SIEMENS
Ingenuity for life

Industrial Communication

SINEMA Server –

Making your network transparent

Brochure

Edition
04/2018

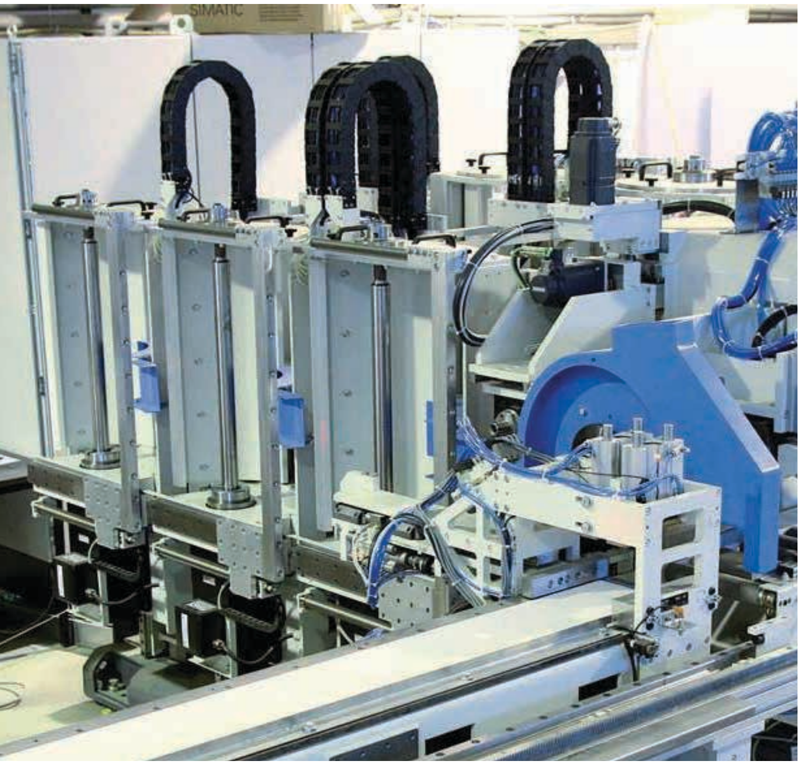
usa.siemens.com/ie

SINEMA Server – for transparent networks

Industrial communication networks lay the foundations for digitalization in modern businesses. Having complete information about the status of a network is indispensable for the reliable and company-wide exchange of data. SINEMA Server network management software enables you to accurately monitor your network for transparent diagnostics.

By 2020, up to 15 billion communication-capable machines will be connected in the industrial Internet of Things (IoT). This enormous number of machines and systems must be able to be visualized and diagnosed in order to have a comprehensive overview of the network data. This makes performing diagnostics a lot easier, especially when faults occur, meaning that system and network downtimes can be minimized.

With a suitable network management software, such as SINEMA Server from Siemens, problems can be detected early and appropriate measures implemented in good time. SINEMA Server is suitable e.g. for discrete manufacturing applications as well as for the process industry.



Even a single failure in the network during operation can result in a rush of alarms.
The combination of topology know-how with the diagnostics values of individual network nodes (including SIMATIC and PROFINET diagnostics) is decisive when it comes to rapidly localizing and eliminating the cause of a network fault. A complete physical map of the network permits analysis of the possible effects of cable or device faults – especially helpful when planning high-availability systems.

SINEMA Server is capable of displaying the entire industrial network – from the diagnostics of network components right through to automation components, such as controllers and distributed I/O devices.

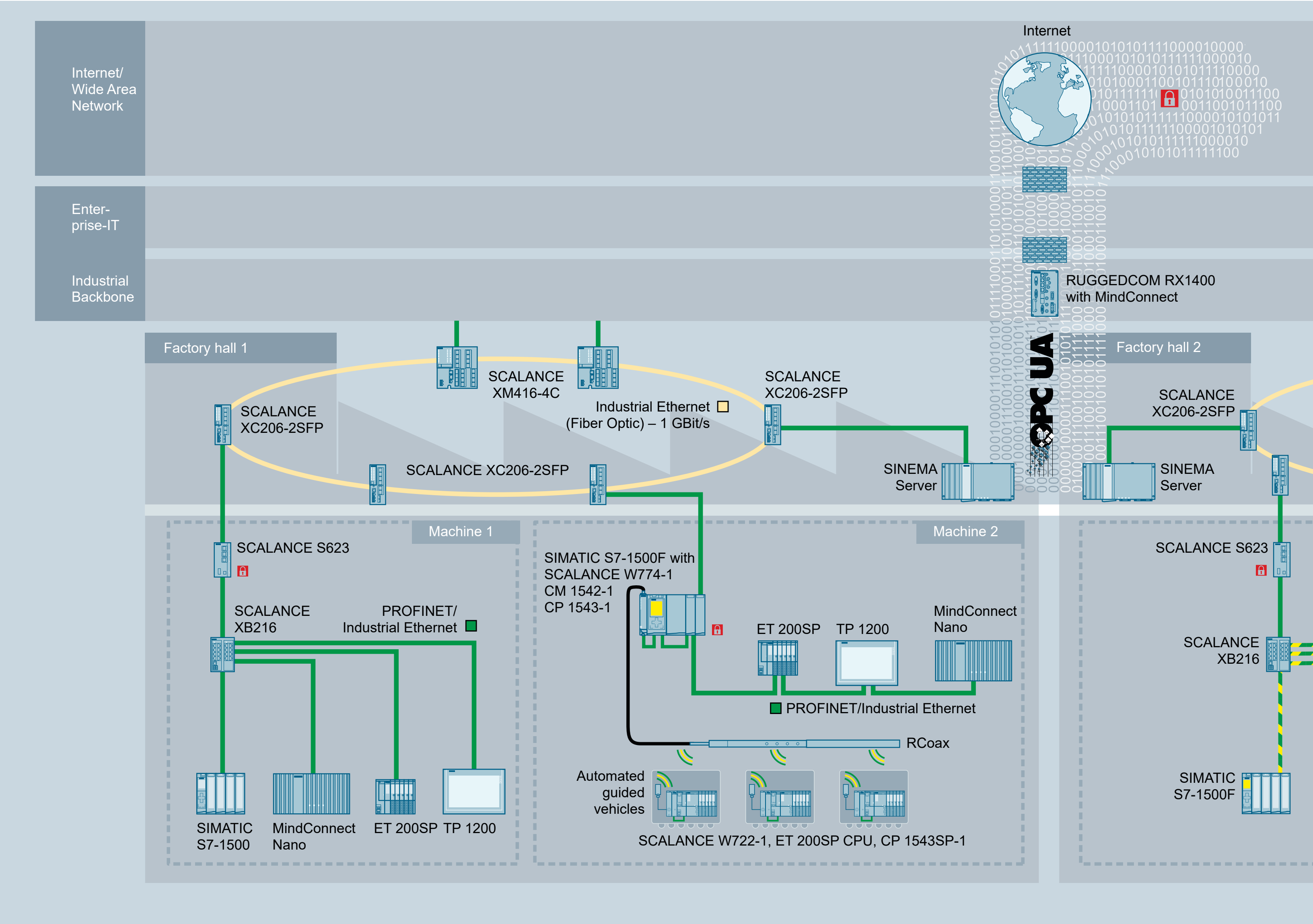
Benefits at a glance:

- Central firmware and configuration management across all devices via CLI
- Clear display of the network topology thanks to automatic component and topology recognition
- Event-based signaling system for transparent network diagnostics display
- Comprehensive diagnostics options via SIMATIC, PROFINET and SNMP
- Standardized network documentation (reports)
- Worldwide access using a standard web browser
- Transfer of data to cloud-based systems via a range of standardized protocols (e.g. OPC UA)
- Profile concept for integrating any required network nodes
- Monitoring of multiple systems with identical IP addresses using Network Address Translation (NAT)
- Validation of network parameters

SINEMA Server

Diagnostics data from the field right into the cloud

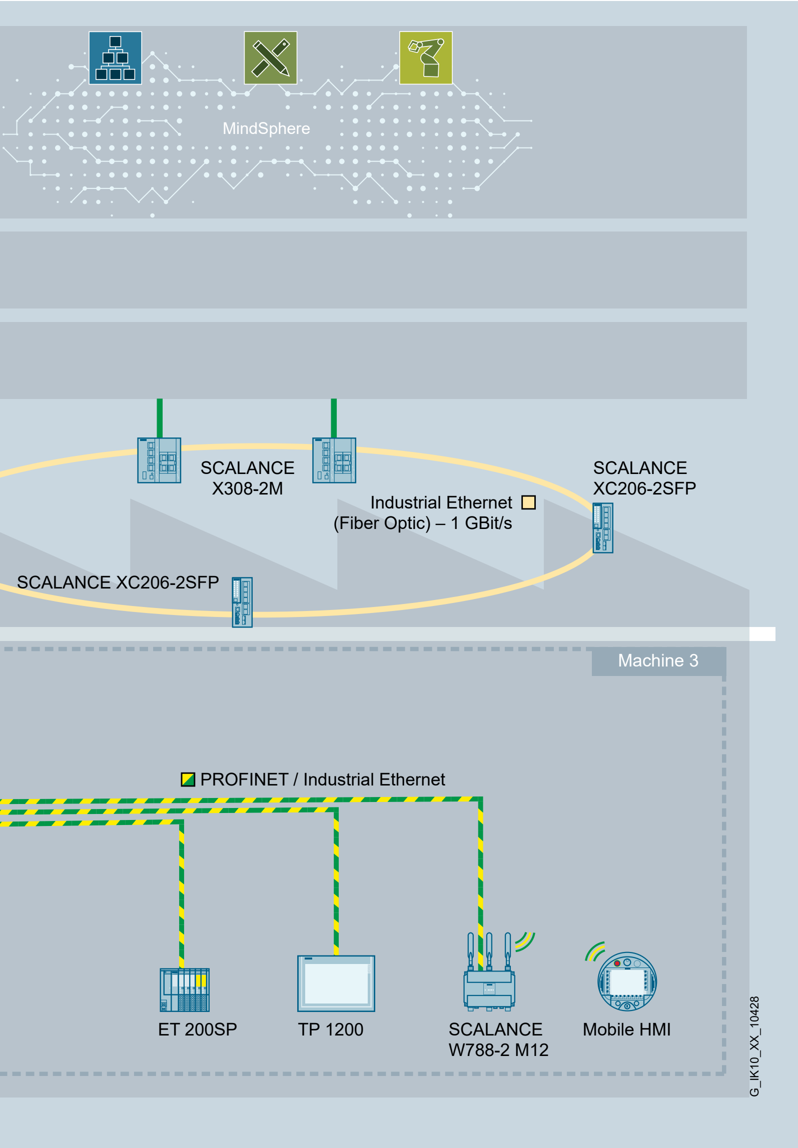
Manufacturing sites are frequently long distances away from each other. It is therefore important to have a global overview, in addition to diagnostics data for as many network components as possible, with a single software solution. The advantage of cloud-based systems is that data can be accessed centrally and independently of a user's location. The status of your systems and machines across the world can thus be accessed at any time – such as via the open and cloud-based IoT operating system, MindSphere. SINEMA Server data (including device and port status, as well as statistical trends) can be transferred to MindSphere using MindConnect via the OPC UA protocol and the RUGGEDCOM RX1400. This means that changes in values, such as an unreachable device, are visible immediately, even in highly distributed plants. This enables preventive maintenance and the avoidance of long downtimes in the event of faults.



Characteristics at a glance

SINEMA Server offers a range of options in the field of network management and diagnostics. For example, the reporting function can display statistics for any period of time. Third-party devices can be included as profiles in SINEMA Server, as well as a host of other features.

The most important SINEMA Server functions at a glance:



Diagnostics

Clearly presented diagnostics – evaluation and presentation of diagnostic states:

Reporting

Statistical overview for any timeframe:

Topology

Topological view of the network:

Validation

Validation of network parameters:

PDF

Monitoring

Reading-out of status information:

Propagation

Forwarding of data to other systems:

CSV OPC

Inventory

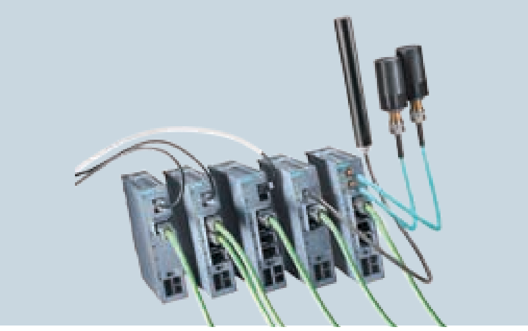
Inventory and documentation of all network nodes:

Management

Configuration of devices via CLI / firmware management:

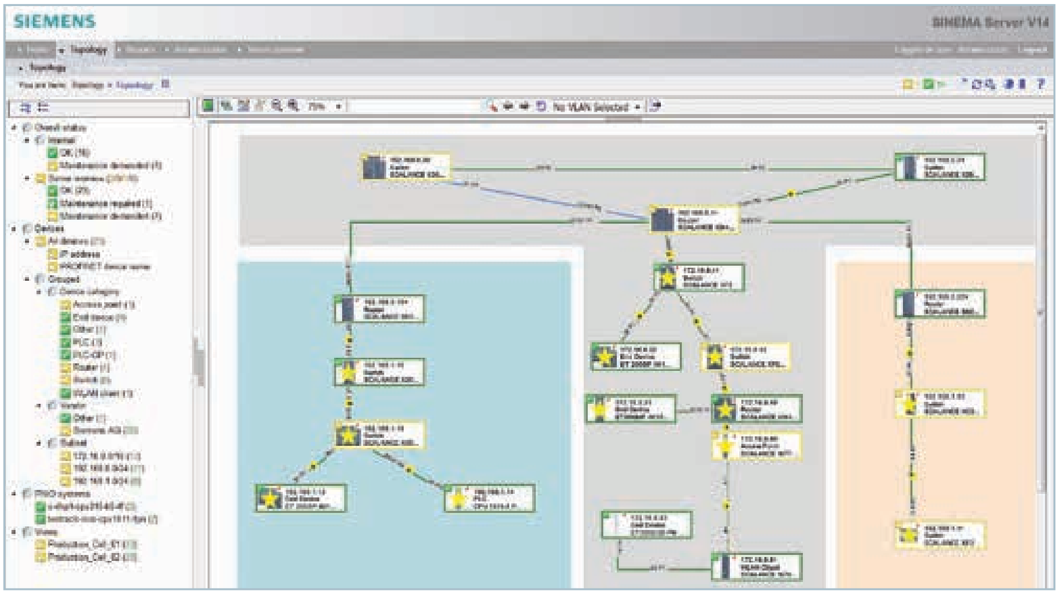
SINEMA Server

The most important functions of the network management software



Intuitive operation

SINEMA server includes the most important functions for the industrial environment. The clear structure of the graphical interface enables intuitive operation. Users quickly receive an overview of the entire network.



Automatic device detection and generation of the network topology

The network management software automatically recognizes PROFINET and Ethernet devices in the network with the aid of the Discovery and Basic Configuration Protocol (DCP) and Simple Network Management Protocol (SNMP), as well as via PROFINET diagnostics. The detected devices are shown graphically in a web browser. This means that the maintenance personnel in process and production plants can monitor the current status of the devices and their connections (topology) at all times without time-consuming configuration. A detailed device overview can be provided for Siemens automation components. These include Siemens network components from the SCALANCE and RUGGEDCOM product families, controllers, such as the SIMATIC S7-1500, as well as any corresponding communication components. Additional field-level components include the SITOP PSU8600 24 V DC uninterruptible power supply, identification systems, drive systems, such as SIMOTION, or continuous gas analyzers like the SIPROCESS GA 700. In addition, third-party devices and their statuses can also be displayed in SINEMA Server and can be seamlessly integrated thanks to the profile concept.

Comprehensive, system-wide diagnostics options

SINEMA Server offers a range of diagnostic options:

- SNMP: for the standardized diagnostics of network components from any manufacturer
- PROFINET: the open Industrial Ethernet standard for manufacturer-independent data analysis
- SIMATIC: for evaluation on the component-internal level for integration into the end-to-end system diagnostics feature within the TIA Portal (seamless integration into the CPU signaling system)

Centralized firmware and configuration management

All of the devices in a monitored network can be configured at the same time thanks to centralized firmware and configuration management via CLI. SINEMA Server enables firmware and other updates to be performed centrally on SCALANCE components (also in bulk). This can be initiated manually or scheduled within desired time windows.

User-specific topology view for a network

As well as the automatically generated view of the topology, SINEMA Server also gives users the option of showing the network nodes in any possible arrangement. These user-specific topologies can also be supplemented with background images (e.g. building or plant diagrams). In the case of faults, this means that the relevant network components can be found and, if required, replaced or repaired more quickly.

Event alarms

For seamless and instantaneous network monitoring, messages need to be detected and users informed immediately. SINEMA Server offers an event handling feature with which all network event messages are acquired and processed. This provides users with all the important event information concerning the network.

User-defined view

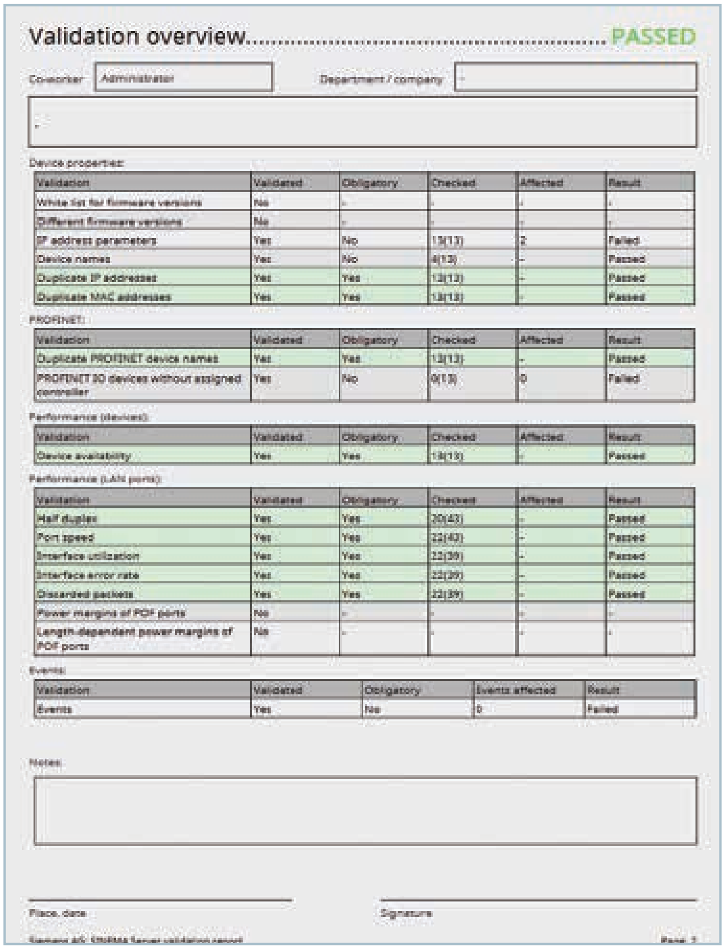
SINEMA Server allows users to assign various roles to users (e.g. administrators, maintenance personnel, etc.). Administrators can define different groups and appropriate rights and views are assigned accordingly. This prevents multiple people from working in the same SINEMA Server system with different roles at the same time.

User-friendly network reports

Network diagnostics encompasses not only the current status of the network, but also the analysis of historical values. SINEMA Server saves all the values read out from the network components, making it possible to carry out time-based filtering and evaluations with convenient reports. This enables the analysis of all previous events, meaning that future issues can be avoided.

Diagnostics of systems with identical IP addresses

Series machine builders in particular often configure their plants with the same IP addresses.
The machines are typically integrated in industrial plants via NAT routers. SINEMA Server is also able to monitor and diagnose these networks connected via such devices.



Validation overview.. PASSED

Co-worker: Administrator Department / company: -

-

Device properties:

Validation	Validated	Obligatory	Checked	Affected	Result
White list for firmware versions	No	-	-	-	-
Different firmware versions	No	-	-	-	-
IP address parameters	Yes	No	13(13)	2	Failed
Device names	Yes	No	4(13)	-	Passed
Duplicate IP addresses	Yes	Yes	13(13)	-	Passed
Duplicate MAC addresses	Yes	Yes	13(13)	-	Passed

PROFINET:

Validation	Validated	Obligatory	Checked	Affected	Result
Duplicate PROFINET device names	Yes	Yes	13(13)	-	Passed
PROFINET IO devices without assigned controller	Yes	No	0(13)	0	Failed

Performance (devices):

Validation	Validated	Obligatory	Checked	Affected	Result
Device availability	Yes	Yes	13(13)	-	Passed

Performance (LAN ports):

Validation	Validated	Obligatory	Checked	Affected	Result
Half duplex	Yes	Yes	20(43)	-	Passed
Port speed	Yes	Yes	22(43)	-	Passed
Interface utilization	Yes	Yes	22(39)	-	Passed
Interface error rate	Yes	Yes	22(39)	-	Passed
Discarded packets	Yes	Yes	22(39)	-	Passed
Power margins of POF ports	No	-	-	-	-
Length-dependent power margins of POF ports	No	-	-	-	-

Events:

Validation	Validated	Obligatory	Events affected	Result
Events	Yes	No	0	Failed

Notes:

Place, date Signature

Siemens AG: SINEMA Server validation report Page 1

Get more information

Making your network transparent
www.siemens.com/sinema-server

Professional Services for Industrial Networks
www.siemens.com/industrial-networks-services

Published by
Siemens Industry, Inc. 2018

Process Industries and Drives
100 Technology Dr.
Alpharetta, GA 30005

Subject to change without prior notice
Order No. NTBR-IBB02-0418
Article No.6ZB5530-1BB02-0BA7

All rights reserved
Printed in USA
© 2018 Siemens Industry, Inc.

The technical data presented in this document is based on an actual case or on as-designed parameters, and therefore should not be relied upon for any specific application and does not constitute a performance guarantee for any projects. Actual results are dependent on variable conditions. Accordingly, Siemens does not make representations, warranties, or assurances as to the accuracy, currency or completeness of the content contained herein. If requested, we will provide specific technical data or specifications with respect to any customer's particular applications. Our company is constantly involved in engineering and development. For that reason, we reserve the right to modify, at any time, the technology and product specifications contained herein.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
http://www.siemens.com/industrialsecurity.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
http://www.siemens.com/industrialsecurity.