stop the entire plant operation. The following groups may be created, for example:
  - All master systems of redundant server pairs in a "Master group"
  - All standby systems in a "Standby group"

Tasks

1. **Software updates:** Planning and execution of centralized distribution of software updates e.g. security updates, hotfixes, installations, virus signature updates, upgrades, project updates etc. from a central location to the individual components to be updated.
2. **Software configuration:** Planning and execution of centralized system configurations, e.g. operating system, virus scanner, Windows update etc. from a central configuration server to the individual systems to be configured.
3. **Backup and restore:** Planning and execution of local and centralized backup of data, programs, operating systems etc. with a central storage location and restoring such backups.
4. **Reporting and diagnostics:** Planning and execution of centralized backup of local diagnostics data, log files, reports etc. for centralized reporting of local events.

Any deviations should only be made after consulting with the plant manager.
An example for this is only local storage of data / backup files, since the loss of the local storage location means that this data would no longer be available.

6 Implementing the security strategies in security solutions

The successful implementation of the security strategies in security solutions for actual automation plants with SIMATIC PCS 7 and SIMATIC WinCC, can only be achieved with responsible cooperation of all those involved. This specifically includes:

- Manufacturer (development, system test, security test)
- Project engineer and integrator (planning, construction, factory acceptance test)
- Plant manager (operation and administration)

The strategies and their implementation must be observed and updated throughout the entire service life of a plant and beyond (beginning at the bid proposal, planning and design, continuing through the migration and up to the demolition of the plant).

The following aspects enable the security concept described here to reach its full potential in automation plants:

- The use of stabile, fault-tolerant and system-tested SIMATIC products.
  These products demonstrate the basic hardening (IP hardening) and predefined security settings, for example, from the Siemens Security Control (SSC) and have been especially designed for industrial application.
- Configuration that uses the latest technology and standards allows a plant design adapted to the security demands.
- Security solutions can only reach their full potential when the plant and components are operated carefully and responsibly in accordance with the intended use declared by the manufacturer.

The following table provides an exemplary overview of the security solutions recommended here for implementing the above-mentioned security strategies. These security solutions are explained in the following sections and described in greater depth in the respective detail documents. They are intended to provide support to responsible-minded plant managers in fulfilling their job of improving the security of their automation plants.

Security solutions	Section in Security concept
Secure plant configurations: • High security large plants • Secure plants • Secure small plant • Secure security cells connection	Security cells and network architecture • High security large plants • Secure plants • Secure small plant • Secure security cells connection
Protection of typical access types	Secure access techniques
Prehardened process control engineering	Hardening
Secure configuration of: • Users and computers • Networks and network services • Operator control permissions	Management and configuration • Managing computers • Managing networks and network services • Managing role-based operator control permissions
Regular updating to close newly discovered security gaps	Patch management and security updates
Checking incoming files for harmful content	Virus scanners
Recording security-related and process specific data	Logging, audit, maintenance and asset management
Regular check and improvement of security level	Security tests

A basic requirement for each of the following security solutions is the use of reliable network peripherals.

All security solutions and test configurations in the examples of the document collection are therefore shown with components of the SCALANCE product family of SIMATIC NET. The process control network (PCN) and the control system network (CSN) are realized as rings with fast media redundancy. The increased availability of these networks results from the very fast reconfiguration time of the network following a fault. This feature of the products was specially developed for use in industrial environments.

Figure 6-1 shows an example configuration from the SIMATIC NET product catalog.

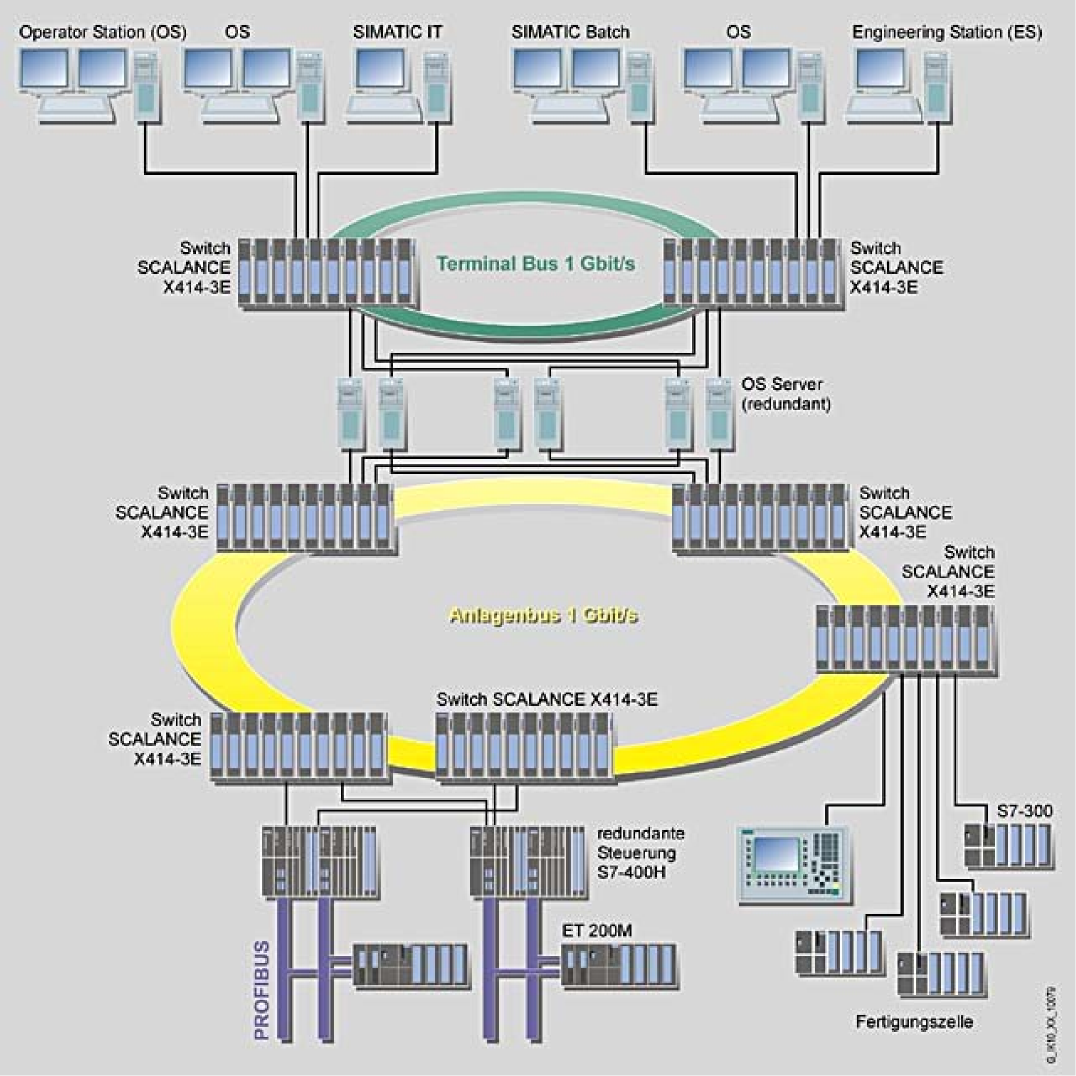

Figure 6-1

The connected terminals in Figure 6-1 do not need to immediately break logical communication connections every time there is a network interruption in the ring. Breaking the communication connections would result in an uncontrolled runtime process or emergency stop of the plant. SIMATIC NET uses a special procedure for controlling the media redundancy to achieve the required, very fast reaction time. The reconfiguration of a network to a functioning network structures is thereby ensured within fractions of a second. In a ring of 50 SCALANCE switches, therefore, the reconfiguration of the network following a fault (such as a wire break or switch failure) is completed in less than 0.3 seconds. The connected terminals remains unaffected by the change in the network. The control of the process or application is assured at all times.

In addition to the realization of fast media redundancy in the ring, SIMATIC NET switches also offer the required functionality for fast redundant connection of rings or network segments. Rings or any type of network segment structures can be connected via two switches.

You can find detailed information on SIMATIC NET as network peripherals at:
http://www.automation.siemens.com/net/index_00.htm

6.1 Security cells and network architecture

Definition of access points for the security cells

Network access points should fulfill the following basis requirements:

- Block prohibited data traffic to the process control and process visualization systems
- Enable permitted data traffic and the normal operation of the process control and process visualization systems

Access points can be:

- Front-end firewall
  A front-end firewall protects the perimeter and allows access to Web publications of the perimeter and remote dialing options of the back-end firewall.
- Back-end firewall
  A back-end firewall protects the PCN production network and allows mainly certificate-based, encrypted and signed access of individual trusted remote stations and trusted networks (e.g. MON of the MES manufacturing control system) and remote and support access to the PCN.
- Three-homed firewall
  A three-homed firewall is a combination front-end and back-end firewall, with a separate "minimal perimeter" for scalable security solutions.
- Access point firewall (special case)
  An access point firewall is exclusively used for maintenance tasks, permitting access to a security cell, which otherwise would require no connection (e.g. to MES).
- Back-end router (e.g. SCALANCE S)
  A back-end router enables load decoupling with high throughput, usually in combination with an upstream three-homed firewall.

The security cell and network designs are intended to finely delineate the area of responsibility of the plant manager (e.g. from the IT administration of the ECN and office network). This means the plant manager must have explicit administrative rights and privileges in his security cell. The decision as to which security cell and network designs should be implemented is generally influenced by the importance and size of the plant, its spatial division, the determined risk and the available budget. The examples in the following sections provide an overview.

The following criteria were generally used for selecting and labeling the plant examples:

- A plant example is referred to as "high security" when it features the highest possible number of security layers (e.g. the front-end/back-end firewall combination is more secure than a single firewall, because if the front-end firewall is breached by an attack, the production-related network is still protected by the back-end firewall).
- A plant example is referred to as "secure" when it features basic security mechanisms (e.g. the perimeter technique of Web publishing instead of direct access to the Web server).
- A plant example is referred to as "large" when it has its own infrastructure (e.g. domain controller) or is connected to the data processing of the company (e.g. connected to the MES layer via SIMATIC IT and therefore to SAP).
- A plant example is referred to as "normal" (and therefore lacks a special label) when a classic DCS is installed in it as a multiple station system (without a special infrastructure) and contains only rudimentary connections or its own MES.
- A plant example is referred to as "small" when is mainly a single station system or multiple station system without connection to other plants or the data processing of the company.

6.1.1 High security large plants

A high security large plant is a plant example with its own perimeter and infrastructure, its own network services and administration, protected service access, protected remote control, secure Web publishing and protected manufacturing control connection.

Figure 6-2 below is a simplified design of a secure large production plant in which the areas are color-codes as follows:

- The PCN (green network).
- The CSN (blue network).
- The upstream **perimeter network** (brown network) belonging to the responsibility area of the plant, protected by a **front-end firewall** and **back-end firewall**.
- A trustworthy MON for the manufacturing control system **MES** (yellow network) can be operated within the plant.
- The office and company network **ECN** (red network) secures itself optionally via its own firewall. This is based on the assumption that the access of non trusted computers to the WAN/Intranet cannot always be controlled. The WAN/Intranet here more or less represents an example of an open company network.

All three production-related areas (green, yellow, brown) are protected as security cells and are independently operational for a defined period of time.

The web-based access from the ECN to a Web server of the plant in the perimeter is made through Web publication of the front-end firewall. User activities can be checked and recorded there using application filters. The process control Web server (e.g. OS Web server) in the perimeter fetches its data from the process control servers (e.g. OS server) in the PCN via a certificate-based, signed connection (IPSec) through the back-end firewall. The back-end firewall checks if this connection can be authenticated and established by the two nodes. This ensures high performance and the security that only known and trusted systems from the perimeter are permitted targeted access to specific systems of the PCN from the perimeter via the back-end firewall.

Support and remote access can take place using several access types and routes. Access is centrally authenticated, authorized and logged through the back-end firewall.
You can find additional information on this in the "Protected service access" section.

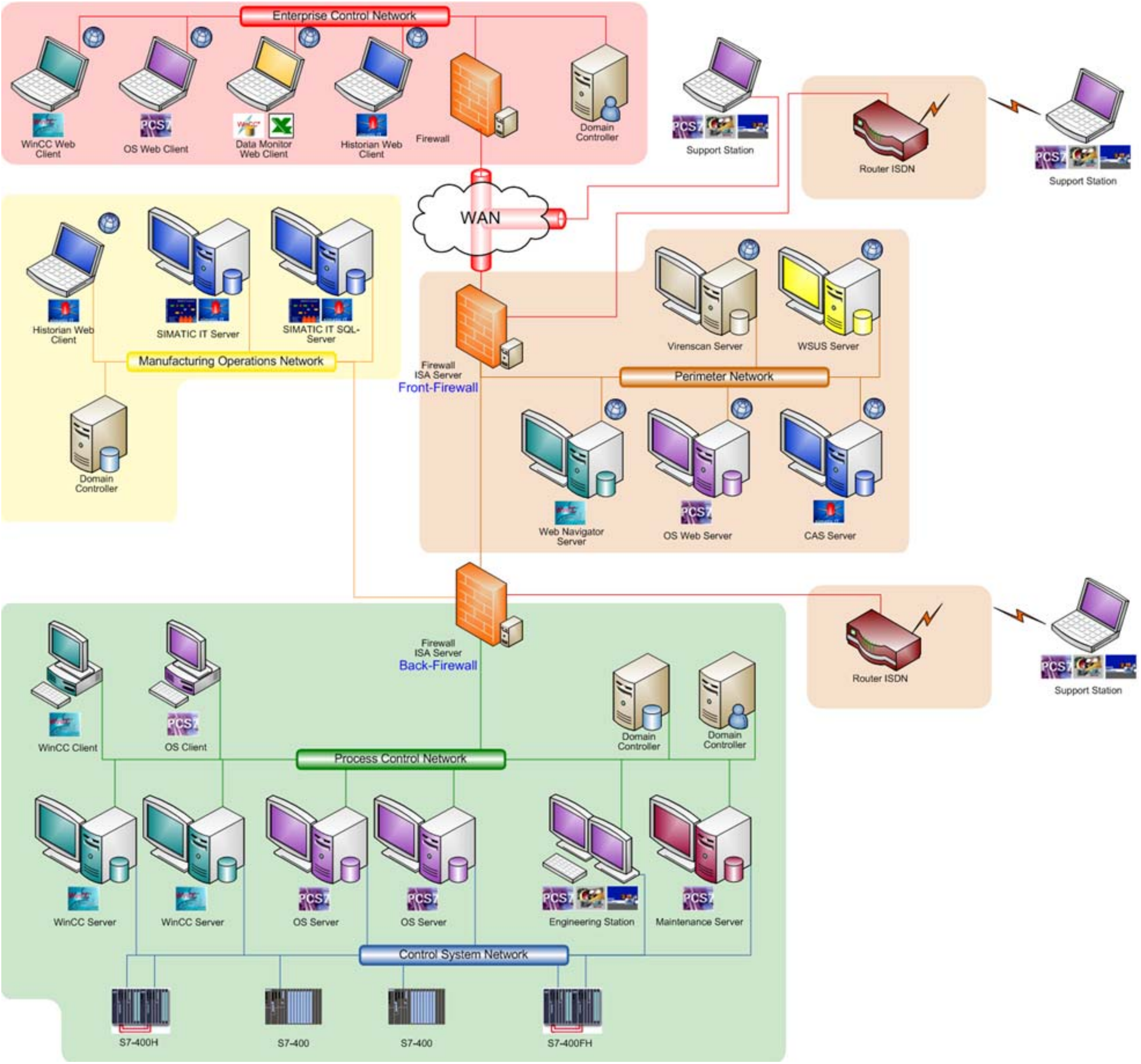

Figure 6-2

Detailed plant description

- Process control multiple station system in a security cell (green)
- Administration and authentication within the PCN through Active Directory using a separate, independent PCN domain (production domain)
- Important network service are provided within the PCN, for example:
  - Name resolution (WINS, DNS)
  - Address assignment (DHCP)
  - Time synchronization (NTP, SNTP)
- Remote, trusted clients and server of the process control systems (e.g. Web servers, MES servers) without direct process interface, are integrated via encrypted or signed communication in the PCN security cell. The mutual authentication is made through certificates; the back-end firewall allows for configured IPSec traffic.
- The perimeter network contains Web servers. These devices publish process control data that has been or will be swapped out and functions as an application gateway. The Web servers provided web-based services such as a certificate authority, security update service etc..
- Non-trusted devices in the ECN office network obtain user-based access to Web-based publishing of the production plant in the perimeter from front-end firewall through perimeter techniques. The authentication takes place through a server-end encrypted connection (HTTPS) using user name and password.
- Trusted users from the MES manufacturing control working in the ECN office network, can be given access to data for selected applications via firewall client software of the front-end firewall. The use of these applications depends on whether or not an application can assume the function of the firewall client (Winsock conform and user context compatible).

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.1.2 Secure plants

A secure plant is a plant example with a three-homed firewall and minimal perimeter, integrated manufacturing control, but without its own infrastructure.

Figure 6-3 below is a simplified design of a secure production plant in which the areas are color-codes as follows:

- The **PCN** (green network).
- The **CSN** (blue network).
- The separate "minimal" **perimeter network** (brown network) belonging to the responsibility area of the plant, protected by a **three-homed firewall**.
- A trustworthy **MON** for the manufacturing control system **MES** (yellow network) can be operated within the plant.
- The office and enterprise network ECN (red network) optionally protects itself with a separate firewall, in the assumption that the access of trusted computers to WAN/Intranet cannot always be controlled. The WAN/Intranet here more or less represents an example of an open company network.

All production-related areas (green, brown) are protected by a common security cell.

The web-based access from the ECN to a Web server in the "minimal" perimeter is made through Web publication of the three-homed firewall. User activities can be checked and recorded there using application filters. The Web server of the process control system in the "minimal" perimeter fetches its data from the servers of the process control system in the PCN via a certificate-based, signed connection (IPSec) through the three-homed firewall. This ensures high performance and the security that only known and trusted server are permitted access to the PCN from the "minimal" perimeter via the three-homed firewall.

The support and remote access can be made via several access methods and routes, but is always centrally authenticated and authorized through the three-homed firewall; this is described in more detail in section "Protected service access".

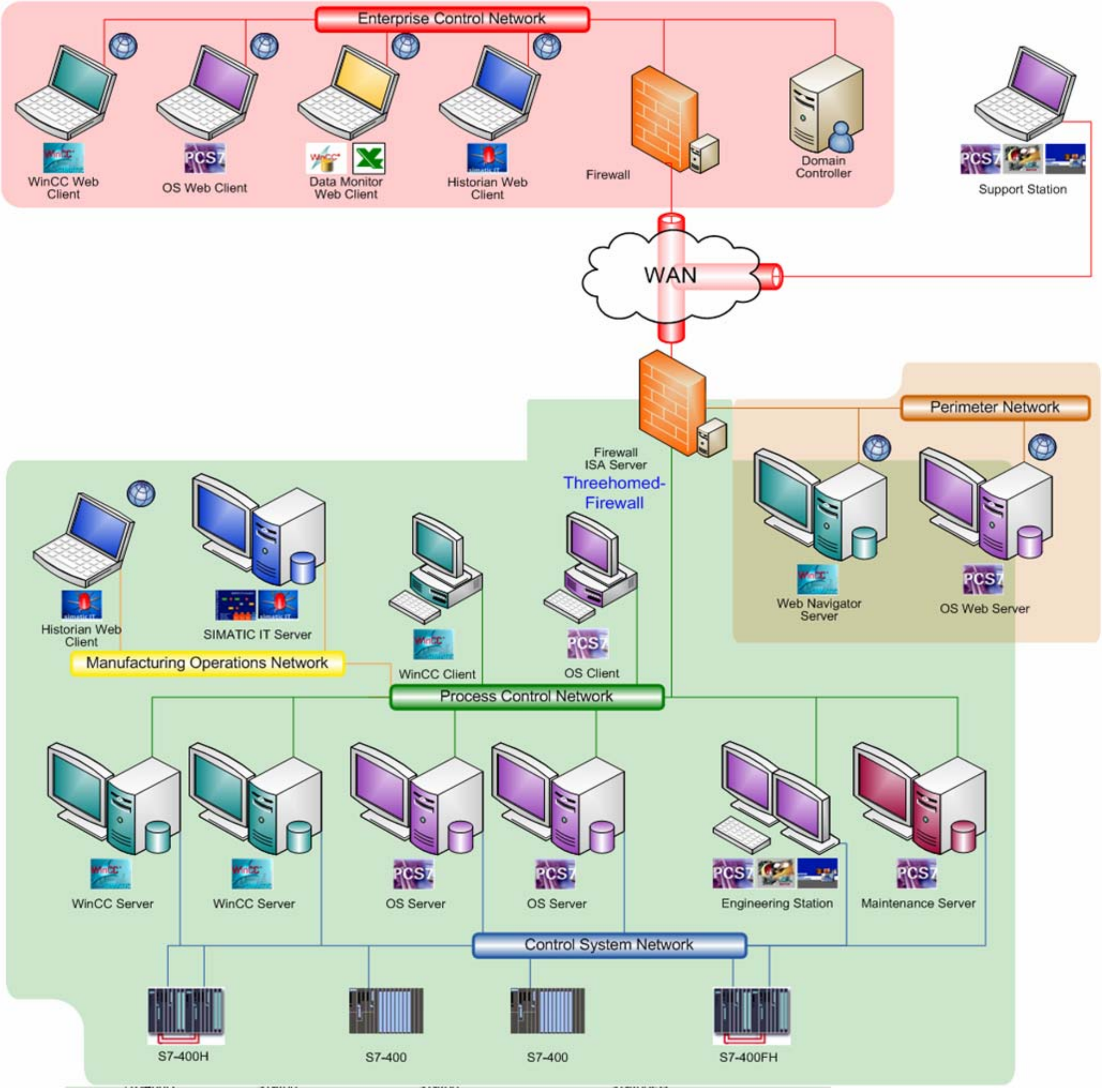

Figure 6-3

Detailed plant description

- Multiple station system in a security cell (green and brown) with separate "minimal" perimeter (brown)
- Since the perimeter of the enterprise and office network (not shown in the figure) does not belong to the responsibility of the plant operator and therefore cannot be used as the DMZ of the plant, plant data to be published is made available via an additional, separate "minimal" perimeter at the three-homed firewall.
  Alternatively, specially hardened systems located in the ECN and under the responsibility and physical control of the plant operator can be given specific access to special data and services of the plant.
- These systems always represent a special configuration and need to be individually planned and adapted to the plant. The plant operator must be informed of deviations from the strategies of this security concept. This information is essential if it restricts the users' area of responsibility or can be influenced by other administrators.

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.1.3 Secure small plant

A secure small plant is an example of a security cell connected via an access point firewall to an external, unprotected network, although all process control functions are implemented within the security cell. This category includes multiple station systems, those with Web clients for example, as well as any number of single station systems.

Figure 6-4 below is a simplified design of a secure small production plant in which the areas are color-codes as follows:

- The **PCN** (green network).
- The **CSN** (blue network).
- The entire security cell is protected by an **access point firewall** that belongs to its own area of responsibility.
- The office and enterprise network ECN (red network) optionally protects itself with a separate firewall, in the assumption that the access of trusted computers to WAN/Intranet cannot always be controlled. The WAN/Intranet here more or less represents an example of an open company network.

The production-related area (green) is protected by a security cell.

Note

Systems operated exclusively within a security cell should never be connected to an external, unprotected network unless it is absolutely necessary. Service access represents the only exception. In general, one or several single station systems should not be operated with a direct connection to runtime in an unprotected network (i.e. outside a security cell), since control of the process is endangered even by a single potential security threat (too few security layers).

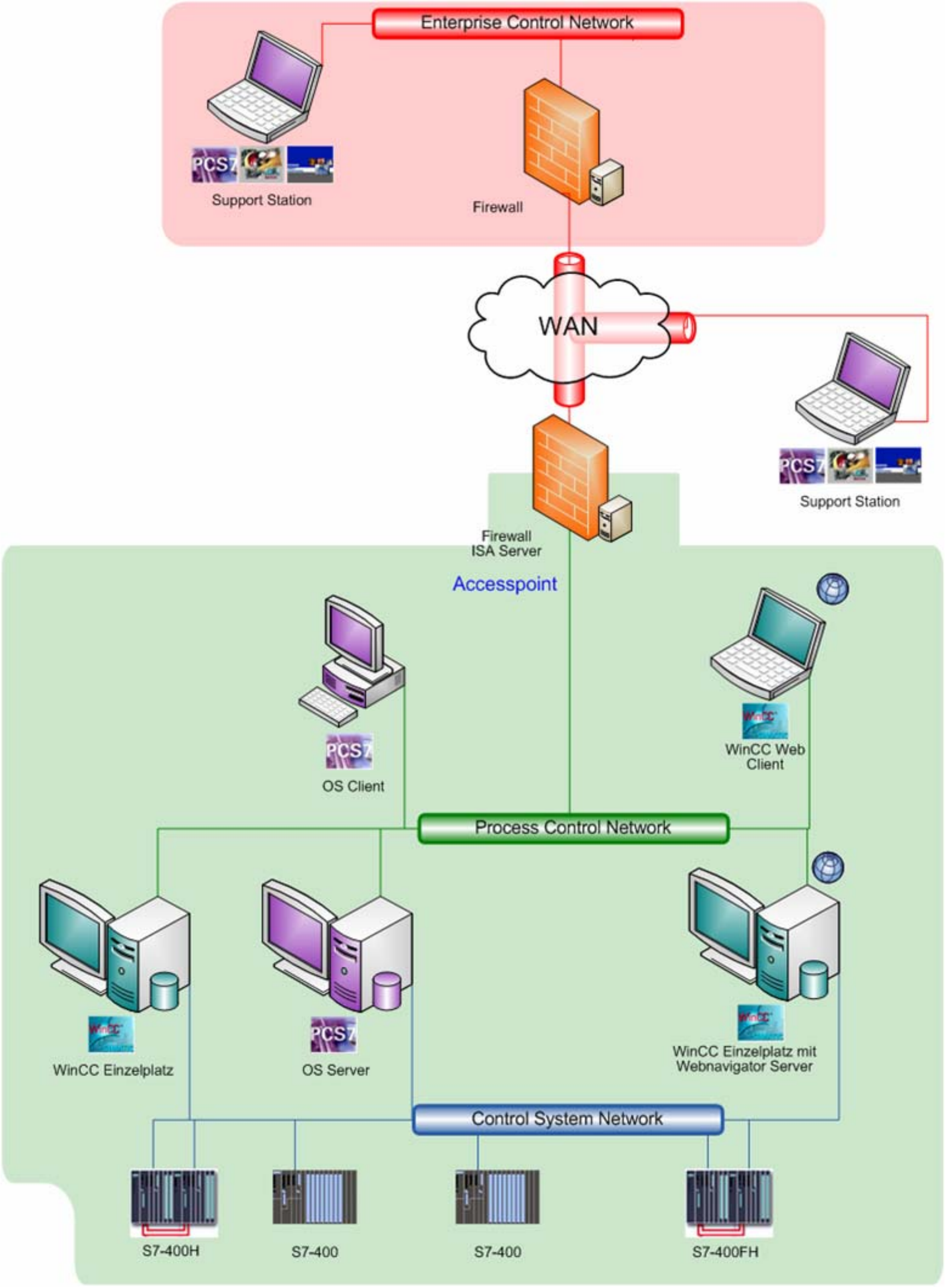

Figure 6-4

The support and remote access for servicing can be made with a variety of access methods and access routes, but must always be centrally authenticated and authorized at the additional firewall (access point firewall) for this security cell.

Additional information

You can find detailed information on this in the Internet at the following address:

http://support.automation.siemens.com/WW/view/en/28580051

6.1.4 Secure security cells connection

The connections between mutually trusted security cells must be made available via encrypted tunnel communication, such as IPSec or SSL/VPN Tunnel. These security mechanisms have no influence on other communication within the security cell. The communication leaving the security cell is encrypted and restricted in its performance.

Notice

All tunnel mechanisms and firewalls are potential "rupture joints" of the network.

For example, the data transmission of a firewall is highly restricted if the firewall goes into a safe state due to a detected attack. All plant units must be designed in such a way that enables the plant to remain operational even during a temporary failure of the security cell connection.

Security cell connections are realized between the following components:

- The access points (back-end firewall, three-homed firewall, access point firewall)
- The security cell participants (local IPSec filter rules of the individual operating systems)
- The security lead gear (SCALANCE S security modules)

Figure 6-5 shows an example of two security cells (production units plant1A and plant1B) protected by access point firewalls. The cells use a common MES component in the plant1A unit. Both firewalls allow configured IPSec communication between the MES component and the stations of the process control system of the second plant1B unit. The MES component and the participating process control stations are configured for certificate-based IPSec communication. Communication is established when one of the participating destination IP addresses is addressed.

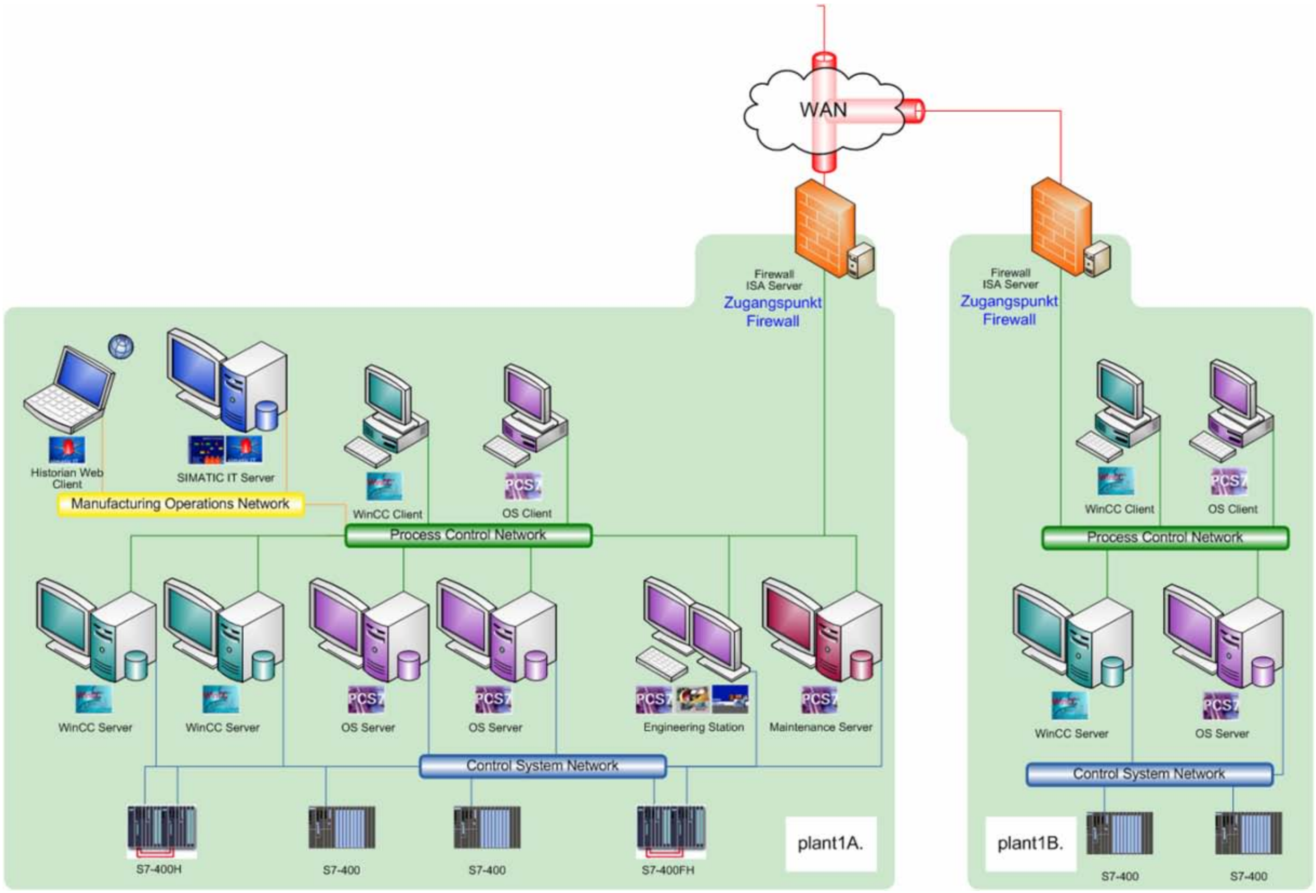

Figure 6-5

Figure 6-6 shows a security cell connection of the CSN implemented for "Industrial Ethernet" with SCALANCE S security modules. The communication between the automation systems specially developed for industrial application cannot be tunneled through a conventional IT firewall. On the one hand, the increased computer load for end-to-end encryption from automation systems would generally lead to decreased performance, and such an IT firewall would not sufficiently protect this communication on the other hand, since no filter rules are available for this. This task is assumed by the specially developed security modules of the SCALANCE S product series, which enable protected data communication of automation and process control system between the plant1A and plant1B units (Figure 6-6 below).

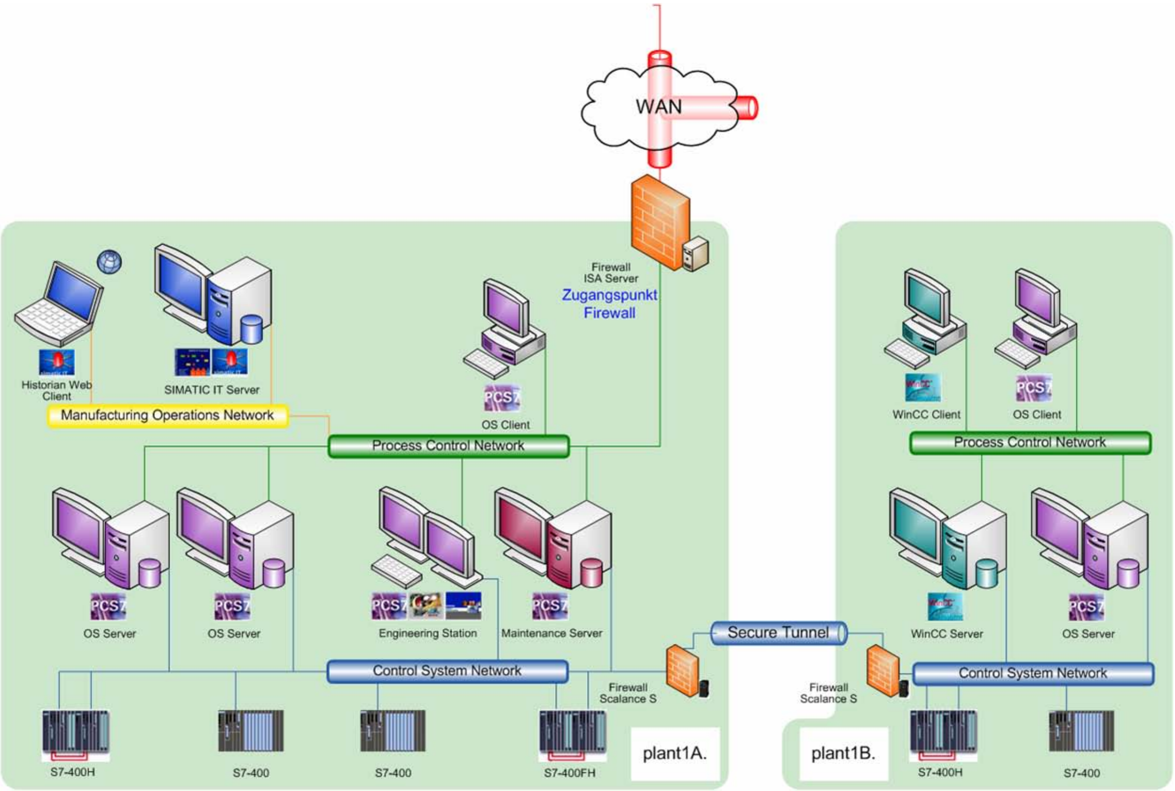

Figure 6-6

Additional information

You can find detailed information on this in the Internet at the following address: http://support.automation.siemens.com/WW/view/en/28580051

You can find additional information on the SIMATIC SCALANCE S product series here: http://www.automation.siemens.com/net/html_00/produkte/040_ind_sec.htm

6.2 Secure access techniques

Definition of access techniques

The implementation of the "defense in depth" security strategy involves specific access techniques depending on the access type and security cell design.

One of the following access types is described as the access technique in each of the examples below (see Sections 6.2.1 to 6.2.4):

- Data exchange / information exchange:
  Data exchange between various production levels, neighboring plants, onshore/offshore components, automation and security cells
  Access technique: **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.**
- Realtime controlling / remote controlling:
  Control or remote support of onshore to offshore or different plants or between the remote control center and the plant
  Access technique: Protected remote control through remote process control computer and remote engineering and **Fehler! Verweisquelle konnte nicht gefunden werden.**
- Maintenance:
  Monitoring and archiving of diagnostic information, data backups, updates or fine tuning of configurations
  Access technique: Secure integrated systems and **Fehler! Verweisquelle konnte nicht gefunden werden.**
- Support:
  All engineering activities, upgrades or changes of the process control system, as well as error diagnostics and correction
  Access technique: Protected service access
- Realtime data:
  Combination of "Data exchange" and "Realtime controlling"
  Access technique: **Fehler! Verweisquelle konnte nicht gefunden werden.** and Secure integrated systems

6.2.1 Secure Web publishing

One of the most modern and secure access techniques is Web publishing. This involves protecting the Web pages of the Web server in the perimeter against external attacks at the front-end firewall. The protection is made possible by the identity change to the published MS ISA server. The name and IP address of the respective Web server are thus not subjected to direct access. The front-end firewall functions as a "representative" of the Web server. The network topology and IP address of the perimeter are not visible to the external network. The dynamic status-based monitoring of the data traffic on the application level in combination with user-based application, command and data filters control each and every opening of a Web page.

For Web servers which require authentication and encryption for client access, MS ISA Server 2006 offers excellent security through filtering on the application level using SSL-to-SSL bridging. In contrast to most other firewalls, MS ISA Server 2006 can check encrypted data before it is forwarded to the respective Web server. The firewall decrypted the SSL data flow, performs a status-based check, encrypts the data again and forwards it to the published Web server.

The MS ISA server can authenticate users based on the local firewall or an Active Directory user database. In addition to the integrated Windows authentication, MS ISA Server 2006 also offers RSA SecurID, RADIUS, RADIUS-OTP, LDAP, Kerberos and form-based authentication for this. Especially the use of Remote Authentication Dial-in User Service (RADIUS) and the capability of delegating authentication requirements of the MS ISA Server 2006 within the framework of defense in depth offers an even better possibility of protecting the accounts and user management against direct access. With the "Kerberos Protocol Transition and Constrained Delegation", the authentication can even be performed for Kerberos servers not based on Microsoft.

The following information and network services of a production network can be made available to an external network via Web publishing, for example:

- Security update (e.g. Microsoft Windows Software Update Services Server)
- Certificate management (e.g. Microsoft Certification Authority, CA)
- Production data (e.g. SIMATIC PCS 7 OS Web Server)
- Production data (e.g. SIMATIC WinCC Web Navigator Server)
- Production data overview (e.g. SIMATIC WinCC Plant Intelligence, WinCC DataMonitor Server)
- Manufacturing control data (e.g. SIMATIC WinCC OPC XML DA Server)
- Diagnostic data (e.g. SIMATIC WinCC Scope (Diagnostics))

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

Additional information about provision, maintenance and support of
Microsoft ISA Server 2006 is available here:
http://www.microsoft.com/germany/technet/prodtechnol/isa/2006/library/default.mspx.

6.2.2 Secure integration of manufacturing control

Trusted clients or servers of manufacturing control (MES or IMS) without a direct process interface are integrated via encrypted communication (e.g. IPsec) in the security cell in the following cases:
When protocols and mechanisms are used for internal data exchange, which was developed for operation within local networks and domains (e.g. OPC/SQL/OLE/OLEDB/ODBC/DCOM).

The mutual authentication of encrypted communication is made via certificates. The authorization is made with Windows-based (e.g. DCOM) and application-specific access rights.

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.2.3 Protected service access

Support and remote dialup is gaining in importance due to the increasingly growing distances between support staff and plants requiring servicing (e.g. support personnel on land, the plant on a ship) and places high demands on the security solutions due to the additional potential security risks.

Firstly, more exceptions need to be defined at the access points (access point firewalls), and secondly, hostile code can be executed in the plant with administrative rights via a support PC - even unintentionally.

To ensure the highest possible security for the plant to be serviced, all access must be centrally authenticate and authorized at the access point firewall using a combination of several techniques and security mechanisms. "Direct dialup" to the device to be serviced offers verification options too weak to be taken into consideration.

Depending on the type of planned dialing - local or remote – and the service access, a variety of requirements and solutions emerge based on the expected risk.

Local dialup

Local dialup, physically within the plant, can only be made through a trusted device and through a trusted user. A special support station is used, for example a stationary engineering station (ES) in the plant or a mobile support PC from a member of the support staff. A stationary ES is secured by the same mechanisms as those used for all process control systems within the plant. If a mobile support PC is used, in contrast, it needs to be checked manually or via mechanisms. Such mechanisms include, for example, quarantine dialup and network access protection.

Remote dialup

The employed security techniques depend on specific risk with remote dialup. The following additional factors must be taken into consideration in comparison to local dialup:

- Type of dialing medium
- Type dialing device
- Purpose of the access
- Dialing medium
  - Point-to-point connections on layer 1-2 (e.g. ISDN, modem, serial) -> lower risk, since only specified devices can dial (depending on the technology)
  - Point-to-point connections on layer 3-4: (e.g. VPN, PPTP, L2TP) -> higher risk for the access point, since anyone (device or user) can be used to dial up a connection

- Dialing device
  - Specified support PC used only for this purpose -> lower risk, since the support PC, its configuration and its security level is known
  - Any, anonymous support PC-> very high risk, unknown security level
- Purpose of the access
  - Support for the process control system software -> little risk, since access only needs to be guaranteed for software which is usually proprietary
  - Support for the process control configuration -> little risk, since access only needs to be guaranteed for configuration data
  - Administrative access -> high risk, since this involves full access to complete systems
  - Access to devices in the CSN -> very high risk, since it is very difficult to restrict access to the process in the plant

Servicing access

Servicing access is made after dialup.
The following options are recommended based on specific roles:

- Remote servicing / remote engineering (VPN client with a service application)
- Remote desktop (VPN client with remote desktop for ES, OS or any, uniquely defined target system)
- Remote terminal (VPN client with access to terminal server and applications released for this purpose on the terminal client)
- Remote assistance (VPN client with NetMeeting for ES, OS or any, uniquely defined target system)

The authorization for servicing tasks is made via user name and password on the servicing software or on the terminal.

Summary

The resulting requirements on the access techniques and their protection in summary:

- All access should be made via a VPN connection with quarantine dialup at the firewall. The questions to be answered, depending on the degree of risk, are how to secure this connection (e.g. encryption level) and which criteria to apply in the quarantine test.
- The authentication for the VPN dialup is made with user name and password at the firewall. The firewall verifies this logon via Radius or Kerberos on the logon server (e.g. domain controller) or in the local user management.
- If the access is made with a specified support PC via the software of the process control system, the support PC connected via VPN can be secured like a remote process control computer.
- If administrative access or even access to the CSN is required, it can only be performed via Remote Desktop, NetMeeting or remote support to the selected plant PCs and the stationary ES.

Which of the above-mentioned accesses is allowed for a given user, is decided by the ISA server based on the user name entered for establishing the VPN tunnel.

Additional information

You can find detailed information on this in the Internet at the following address: http://support.automation.siemens.com/WW/view/en/28580051

6.2.4 Protected remote control through remote process control computer and remote engineering

Remote control and remote engineering of a plant place very high demands on the security concept which is to be implemented. Misuse can result in a great deal of damage.
In general, there is a difference between trusted devices and non-trusted devices.

- Trusted devices are those under the control of a plant manager and administered by him. Remote, trusted computers of the process control systems (clients, servers and engineering stations) without direct process interface, are integrated via encrypted communication in the security cell.
  - The mutual authentication of the encrypted communication is made via certificates (e.g. Windows IPSec or upstream SCALANCE S security modules).
  - The authorization is made with Windows-based (e.g. DCOM) and application-specific access rights.
- Non-trusted devices are those temporarily integrated in the plant, even if they are being used by a trusted person. These devices can be given user-based access to Web publications of the process control system. Access is made via perimeter techniques through the front-end firewall.
  - The authentication takes place through server-end encryption (e.g. HTTPS) using user name and password.
  - The authorization is made with Windows-based and Web application-specific access rights.

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.2.5 Secure integrated systems

Secure integration of auxiliary systems with additional or parallel access to the process is explained using an example of the "Process Information Management and Acquisition" system (PIMAQ). Since access of the PIMAQ system is made simultaneously to the control of the process control system, the PIMAQ system must be connected in the following way in order to realize the strategies of this security concept:

1. The PIMAQ communication server with direct access to the automation systems in the CSN should be placed in the PCN.
2. The PIMAQ server in the perimeter and the PIMAQ communication server in the PCN are connected through a certificate-based IPSec tunnel via the back-end firewall in such a way that enables the back-end firewall to detect the correct configuration of the tunnel (including the mutual authentication of the nodes in the VPN).
3. The PIMAQ server permanently provides the collected and archived data for the PIMAQ Web clients or the IP21Explorer clients in the ECN (the office network or Intranet). The Web server of the PIMAQ server is published via the front-end firewall in the ECN for this.

The following options are available for the authentication of the remote clients of this auxiliary systems:

- Authentication through firewall client software installed at the client end, which logs on users at the firewall and subsequently allows access to the server.
- Authentication on the servers and Web servers of these systems, based on application-specific access rights. This authentication is documented by and the responsibility of the respective manufacturer.

Clients or servers of auxiliary systems with very high communication load must be operated within the security cell to prevent the firewall from blocking the data flow.

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.3 Hardening

For SIMATIC PCS 7 and SIMATIC WinCC, hardening means deactivating or restricting functions and programs that are not required for the operation of the computer within the plant environment.

Potential security threats can only be effectively limited if each and every member of the security cell is hardened.

The following measures are required for hardening:

- Disabling / removal of unneeded services
- Use of a firewall to restrict the external availability of services which are only needed locally
- Use of a firewall to restrict the external availability of services to defined network addresses or protocols and which are only needed by specifically known network devices or external application
- Restriction of the availability of services to those needed by specifically known devices or users using an exactly defined access permission via the local security system (e.g. the COM-/DCOM security configuration) of the component service administration
- Restriction of local and remote file, registry, sharing and database access to specific and known local groups, users, services and applications

SIMATIC Security Control

SIMATIC Security Control is a program that can perform application-specific hardening of a computer in a local IP subnet. SIMATIC Security Control is integrated by default in SIMATIC PCS 7 and SIMATIC WinCC.

The option enabling SIMATIC Security Control to automatically perform the settings for hardening must be explicitly confirmed when the program is installed.

The communication to non-configured devices or to other subnets, as well as the use of non-configured users is not possible or extremely restricted.

Note the following when changing the plant configuration or changing the role of users:
The local firewall configuration or the local group membership needs to be adapted.

Local group memberships

The rights required for operation is preconfigured to special local "SIMATIC" Windows groups by the setup routine of the individual SIMATIC products. Newly created users must be made a member of at least these local "SIMATIC" Windows groups if they are to use these products.
Additional membership in the normal Windows groups (e.g. Power users, Users) is required for local operation. Any required local membership in the normal Windows groups is described in the respective product documentation.

Component service security (COM & DCOM)

The required rights for local and remote access to administrative objects and programming interfaces of the Windows COM components, COM+ and DCOM applications are preconfigured to special local "SIMATIC" Windows groups at the end of the setup routine for the SIMATIC products.

Local Windows firewall

If you do not want to operate SIMATIC products within a local IP subnet, you need to adapt the settings of the local Windows firewall for the devices involved to the IP subnets or individual IP addresses used.

IPSec Bypass Technology

The use of "IPSec Bypass Technology" represents a special measure. The use of local IPSec filter rules makes it possible to establish IPSec-protected communication to another computer without special configuration of the local Windows firewall. This communication connection requires either Kerberos authentication and there membership in an Active Directory domain of the computer involved or specially provided certificate.

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.4 Management and configuration

6.4.1 Managing computers and users

The management of computers and users in a production plant can be organized centrally through a Windows domain (Active Directory domain) or distributed in Windows workgroups.

Mixed configurations of central and distributed management are also generally possible. Required mixed configurations should be specifically adapted for each plant. Experience shows that incorrect configurations occur more often with distributed configured components and conflicting settings are hard to find in such cases.

One advantage of central management is the importance of reduced maintenance efforts and the substantially higher security achieved, for example, by using domain internal Kerberos authentication instead of NTLM authentication within a workgroup.

The decision to use distributed or central management should be made based on the number systems to be maintained or the necessity (e.g. company security policies) of using an Active Directory domain.

An Active Directory domain always creates the following requirements:

- Redundant user management
- Use of Kerberos authentication
- Public key infrastructure (can also be used for IPSec)
- Central "single sign-on" user logon and verification
- Central user logon and verification from an "foreign" domain (e.g. via a "one-sided trust" to another network with its own Active Directory management)
- Central group policy based configuration e.g.
  - Distribution of security updates
  - IPSec bypass technology
  - Software installations
  - Group memberships

Regardless of the type of management (distributed or central), the responsibility and management areas of the IT department in the office network and the plant operating personnel must be carefully defined.
The following examples clarify the importance of defining the areas of responsibility and management:

- An administrator of the IT department cannot inadvertently reboot the plant PC or configure it incorrectly.
- An administrator of the plant operator personnel cannot inadvertently change the domain settings of foreign domains.

If management is to be performed through a domain, an administration plan must always be developed. The administration plan defines the design of the infrastructure including the name space, domains structure, forest and trusts for other domains, e.g. the office domain. The decision about the infrastructure design strongly depends on the number of plants, the size of the plants and the amount of work associated with them. The company policies must also be taken into consideration and implemented as well.

In general, segregated forests are recommended for the office networks and production networks, since the protection of data, permissions and rights are made separately for both forests, as is the directory replication. Only organizational changes, configuration changes and adding new domains to the forest have an effect throughout the forest. Access to resources is enabled by one-way or two-way trusts for the forest. Since each forest (office and production) is managed separately, adding a forest increases the management expenditure considerably. Forest trusts facilitate the management of a segmented Active Directory infrastructure within a company, in that it supports cross-forest access to resources and other objects.

The appendix provides a figure which offers an example of three different management scenarios:

- Scenario 1 shows two independent forests for the business and production layers, connected by a bidirectional transitive forest trust
- Scenario 2 shows two independent forests for the business and production layers, connected only by actually needed unidirectional intransitive trusts between the production domain and individual department domains of the business layer
- Scenario 3 shows a forest for the business layer and the domain forest below it for a dependent production domain

Additional information

You can find detailed information on this in the Internet at the following address: http://support.automation.siemens.com/WW/view/en/28580051

You can find additional information on the topic "Creating a new forest" here: http://technet2.microsoft.com/windowsserver/en/library/31ce4349-7046-496a-a3cf-a8b49f7dbb5e1031.mspx

You can find additional information about cross-forest access to resources in several forests here: http://technet2.microsoft.com/windowsserver/en/library/517b4fa4-5266-419c-9791-6fb56fabb85e1031.mspx

6.4.2 Managing networks and network services

The management of the local network settings, the networks and required network services of a production plant can be organized distributed or centrally.

Mixed configurations of central and distributed management are also generally possible. Required mixed configurations should be specifically adapted for each plant. Experience shows that incorrect configurations occur more often with distributed configured components and conflicting settings are hard to find in such cases.

One advantage of central management is the importance of reduced maintenance expenditures and the substantially higher security achieved, for example by the following options:

- Use of domain internal Kerberos authentication instead of NTLM authentication within a workgroup
- Automatic DNS registration when using a DHCP-DNS server network

The decision to use distributed or central management should be made based on the number systems to be maintained or the necessity of using central management.

The necessity of an Active Directory domain is described in more detail in the section "Managing computers and users".

Central management (usually domains)

All required information and settings can be configured centrally:

- IP address via DHCP (automatic address assignment)
- Name resolution DNS, WINS (automatic, central name registration, can be subsequently queried by other network nodes)
- Time synchronization (NTP, SNTP)

Distributed management (usually workgroups)

All required information and settings must be configured locally.

Be aware that the following settings are often the source of errors in complex plants, since typographical errors or duplicate entries easily occur:

- IP address (serves to uniquely identify a network node in a network)
- Computer name and NetBIOS computer name (serves to uniquely identify a computer for persons and applications in the network)
- Name resolution (used to convert the computer name (FQDN) and NetBIOS computer name of a computer into an IP address)

Additional information

You can find detailed information on this in the Internet at the following address: http://support.automation.siemens.com/WW/view/en/28580051

You can find additional information about the topic of "PCS 7 Time Synchronization" at the following addresses:

http://support.automation.siemens.com/WW/view/en/28518882 and http://support.automation.siemens.com/WW/view/en/27236051

6.4.3 Managing role-based operator control permissions

The unique identification of persons and the assignment of permissions to these persons belong to the most important security measures of every company.

The following describes the special consideration for automation in regard to the management of role-based operator control permissions and their integration in the security concept of PCS 7 and WinCC.

Difference between a user and an operator

A difference is made at logon to a process control computer between logging on to the operating system by a user and logging on to the process control system by the operator. The user has the right to use or administer specific applications of the process control system; within these applications (e.g. WinCC Runtime) the operator has the operator control permissions to perform operations in the automation plant and thereby control the process. The minimal principle is applied for assigning all rights and permissions. This means that users and operators receive only those rights that are required to fulfill their jobs.

Automatic logon of the user

The permanent graphic display of the runtime and the operator control is in the foreground for visualization in process control systems. The operator logs off from the software of the process control system and usually does not close the graphic display. This is in contrast to the logoff of a user, who started the software of the process control system. Automatic logon of a user can be configured for specific products (e.g. for SIMATIC WinCC) to end the graphic display and prevent unauthorized start of applications by the operating personnel. The user used for this does not correspond to a real person, it is a representative of the process control system software and a product-specific system account (e.g. with SIMATIC WinCC this product-specific system account is a member of the SIMATIC HMI group).

The product-specific system account is not a system account of the operating system.

Rights management of the user

The rights management of users in the Windows operating system is realized according to the strategies recommended by Microsoft. SIMATIC Security Control creates the required SIMATIC groups during the installation of a SIMATIC product (e.g. WinCC), the members of which can start and use this product.
The administrator organizes the users with the same job into groups. The administrator creates a user account for such a user and enters the user in the available SIMATIC groups. This allows the user to use the software.

Rights management of the operator

Operator management and its role assignment is configured via SIMATIC Logon and the configuration dialogs of the individual components (e.g. SIMATIC WinCC: "WinCC UserAdministrator"). SIMATIC Logon consists of the following components:

- SIMATIC Logon Service:

  Central access protection for SIMATIC applications and plant areas

- SIMATIC Logon Role Management:

  Role management for applications and their assignment to Windows groups including assignment of permissions

- SIMATIC Electronic Signature:

  Creation of electronic signatures for state transitions in the process and for accessing the process

- SIMATIC Logon Event Log Viewer:

  Takes on the task of recording and displaying events for an application

  The basic idea of SIMATIC Logon is the central availability of the logon information ("single sign-on" principle) for the operator. The tried-and-proven security mechanisms of the Window logon and user management is used for this purpose. Name, logon name and password (identity) of the operator are stored as a Windows user account in the Windows domain (or in the local user database) and are made available for authentication of an operator via the SIMATIC Logon Service. The role-based operator control permissions are configured through the operator's membership to Window groups of the same name.

Logon via SIMATIC Logon Service

SIMATIC Logon Service is the basis of SIMATIC Logon. Figure 6-7 shows the process that runs automatically when a user wants to log on for an application (e.g. SIMATIC WinCC), if SIMATIC Logon is integrated in the application.
The user logs on and off for the application exclusively through the SIMATIC Logon Service.

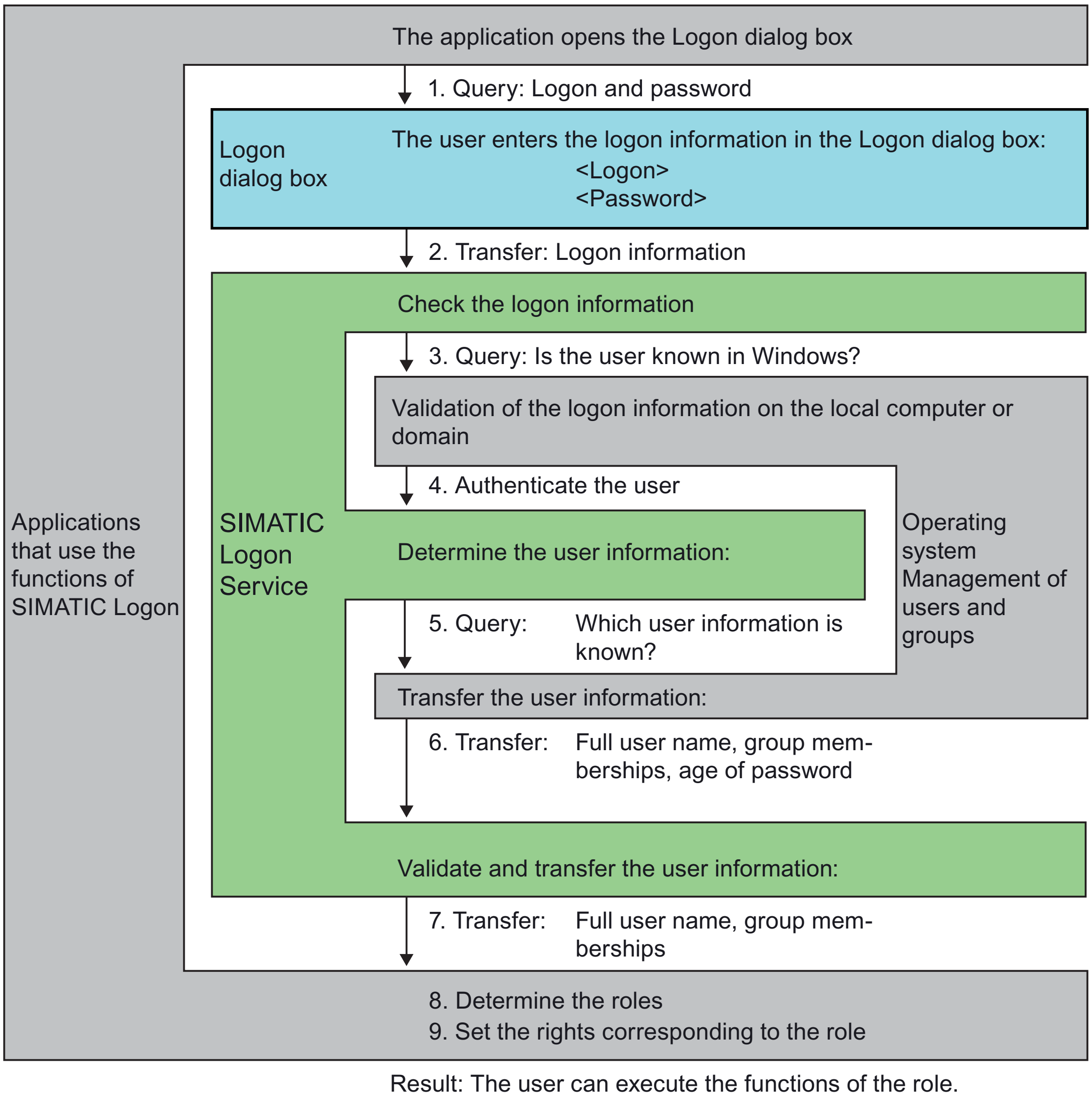
The application opens the Logon dialog box
1. Query: Logon and password
Logon dialog box
The user enters the logon information in the Logon dialog box:
<Logon>
<Password>
2. Transfer: Logon information
Check the logon information
3. Query: Is the user known in Windows?
Validation of the logon information on the local computer or domain
4. Authenticate the user
Applications that use the functions of SIMATIC Logon
SIMATIC Logon Service
Determine the user information:
Operating system Management of users and groups
5. Query: Which user information is known?
Transfer the user information:
6. Transfer: Full user name, group memberships, age of password
Validate and transfer the user information:
7. Transfer: Full user name, group memberships
8. Determine the roles
9. Set the rights corresponding to the role
Result: The user can execute the functions of the role.

Figure 6-7

Central and fail-safe rights management with SIMATIC Logon

The use of SIMATIC Logon in combination with an Active Directory domain enables fault-tolerant and fail-safe authentication (and logon) of operators, if at least two domain controllers are realized in each domain and security cell.

Local domain user accounts of the production domain are used to configure operators. Selected user accounts can also be assigned access rights through trust-linked office domains.

In addition to central operator management with SIMATIC Logon, a local emergency operator permission must be created in case the SIMATIC Logon Service cannot be reached due to complete network failure.

Distributed rights management without SIMATIC Logon

Operator permission management for a specific SIMATIC application (e.g. WinCC Useradministrator) can also be made fully local, although this is not recommended due to security reasons.

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.5 Patch management and security updates

Patch management is a regular procedure for installing patches on plant computers. The following questions need to be answered during the planning:

- Which patches are to be installed?
- When are patches to be installed?
- In what order are patches to be installed?
- What method should be used to install these patches on the plant computers?

Patch management for a plant is only effective when they are part of a comprehensive security concept. Patch management and security updates alone generally cannot protect a plant against security threats.

Patch and security updates

- Patch
  The term patch for Microsoft means all types of updates, service packs, feature packs and similar installations, regardless as to whether or not these relate to security.
- Security updates
  The term security update, in contrast, is exclusively security-related.

Using path management

Patch management should never inhibit runtime operation of a plant. The following configuration have been tested and are recommended to ensure this:

- Central patch management
  Patch management should be performed centrally for reasons of management but also for technical security reasons (not every computer downloads its patches from Microsoft; a server, preferably located in a perimeter network, centrally downloads the patches once and then distributes them to the plant computers).
  The plant administrator is therefore provided centralized configuration and monitoring and the plant computers require no Internet access. The patch server, located in a perimeter network separated by a firewall, accesses the Internet, device or a higher-level patch server in the Intranet.
- Windows Server Update Service (WSUS)
  WSUS is recommended for central patch management. It is provided free-of-charge by Microsoft and offers all the functions required for patch management.
  WSUS offers a variety of different patch classes for almost all Microsoft products.

- **Update classes**
  The introduction of WSUS and the further development of Windows Update to Microsoft Update (patches for numerous Microsoft products) has created new classifications for the individual patches:
  - Definition updates
  - Feature packs
  - Service packs
  - Security updates
  - Tools
  - Drivers
  - Update rollups
  - Critical updates
  - Updates

The following updates are important for safe and stable plant operation:

- **Security updates:** Corrects errors that can be used to attack the system. This is why it is important to install security updates as quickly as possible.
- **Critical updates:** Corrects errors in the software, for example, display errors, errors leading to increased processor load, or errors that result in failure of the operating system. Critical updates should therefore be installed at regular intervals.

These two update classes are subjected to a compatibility test for specific versions of each SIMATIC product and rated as compatible when the test is completed successfully. A list of tested patches is permanently available in the Internet. You can find information on this at the end of this section.

Patching the systems is not used as the only security measure to protect a plant or the enterprise network. The realization of defense in depth (application of all security techniques described in this security concept) means a potential attacker must first overcome multiple security barriers before he might exploit weak points from a lacking security update. This protection gives you more time to evaluate and test patches to be installed.

Procedure for path management

Since maintaining control over the process is the most important rule, the installation time for the patches must be specifically selected by the administrator. Firstly, many patches require the system to be rebooted; secondly patches may create problems, although this seldom occurs. It is therefore recommended to test the patches beforehand on a separate test system. In addition, you should form groups (for example, one group with all master servers and one with all standby servers) and install the patches group-by-group.

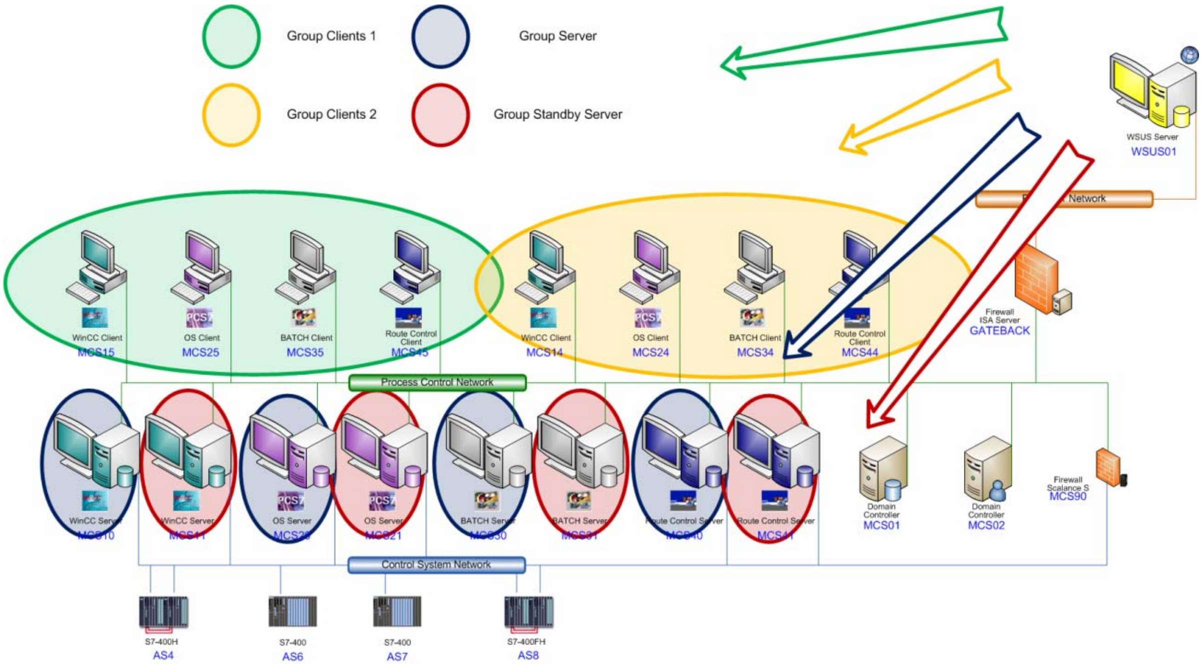

Figure 6-8

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

Information on the topic: "What is the procedure for implementing Microsoft Security Patches in SIMATIC WinCC?" can be found here:
http://support.automation.siemens.com/WW/view/en/18752994

Information on the topic: "What is the procedure for implementing Microsoft Security Patches in SIMATIC PCS 7?" can be found here:
http://support.automation.siemens.com/WW/view/en/18490004

6.6 Virus scanners

Using virus scanners in a plant is only effective when they are part of a comprehensive security concept. A virus scanner alone generally cannot protect a plant against security threats.

Definitions

- Virus scanner client
  Computer which is examined for viruses and managed by the virus server.
- Virus scanner server
  Computer which centrally manages virus scanner clients, loads virus signature files and deploys them on the virus scanner clients.

Using virus scanners

The use of a virus scanner should never inhibit runtime of a plant. Ultimately, this means that even a virus infected computer should not be shutdown immediately, if this results in losing control of the production process. A virus scanner should therefore fulfill the following requirements for application in industrial control components (IACS):

- The virus scanner must be installable without its own firewall if a local firewall adapted to runtime is to be used.
- The virus scanner clients can be divided into (product-specific and tasks-specific) groups and configured separately.
- It must be possible to disable automatic distribution of virus signatures and other updates.
- It must be possible to distribute virus signatures and other updates manually and group-by-group.
- It must be possible to scan files and the system manually and group-by-group.
- If a virus is detected, it should be possible to configure a message without having to automatically perform a file action such as "Delete", "Wipe" etc.
- All messages must be logged on the virus scanner server.
- It should be possible to suppress the local message window on a virus scanner client, since it may hide important process control messages.

Note

The installation of software is often a process that represents a serious and complicated change to the system involved. The storage location of the files to be installed must always be free of viruses (e.g. a file server with its own virus scanner or a DVD that has been scanned for viruses). A virus scanner may not unnecessarily inhibit or corrupt the installation; it should therefore be possible to completely deactivate it during installation if problems occur.

Basic virus scanner architecture

The following section recommends a virus scanner architecture for the implementation of the requirements described above.

A virus scan server receives its virus signatures from the update server of the respective virus scan manufacturer in the Internet or from an upstream virus scan server and manages its virus scan clients.

Additional administrative access to the virus scanner server is possible via a Web console.

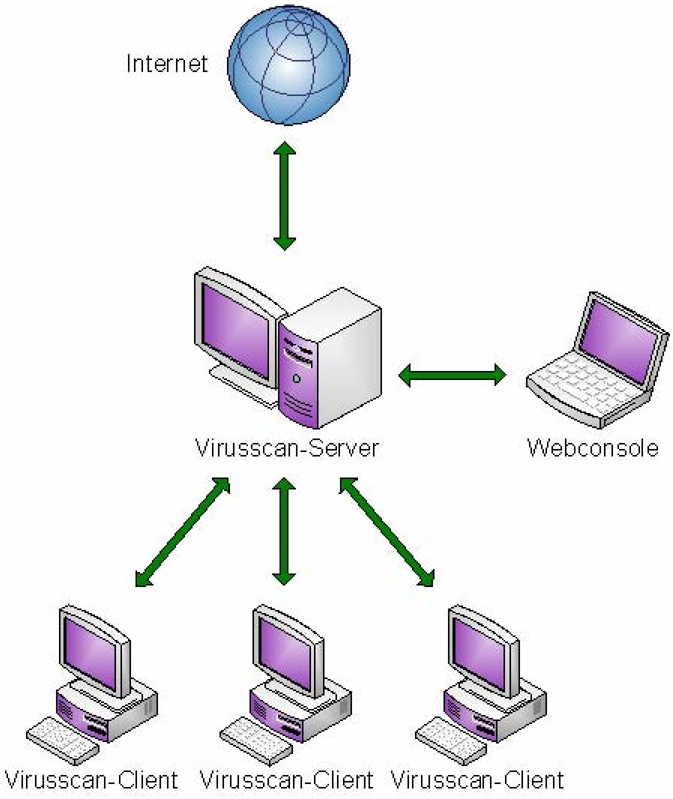

Figure 6-9

Several virus scanner servers can be used, depending on the manufacturer. They can be arranged in a hierarchy.

Once the virus scanner server has obtained the virus signatures and checked them in a test plant, the virus signatures are distributed group-by-group to the virus scanner clients. Four groups have been created in the following figure, for example. More or fewer groups can be created, depending on the requirements of the plant. However, there should always be at least two groups.

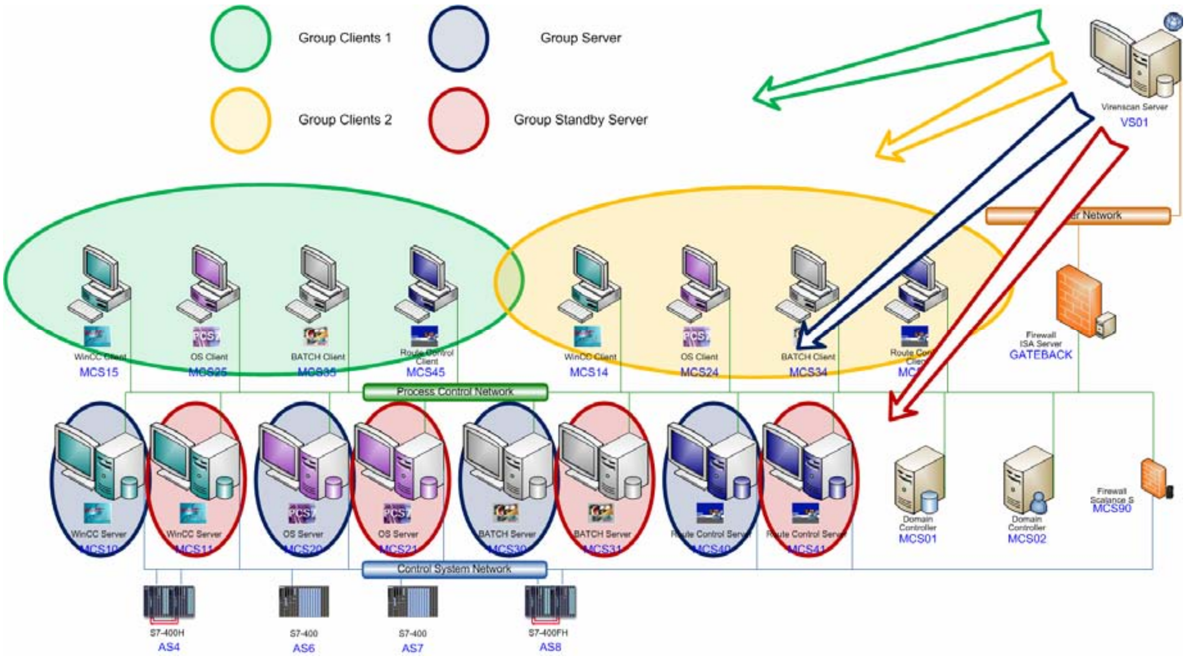

Figure 6-10

Additional information

You can find detailed information on this in the Internet at the following address: http://support.automation.siemens.com/WW/view/en/28580051

6.7 Logging, audit, maintenance and asset management

The capability of detecting attempted and actual security threats is rapidly developing. Due to the requirements for verification in many branches, more and more functions, such as reporting and event log evaluation, must be included in current security concepts. Runtime must still continue without interference in spite of the additional load, however.

The following reporting can be configured and evaluated as needed, in addition to the alarm and messaging systems of process control for example:

- Local event logs
- Domain controller event logs
- Firewall event logs
- Virus scanner logs
- Audit trail

Asset management in plant engineering involves the management of equipment, activities and measures that are employed to maintain or increase the value of the plant.

Asset management is a very sensitive subject in the field of security engineering, since this data also presents a weak point in a plant. In general, asset management and its administrative rights should be restricted to the functional area within the plant's security cell. The procedures described in "Secure access techniques" section can be used to publish maintenance data beyond the borders of the security cell. This reliably prevents direct access from the outside – for example, to sensors or actuators on the field level.

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

6.8 Security tests

To keep a plant security up-to-date, previously implemented security measures must be tested at regular intervals, and updated and supplemented if needed. This is necessary because the rapidly developing technology creates new security requirements on the one hand, and new threats are arising all the time on the other.

Network administrators can employ so-called "Security scanner" automated tests on target systems. Security scanners rely on special databases, for example those of the SANS Institute (SysAdmin, Networking and Security). They provide you with a list the latest known and widespread security gaps, for example, the CVE list (Common Vulnerabilities and Exposures). Security scanners check for known vulnerabilities on the examined system.

Security scans are basically divided into two categories:

- Blackbox scan
- Whitebox scan

Blackbox scan

A blackbox scan checks a given system for security vulnerabilities from the point of view of the attacker, who has no internal information about the system. The system is considered a closed unit in a blackbox scan, i.e. neither the configuration nor the network structure of the target system is known.
In a blackbox scan, the vulnerabilities identified from the outside are recognized as points of attack (e.g. open ports, available services, etc.). Any additional opportunities for attack offered to the hacker by the system once these vulnerabilities have been exploited remains open.

Whitebox scan

In contrast to a blackbox scan, a whitebox scan relies on internal system information. Here too, a given system is examined for weaknesses, but this time from the point of view of an administrator. A whitebox scan (also referred to a glass box scan) examines the individual components of the system and their interaction, and determines the configuration critical for security as needed.
The whitebox scan also detects dangers, arising from outdated versions of user software, for example, or from neglected user account management.

Microsoft Baseline Security Analyzer (MBSA)

The MBSA tool is recommended for Whitebox scans in this security concept. It can be used for the following purposes:

- Searching one or more computer for vulnerabilities, from poor user management for example
- Determination of the availability of security updates for one or more computers

Penetration tests

Penetration test tools are special security scanners. Penetration tests are performed with the resources and methods that an hacker would use to gain unauthorized access to the system.

Notice

A running process control plant should never be checked with penetration test tools! The use of penetration test tools is always associated with the risk of permanent damage to the tested system (or the installation or configuration of the system).

The use of security scanners in the Whitebox Scan or the service period (plant stoppage) must be supported by the manufacturer for each product; this may need to be assured beforehand!

Additional tools can be used, for example, for security tests in laboratory environments:

- Port scanner
- Network/OS vulnerability scanner
- Application/database vulnerability scanner
- Password cracker (attention, first check current legal regulations!)
- File search and analysis tool
- Network analyzer
- Exploit tool

Additional information

You can find detailed information on this in the Internet at the following address:
http://support.automation.siemens.com/WW/view/en/28580051

7 Appendix

Norms and standards

Since the ISA-99 series is currently one of the most important security standard for protecting industrial automation plants, the following is a excerpt (marked in blue) from ISA-99.00.01 – Part 1, which itself describes the structure of the new standards:

- ISA-99.00.01 – Part 1: Scope, Concepts, Models and Terminology

  Part 1 (this standard) establishes the context for all of the remaining standards in the series. by defining a common set of terminology, concepts and models for electronic security in the industrial automation and control systems environment.

- ISA-99.00.02 – Part 2: Establishing a Manufacturing and Control Systems Security Program

  Part 2 will describe the elements of a cyber security management system and provide guidance for their application to industrial automation and control systems. This part also provides detailed support in relation to process activities and key elements for developing a management system for cyber security.

- ISA-99.00.03 – Part 3: Operating a Manufacturing and Control Systems Security Program

  Part 3 will address how to operate a security program after it is designed and implemented. This includes definition and application of metrics to measure program effectiveness.

- ISA-99.00.04 – Part 4: Specific Security Requirements for Manufacturing and Control Systems

  Part 4 defines the characteristics of industrial automation and control systems, which distinguish themselves from other IT systems based on the security aspect. Based on these distinguishing characteristics, the standard clarifies the specific security requirements for this category of systems.

Beyond this, the ISA-99 committee has presented to date two technical reports on the topic of electronic safety in the field of industrial automation and control systems.

- **ANSI/ISA-TR-99.00.01-2004 – Security Technologies for Manufacturing and Control Systems**

  Technical Report 1 describes various security technologies in regard to their application in industrial automation and control systems. This report will be updated in the future to take changes in the technology into consideration.

- **ANSI/ISA-TR-99.00.02-2004 – Integrating Electronic Security into the Manufacturing and Control Systems Environment**

  Technical Report 2 describes how electronic security can be integrated in industrial automation and control systems. The content of this report will be replaced by this standard upon the conclusion of the standards in Part 2.

Names in the figures

The following divisions of the DNS name spaces facilitate the assignments in the demo plant:

- enterprise.com
  Complete **external** name space of the company for remote access and Web publishing in the Internet
- enterprise.local
  Complete **internal** name space of the company (Intranet)

  department1.enterprise.local
  Intranet name space for the **enterprise layer** (office network) of department 1 responsible for production area 1
- manufacturing-execution1.production1.enterprise.local
  Internal name space of the **manufacturing control** of plant 1
- production1.enterprise.local
  Complete internal name space of the **process control** of plant 1
- plant1A.production1.enterprise.local or plant1B. production1.enterprise.local
  Internal name space of the **process control unit** 1A (basically, plant1B for unit 1B etc.)
- perimeter1.production1.enterprise.local
  Internal name space of the **perimeter network** of plant 1 (is also used in this way for publishing in the Intranet)
- production1.enterprise.com
  External (e.g. in Internet) **published** name space of the perimeter network of plant 1

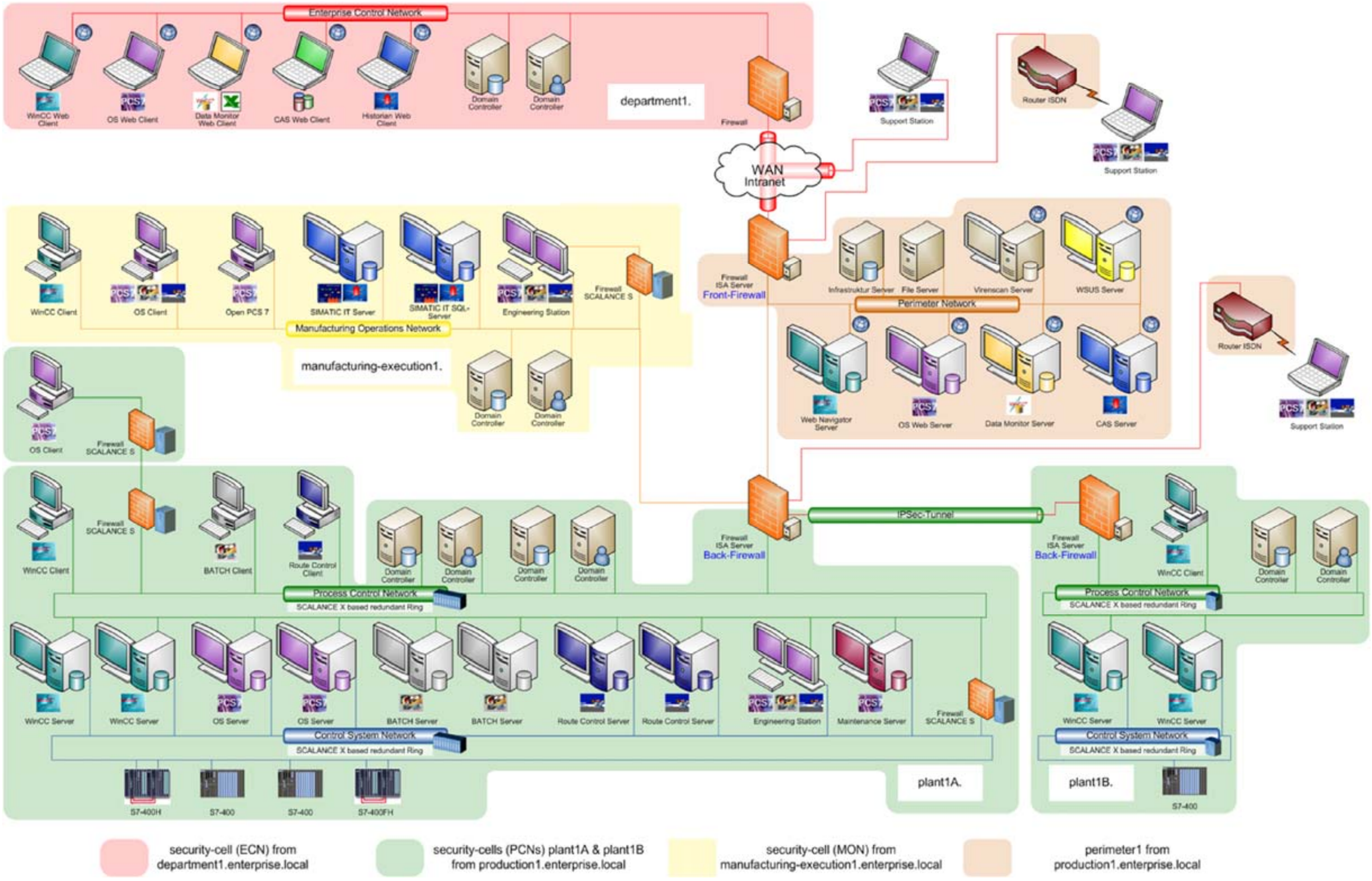

Figure 7-1 Basic design of the demo plant

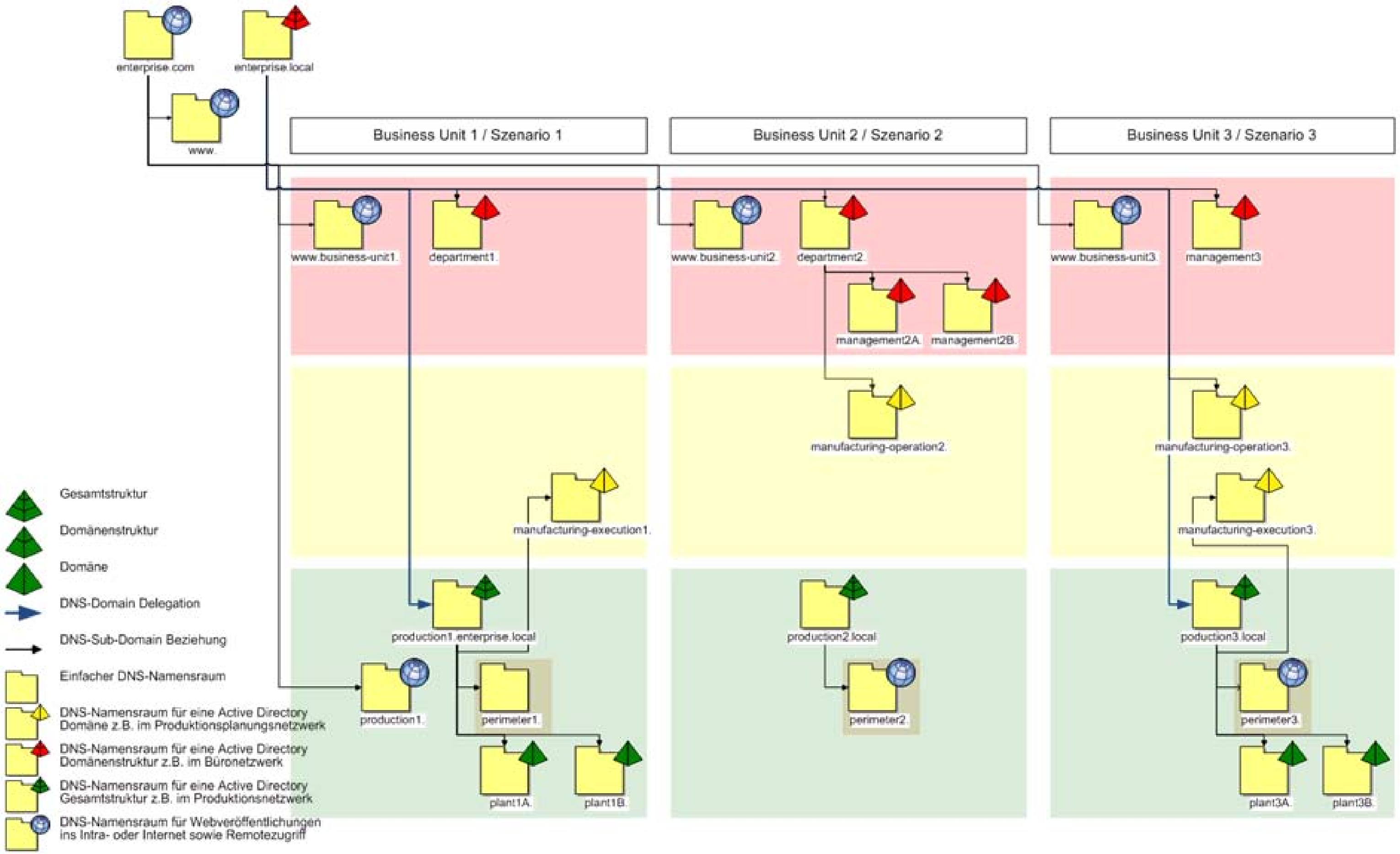
enterprise.com
enterprise.local
www.
Business Unit 1 / Szenario 1
Business Unit 2 / Szenario 2
Business Unit 3 / Szenario 3
www.business-unit1.
department1.
www.business-unit2.
department2.
www.business-unit3.
management3
management2A.
management2B.
manufacturing-operation2.
manufacturing-operation3.
manufacturing-execution1.
manufacturing-execution3.
production1.enterprise.local
production2.local
poduction3.local
production1.
perimeter1.
perimeter2
perimeter3.
plant1A.
plant1B.
plant3A.
plant3B.
Gesamtstruktur
Domänenstruktur
Domäne
DNS-Domain Delegation
DNS-Sub-Domain Beziehung
Einfacher DNS-Namensraum
DNS-Namensraum für eine Active Directory Domäne z.B. im Produktionsplanungsnetzwerk
DNS-Namensraum für eine Active Directory Domänenstruktur z.B. im Büronetzwerk
DNS-Namensraum für eine Active Directory Gesamtstruktur z.B. im Produktionsnetzwerk
DNS-Namensraum für Webveröffentlichungen ins Intra- oder Internet sowie Remotezugriff

Figure 7-2: Basic DNS name space of the demo plant

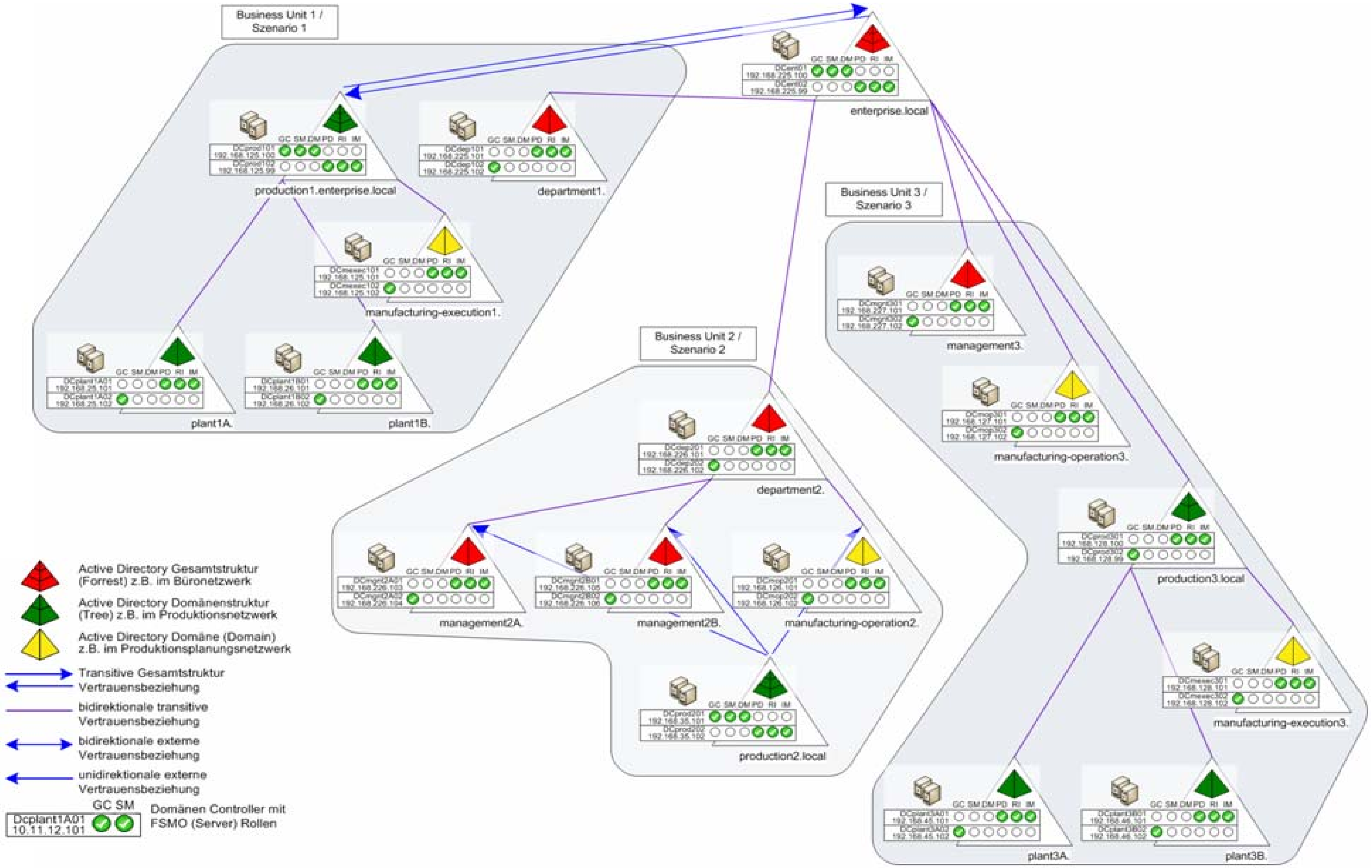
Business Unit 1 / Szenario 1
Business Unit 2 / Szenario 2
Business Unit 3 / Szenario 3
GC SM DM PD RI IM
DCent01 192.168.225.100
DCent02 192.168.225.99
enterprise.local
DCprod101 192.168.125.100
DCprod102 192.168.125.99
production1.enterprise.local
DCdep101 192.168.225.101
DCdep102 192.168.225.102
department1.
DCmexec101 192.168.125.101
DCmexec102 192.168.125.102
manufacturing-execution1.
DCplant1A01 192.168.25.101
DCplant1A02 192.168.25.102
plant1A.
DCplant1B01 192.168.26.101
DCplant1B02 192.168.26.102
plant1B.
DCdep201 192.168.226.101
DCdep202 192.168.226.102
department2.
DCmgnt2A01 192.168.226.103
DCmgnt2A02 192.168.226.104
management2A.
DCmgnt2B01 192.168.226.105
DCmgnt2B02 192.168.226.106
management2B.
DCmop201 192.168.126.101
DCmop202 192.168.126.102
manufacturing-operation2.
DCprod201 192.168.35.101
DCprod202 192.168.35.102
production2.local
DCmgnt301 192.168.227.101
DCmgnt302 192.168.227.102
management3.
DCmop301 192.168.127.101
DCmop302 192.168.127.102
manufacturing-operation3.
DCprod301 192.168.128.100
DCprod302 192.168.128.99
production3.local
DCmexec301 192.168.128.101
DCmexec302 192.168.128.102
manufacturing-execution3.
DCplant3A01 192.168.45.101
DCplant3A02 192.168.45.102
plant3A.
DCplant3B01 192.168.46.101
DCplant3B02 192.168.46.102
plant3B.
Active Directory Gesamtstruktur (Forrest) z.B. im Büronetzwerk
Active Directory Domänenstruktur (Tree) z.B. im Produktionsnetzwerk
Active Directory Domäne (Domain) z.B. im Produktionsplanungsnetzwerk
Transitive Gesamtstruktur Vertrauensbeziehung
bidirektionale transitive Vertrauensbeziehung
bidirektionale externe Vertrauensbeziehung
unidirektionale externe Vertrauensbeziehung
GC SM
Dcplant1A01 10.11.12.101
Domänen Controller mit FSMO (Server) Rollen

Figure 7-3: Basic design of the domain management in the demo plant