Introduction
Thanks to the power of its Information Platform, and to the versatility of its architecture, Tenore can easily be employed as a Supervisory and Control Station in a SCADA system for the management of Power, Gas and Water Networks, as well as all of those applications requiring integration and control of geographically distributed systems and remote data acquisition.

ABB Energy Automation recognizes, however, that these types of systems have special requirements in terms of management of distributed architectures, interfacing to heterogeneous equipment, communications and openness. For this reasons, we have extended the core Tenore Information Platform with a set of SCADA oriented features, to bring to our Network Management customers a state-of-the-art solution to their specific needs. The combination of these new features with the consolidated and powerful Tenore Information Platform can satisfy the most demanding requirements for distribute, remote and dependable control.

IndustrialIT Enabling allows Tenore to operate smoothly with all the new products of the IndustrialIT Product Strategy, preserving the customer investments in technology and experience.

Overview of SCADA Extensions
The SCADA Extensions to InformIT Information Management Tenore address the specific requirements of customers facing the Supervision and Control of geographically distributed Networks. More specifically, features have been included to provide solutions in the following functional areas:

- Management of distributed servers architectures
- Interfacing to a wide selection of devices, including RTU, PLC and IED (Protections)
- Remote access to the system
- Intuitive visual representation of the network and equipment status
- Maintenance of distributed networks
- Management of flexible security and distributed operating teams

These will be discussed in more details in the next pages.

Features and Benefits at a Glance
- Multi-master inter-operation
- Up to 128,000 tags per server
- Web Extensions support
- Windows 2000 platform
- OPC Server and OPC Client support
- Support for multinational languages
- Multilevel security
- Scanner suite for foreign protocols
**Distributed Architecture**

Tenore is based upon a distributed, open, client/server architecture taking advantage of distributed servers.

Servers can be combined to extend the number of managed points beyond the physical limits of a single server. Thanks to the distribution of the database, it is possible to manage a virtually unlimited number of points in a single system. Clients can access points on any of the servers in the network, allowing the creation of graphical views that span the domain of any individual node.

The server expansion can occur both horizontally and vertically:
- Horizontally, by adding new servers at the same hierarchical level
- Vertically, by adding new servers at a higher hierarchical level.

**Store and Forward**

The communication between servers, both horizontally and vertically, is based on the proprietary, highly robust and efficient Tenore-to-Tenore protocol. This protocol is built on TCP/IP, therefore it can employ any communication vector supporting this protocol. This includes communication over telephone lines using a modem.

Every node in the architecture can be made redundant, taking advantage of the standard multi-master features of the Tenore Information Platform. Additionally, the communication across hierarchical levels has been extended to support Store and Forward policies. To all practical purposes, this is equivalent to applying redundancy to vertical communication: in fact, when a node at a higher level loses communication or, in general, fails, the node at the immediately lower level will store all real-time, historical and configuration data and send it to the higher level as soon as it comes back on-line.

**Front End Servers**

Scalability is essential for SCADA systems. Customers want to be sure that their system will grow together with the plant. Tenore servers are like building blocks, which can be added to an existing system while this is on line.

One special server option, useful for widely distributed networks, is the Front End. Normally installed on an industrial computer, this special configuration can be used to collect remote data and forward them to a central server. Since these nodes will only perform data acquisition functions, their cost will not depend on the number of configured tags, giving the customer an extremely cost effective solution for very large systems.
Centralized Database Management
In a distributed architecture, with several server nodes and data acquisition equipment, each element of the architecture requires a specific configuration database. Managing the overall system configuration may soon turn into a time-consuming and error-prone task.

This problem is resolved by Tenore thanks to the Distributed Database Manager (DDM), a special tool providing the SCADA users with a single point of entry for configuration data, regardless of the number of nodes.

DDM provides a tree-view of the system architecture, including redundant servers, front-end servers and data acquisition nodes. By selecting a node in the system, DDM presents its specific configuration files, which can be modified directly from this view. Additionally, for those devices supporting this service, it is possible to send the file to the destination node and to launch the configuration procedure. Currently, the nodes supporting this service are all types of Tenore servers and the UP01/02 Remote Terminal Unit, by ABB Energy Automation.

Communication Infrastructure
One of the defining aspects of a SCADA system is its ability to supervise and control widely distributed equipment. The efficiency and flexibility of a solution is therefore proportional to its ability to work with the available communication vectors. Depending on the type and criticality of the Remote Terminal Units and the data they are responsible for, several options are available to maximize the system performance and minimize its total operating cost. The Tenore SCADA Extensions has been used in systems where the communication infrastructure includes:

- LAN/WAN
- Switched lines
- Radio
- Cellular
- Satellite

Standard protocols for SCADA communication
Normally, a SCADA system is required to integrate and interoperate with equipment from several vendors. While it is expected that systems containing equipment provided by a single vendor will offer a better degree of integration, it is also demanded by the customers that they are not locked into this situation and have freedom of choice when selecting RTUs, IEDs and Instrumentation. This trend naturally requires that the SCADA central system has the ability to work with the most extensive set of supplier. ABB Energy Automation can offer a complete portfolio of integrated components, but the Tenore SCADA Extensions will work equally well with any piece of equipment compliant with the following protocols:

- IEC 870-5-101
- IEC 870-5-103
- IEC 870-5-104
- Modbus
- SPABUS (ABB Protections)
**Internet and Thin Clients**

In a geographically distributed system, remote access to the equipment information for acquisition and control purposes is a fundamental requirement. Support for multiple communication vectors and protocols, as seen above, will ensure that these information will be accessible to the distributed servers performing data acquisition and management functions.

However, data visualization and control is often required from locations different than the ones where the servers are located. For this reason, the ability to remotely access the servers is of paramount importance for a modern SCADA system. The Tenore SCADA Extensions take advantage of the state-of-the-art Web technology to satisfy this need.

Each Tenore server has an integrated web server, which publishes for the Internet all real time, historical and configuration information. These can then be viewed remotely by displaying HTML pages with Microsoft Internet Explorer.

This is normally defined as thin client technology: a remote PC does not need to install any proprietary software, since the Internet browser is used as the remote operating environment.

All HTML pages are stored and managed by the web server, and downloaded to the remote node on request.

**Remote Access Security**

Security is guaranteed through standard hardware and software components, like switches, bridges and firewalls. Additionally, each access attempt is subject to verification of the user identification and password, which will also define the user profile and its authorization level. The users are the same as defined for local access to the standard (or thick) client.

To increase the security of the system and provide a physical separation of the SCADA server and the web server, the latter can be located on a dedicated computer, which will retrieve the plant information from the former. The two can be isolated using standard network security components.

**Exchange of graphical pages**

It is possible to display all accessible information with HTML pages, since access functions are provided which can be inserted in a page script. The standard Tenore client, as shown in Fig. 4, can also display the same pages used for remote access, since it is a web browser itself.

Additionally, a component is available for use in HTML pages to display standard Tenore graphics in Internet Explorer. Thanks to this components, which is downloaded the first time the remote client accesses the web server, a thin client is functionally and visually equivalent to the thick, standard client.
Graphical Extensions
Operators interact with the controlled plant using graphical pages representing the components of the system in a schematic way. Providing graphical pages that represent the network with familiar symbols increases a SCADA operator interface usability and user-friendliness. For this reason, the Tenore SCADA Extensions include a library of predefined static and dynamic graphical objects typical of an electrical, gas or water transmission and distribution network (switch, breakers, transformers, pumps, motors, pipes, etc.). Some of these symbols are prepackaged with all the associated tags. When configuring a graphical page, the selection of one of these will automatically create the association with all the related tags. Figure 5 shows and example of SCADA graphical page.

People Finder
For a geographically distributed system, as it is often the case for a SCADA, the maintenance personnel is normally many kilometers away from the source of a problem, and it may be difficult, especially when parts of the network are not manned, to notify them of impending or occurred problems. Furthermore, maintenance personnel on the field may not have ready access to detailed information about the problem itself, since they may be far and away from the control center.

The People Finder application is designed with these two problems in mind:
- Ready notification of remote maintenance personnel
- Ready access, from remote location, to diagnostic information

The first problem is addressed by a GSM gateway embedded in the Tenore server. This gateway can capture alarms and events, which, if specifically configured for this purpose, can generate SMS messages or GSM phone calls to the personnel on call. The messages or calls will have access to a phone book of the personnel with their shift assignments. Each attempt to locate a remote technician will await for an acknowledge and, after a configurable time-out, will move on to the next person on the list.

The second problem is addressed by the embedded web server, described elsewhere in this brochure, which will make available detailed diagnostics by simply connecting a laptop to a network or an ISP via a modem.

Combining the timely notification and easy access to details of the problem, customers can be confident that help is on the way.
Centralized Security Profiles Management

A challenge that is often faced by a distributed SCADA system with several control centers is the user security management. To facilitate this task, Tenore SCADA provides a centralized tool for the assignment of authority profiles for the configured users.

The main purpose of this tool is to prevent conflicts between operators in different control centers, and to provide a unequivocal identification of who has performed certain actions at any given time.

In general, a user security profile, containing the identification of what control actions he/she is enabled to perform, is a combination of the physical location and the individual profile.

Users need to be configured for every physical location. The centralized security profiles manager can visualize a list of all the users configured for a certain physical location. From the same tool is then possible to decide if a remote location can be temporarily transferred control of the section of the system connected to it. At this point, users with control authorization for that remote location can perform actions on the system itself.

This delegation from center to remote remains in effect until revoked by the center.

Thanks to this central management tool, it can be guaranteed that only one user at a time will be able to interact with each section of the controlled network, enhancing the safety and reliability of the overall system.