IP-based SCADA-applications are increasing rapidly. This brochure gives you an idea of market-trends and introduces you into the basics of SCADA over IP including related migration scenarios and the underlying Utility Communication Systems.
Fast-changing Technologies and Markets

Introduction

Ethernet* & IP in public telecom and IT infrastructures for enterprises have been established for many years. The increasing cost-pressure and the need for compatibility in data exchange processes also force utilities to move towards integrated network solutions where Ethernet & IP play a significant role. The tremendous success of the Internet together with the fact that IP can virtually be used over any physical media has made IP the universal service-provision interface. The fact that both the ITU-T and the IEC have accepted IP as a network and access protocol, and the highly valuable assets such as the utilities’ fibre-optic backbones lead to a tremendous growth of IP-based solutions also for operational applications like network control and SCADA.

Ethernet to the Device-Level

For many years, Ethernet was mainly used for office LAN communication. Major independent consulting groups like ARC however predict a quick penetration of Ethernet/IP-enabled devices even for field devices (see Fig. 1).

Other sources say that about 20 % of these solutions in the so-called “harsh environment” are realized with dedicated “Industrial-Ethernet” devices; other solutions for utility networks demand even more know-how and precautions. This means that this is a task for System Integrators who are familiar with the utility environment.

Business Role of SCADA systems

SCADA systems have moved away from just being a management tool for electrical grids or pipelines. They became knowledge management tools learning and accumulating continuously technical as well as commercial information that is serving a more and more diverse range of user groups. This is becoming a particularly important factor for users in the wake of integration issues with linking to enterprise and business applications. SCADA vendors are now looking to improved responsiveness to the integrated business practices of the power industry. ABB’s Industrial IT philosophy is fully in line with this trend, which makes sure that all users within a utility have real-time access to the information which they really need, and for which they have access rights.

The SCADA marketplace is being transformed because of new technology and significant changes in the way companies are streamlining business processes. ABB recommends SCADA systems and components that can support these advantages and opportunities in this fast-changing marketplace. Users are clearly showing more interest in integrating their SCADA with corporate IT. As energy companies become more focused on their supply, chains and systems that were once the exclusive domain of operations now need to be integrated with more enterprise-level systems.

As SCADA systems are however the source of all basic operational data to be used for business applications such as energy trading, significant investment will be made over the next few years (see Fig. 2).

Figure 1: Ethernet down to the process device
(Source: ARC Automation Research Cooperation)

Figure 2: Fast growth of the SCADA market
(Source: ARC2002)

* Please see the back page for a list of the abbreviations used.
Communication Networks for IP-based SCADA systems

Network structure and LAN-WAN definitions

Utility Communication Networks can be implemented in a hierarchical or flat structure:

- **Hierarchical:** dedicated SDH equipments for the transport level (eg. FOX515T) with Access Multiplexers feeding into the SDH backbone (see Fig. 5 / Level X)
- **Flat:** no SDH overlay; the equipment used covers access as well as the transport functions (eg. legacy up to STM-1 with ABB’s FOX515 Multiplexer) (see Fig. 5 / Level Y)

IP-oriented LANs and WANs can be part of both of the above mentioned structures, because ABB’s transport and access devices both have integrated Ethernet Interfaces. Earlier investments are well protected because of the integration capabilities.

The definition of LANs as an Ethernet/IP-based network within an office or substations seems to be pretty clear. However, when talking about WANs, big misunderstandings arise, because for most IT people they consist of router connections at speeds much less than 2 Mbps. ABB’s FOX solutions can easily provide much higher WAN capacity on the utilities’ own infrastructure. This capacity allows the transport of other IP-based applications along with the SCADA data without interference.

Communication Requirements

To run SCADA information over a network, various aspects have to be considered:

- **Type of equipments used**
  Are the RTUs IP-enabled?
  What kind of Ethernet IF do they support? The most convenient is 10/100 BaseT IF, such as is supported by ABB’s RTU560.

- **Bandwidth used by RTUs**
  Traditional RTUs with serial interfaces did not need more than 10 kbps. This has only changed little, due to management-traffic, which supports the remote configuration of RTUs in a very efficient way via IP. Experience has shown that bandwidth is not an issue with RTUs.

- **Bandwidth used for Inter-SCADA-Centre communication**
  Normally, two or more SCADA-centres are connected via ICCP/TASE.2 running over IP. For hot stand-by, shared operation and back-up functionality, an IP-bandwidth of at least E1 capacity should be provided.

- **Network redundancy criterias and protection schemes**
  The topic of redundancy planning - the definition of protection paths for data and communication signals is a key task. One has to distinguish two Ethernet/IP traffic protection mechanisms:
    - Layer-2-based switched networks have to re-establish the Spanning Tree, which may be dozens of seconds. Therefore, Layer-3-based routing can be the better choice.
    - Whenever IP traffic is carried via PDH/SDH mechanisms such as 1+1, ring protection can swap the traffic to a predefined alternative route within few milliseconds, which means long before re-routing even starts.

- **Restoration times in case of failures**
  “Real-time” is a very relative term; whereas information transfer in IP enviroments is faster than with traditional serial transmission (e.g. RS-232), restoration time may be higher. This, however, depends very much on the chosen traffic protection schemes indicated above.

- **Other IP services within the network**
  To make best use of an Ethernet infrastructure, additional services such as office communication or voice may run over the same network. VLANs with dedicated bandwidth allocation can be used to provide the required QoS for each application.
Integration of existing RTUs

To protect earlier investments in serial RTUs, the following are possible scenarios to move towards an IP-based SCADA system:

- Use decentralized FE’s which collect and consolidate serial traffic based on the IEC60870-5-101 from the old RTUs (Fig. 5 / Sector A). Connect those FE with the IEC60870-5-104 protocol via IP over PDH/SDH to the control centre where SCADA data will be extracted by the SCADA servers.

- User Terminals (TS) which allow a varying number of serial lines coming from old RTUs to be transmitted via IP to the control center. In this case, the IEC60870-5-101 protocol is not converted for the transport (Fig. 5 / Sector B). The SCADA servers run software which allows the individual RTUs to be contacted via virtual COM-ports.

- Keep the existing installations and just connect new RTUs directly via IP over PDH/SDH (Fig. 5 / Sector C).

SCADA over ABB’s Network Solutions

ABB’s communication solutions provide connectivity over Utility Networks for all the services required. For IP-oriented LAN/WAN applications, EoS guarantees Layer 1-4 functionality, which means the individual network users get:

- Defined electrical or optical interface, eg. 100BaseT on a RJ45 or optical Gigabit Ethernet

- Defined protocol support, eg. for all applications running over TCP/IP

- Guaranteed performance parameters, eg. minimum bandwidth or maximum switch-over times

- VLANs with dedicated bandwidth

- Network resilience according to the requirements of the application

- Any other IF type for other utility services (telephony, sync./async. data, video)

Running all the different services over the utilities’ own network provides better performance at lower cost.

Figure 5: Integration of existing RTUs
Communication for traditional SCADA Systems

Most Remote Terminal Units (RTUs) of the past transmit their information via a serial interface running typically at 9600 Baud or less. They can be connected to the Front-End Processor (FE) either directly, via dial-up modem, or any other devices supporting transparent serial communication (see Fig. 3). Where lines were a premium, multidrop/partyline-systems were used.

Looking to the OSI-Communication model, SCADA-specific protocols like the IEC60870-5-101 are running on top of Layers 1-4, which provide a predefined point-to-point connection.

The main task of FEs is to terminate all the dozens of serial lines coming from all the RTUs. The FE extracts the protocol information, consolidates it, and provides it via LAN to the SCADA-servers usually embedded in an IP connection.

For inter-control-centre communication, normally faster leased lines carrying eg. TASE.1 are required.

Introducing IP Technology

One of the main reasons why the Internet Protocol (IP) is tremendously successful is the fact that it can be used over virtually any physical media. But IP is just a part of protocol suite, often simply called TCP/IP. Talking in OSI terms, one can exchange each of the layers individually without affecting the overall functionality. Fig. 4 indicates how the stack could look like.

The most relevant advantages brought by the IP technology are:

- Efficient use of the bandwidth avoiding the allocation of capacity where this is not necessary
- Widely accepted standards based on proven technologies and high degree of interoperability
- Reliability, because in IP networks packets are instantly re-routed if a node or link fails
- Scalability to cope with growth
- A very high degree of freedom to evolve network performance according to the strategic needs of the utility
- The optimization of the Total Cost of Ownership, taking into account initial investments and later costs for operation, upgrade, maintenance, and related personnel cost
- Protection of the investment - secured by the integration of Ethernet/IP over existing transport networks (eg. fibre-optic backbones or TDM-based access solutions)
Communication and SCADA Systems used

FOX515T: Utility focussed Transport multiplexer with unseen flexibility for SDH (STM-1 - STM-64 / WDM) and LAN/WAN-services.

FOX515: Utility Access MUX with trunk capacity up to STM-1 providing a wide range of user interfaces for legacy, data and voice. Integrated teleprotection functionality and other utility specific features fit all Access requirements of utilities.

FOX515X: Extends FOX515’s trunk capacity smoothly to STM-4 and 16 and adds strong GFP based Ethernet / IP functionality including routing to the network.

FOX515M: Connects via STM-1 and provides 4 E1, 4 Ethernet ports and 2 free configurable V.35/V.36/X.21 legacy ports for n x 64 kbps services for small installations in remote premises.

RTU560 family: Supporting
- IEC 60870-5-101
- IEC 60870-5-104
- DNP 3.0, also based on TCP/IP
- Modbus
- Indactic 23 / Indactic 33
- RP570/571

Benefits of IP-based SCADA Systems

- Unlimited locations for Servers and Clients: Users can install and move their SCADA servers, RTUs and Terminal Servers (if any) to any site. This gives high flexibility in terms of redundancy and security.
- Failover of SCADA Servers: Servers connected to the IP network (even in distributed LAN/WAN structures) provide mutual back-up for optimized availability.
- Service Takeover and Remote Support: More and more Control Centres are not manned during the night. During this period, either other regions can take over control, or a supervisor logs in via VPN in case of alarms.
- Savings: With IP-enabled RTUs, Front-End devices are no longer required; a lot of hardware, spares, and cabling can be saved and maintenance costs are reduced.

Abbreviations

CCNS Converged Corporate Network Solutions
E1 2048 kbps PDH signal
E0s Ethernet over SDH
FTP File Transfer Protocol
FE Front-End
ICCP Inter-Control-Centre Communication Protocol (similar TASE.2)
IP Internet Protocol
LAN Local Area Network
PDH Plesiochronous Digital Hierarchy
QoS Quality of Service
RTU Remote Terminal Unit
SDH Synchronous Digital Hierarchy
SMTP Simple Mail Transfer Protocol
TDM Time Division Multiplexing
VLAN Virtual Local Area Network
WAN Wide Area Network

References
- ARC Advisory Reports
- CIGRE Study Committee 35
- IEC60870