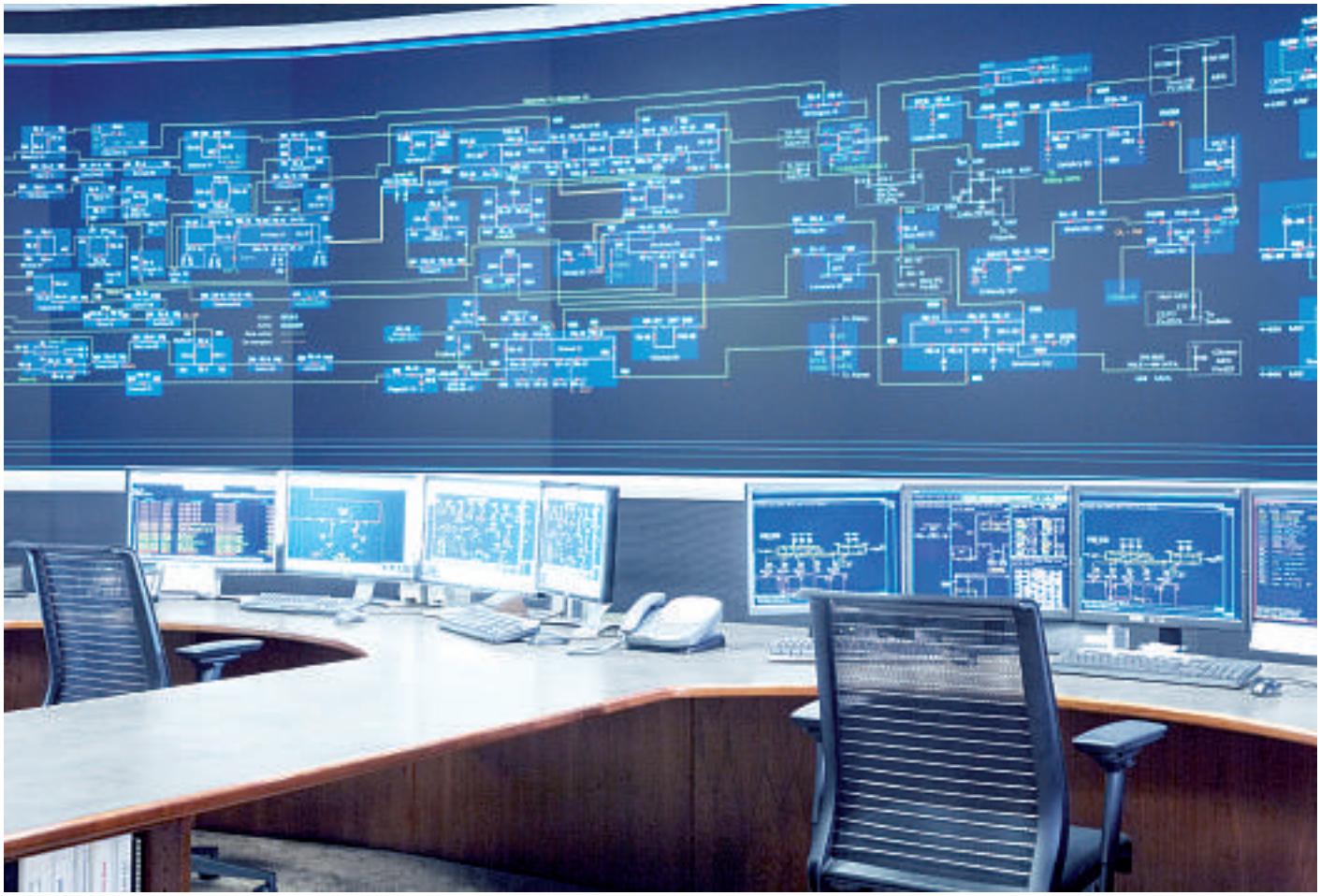
SCADA over IP-based LAN-WAN connections
Application



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 for the underlying utility communication system.

Power and productivity
for a better world™

Fast-changing technologies and markets

Introduction

Ethernet & IP in public telecom and IT infrastructures for enterprises are established since 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 an universal protocol. The world-wide acceptance of IEC61850 is another driver of Ethernet based applications in utilities; today mainly within the substation but with the extension of the standard, new services will be defined also between sub-stations and towards control-centers. The highly valuable assets such as the utilities' fibre-optic backbones including Ethernet over SDH (EoS) and native Ethernet based transport mechanisms lead therefore to a tremendous growth of LAN-based solutions for operational applications including network control and SCADA.

The worldwide electric power SCADA market is growing at a compound annual growth rate (CAGR) of 9.3 percent (forecast through 2014). A report published by ARC Advisory Group projects this substantial growth will result from a confluence of new technology and worldwide infrastructure spending fueled by sovereign investment programs. These investment programs are focused on the expansion of grid capacity in emerging markets, plus upgrading of aging transmission and distribution infrastructure including improvement of reliability and efficiency. Hand in hand with afore mentioned investments, additional infrastructure will be required to satisfy communication and control needs for smart grids.

Long lasting legacies

For many years, Ethernet was mainly used for office LAN communication. One of the reasons was the limited availability of utility hardened Ethernet-devices complying with harsh environments, another one the non-deterministic behavior of switched / routed networks.

Meanwhile the reluctance of utilities has widely disappeared due to the fact of LAN-equipment fitting utility applications much better. As example utility switches and routers of ABB's communication portfolio can be taken here.

Many of 'traditional utility devices' such as RTU's or even relays are today equipped with Ethernet interfaces. This shall however not imply that all services can be migrated straight away in a 'plug & play' manner to an Ethernet-based communication infrastructure. Differential protection services can be mentioned as one of the most delicate applications.

One has to consider the millions of installed utility devices with legacy interfaces like RS232 or RS485 operating typically at transmission rates of few thousand bauds. Therefore it can be concluded that the only thing that is certain about utility communications systems is that utilities usually will have for many more years a 'mix of everything'. This paper addresses exactly this issue of mixed technologies, protocols and equipment generations taking RTU's / SCADA systems as an example.

New role of SCADA systems and arising threats

SCADA systems have moved away from just being a management tool for electrical grids or pipelines. They became knowledge management instruments 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 utilities 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. Legacy SCADA system components may still work as initially designed, however, new operational and business processes often require new, higher-level functionality not included in the original components. Such extensions including new physical and logical communication network connections bear additional risks in term of cyber security. SCADA systems were traditionally "walled off" from business systems and were operating independently via the operational network only. Prior to the awareness of the risk of possible attacks, this seemed to provide all the protection the SCADA system needed. Their often proprietary character (operating system, protocols etc.) were often seen as additional safety assurance. The continuing trend to highly standardized systems and communication stacks undermine however the alleged system robustness significantly. In reality, their security is now often only as strong as the security of the communication network.

The following clauses focus on possible migration scenarios for utility communication networks in the light of the transition from traditional SCADA systems with serial, IEC60870-5-101 based RTU's into the Ethernet / IP dominated world.

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 including EoS supporting equipments for the transport level (e.g. Implemented with FOX-devices) with access multiplexers feeding into the SDH backbone (see fig. 1 / Level X)
- Flat: no SDH overlay; the equipments used cover access as well as the transport functions (e.g. legacy up to SDH with ABB's FOX- Multiplexers) (see fig. 1 / 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 and support latest LAN standards, including sophisticated VLAN- & provider bridging features.

Due to the continuous adaptation to latest standards and ABB's commitment to continuity and network management integration, earlier investments are well protected.

The definition of LANs as an Ethernet/IP-based network within an office or substations seems to be pretty clear. However, utility specific applications often have special requirements in terms of timing, packet loss rate and traffic handling (e.g. IEC61850 GOOSE Messages or SCADA protocol-handshakes). Due to very stringent delay and jitter demands, L3-routing or similar mechanisms are often not acceptable in such networks. When used in sub-stations, robust LAN-devices able to cope with harsh EMC and temperature environments need to be used instead of enterprise/office type equipment.

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 interface do they support? The most convenient is 10/100 BaseT, such as is supported by ABB's RTU560.
- **Bandwith 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. Experience has shown that bandwidth is not an issue with RTUs.
- **Bandwidth used for SCADA-Centre communication**
  Normally, two or more SCADA-Centres are connected via ICCP/TASE.2 running over IP. For hot standby, shared operation and back-up functionality, an IP-bandwidth of at least several E1's 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 take some dozens milliseconds up to seconds, depending on used recovering mechanism and network topology.
  - Whenever IP traffic is carried via PDH/SDH mechanism such as 1+1 or ring protection, the traffic is swapped to an alternative route within few milliseconds.
- **Restoration times in case of failures**
  "Real-time" is a very relative term; whereas information transfer in IP environments 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 may be used to provide QoS for each application.

Migration strategies

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. 1 / Sector A). Connect those FE with the IEC60870-5-104 protocol via IP or EoS to the control centre where SCADA data will be extracted.
- User Terminal Servers (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. 1 / 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. 1 / Sector C).

SCADA over ABB's network solutions

ABB's communication solutions provide connectivity over utility networks for all the services required. The widely deployed fiber-based PDH/SDH networks represent a robust high-capacity transport mean that can be smoothly extended by adding enhanced Ethernet features. FOX offers EoS over STM-1…64 or even native 10GE trunk-functionality for WANs.

For utility graded LANs inside sub-stations or plants, ABB's AFS/AFR L2/3 switch-family complements the portfolio for Ethernet-oriented applications whereas ABB's AFF – devices provide firewall functionality specifically for the utility environment. This unique communication portfolio covers all needs in terms of connectivity, capacity, security, availability and service flexibility. The following list mentions just a few features:

- Wide range of interfaces, from traditional RS232, teleprotection, telephony, sync./async. data up to 10 Gbit/s LAN or STM-64
- Packet over SDH or Circuit emulation for TDM-traffic if Ethernet is the native transport mean
- Protocol support for all applications running over Ethernet, including IEC61850
- Guaranteed performance parameters, e.g. minimum bandwidth or maximum switch-over times
- VLANs with dedicated bandwidth
- Network resilience according to the requirements of the applications

Running all the different services over the utilities' own network provides better performance with higher security at lower cost.

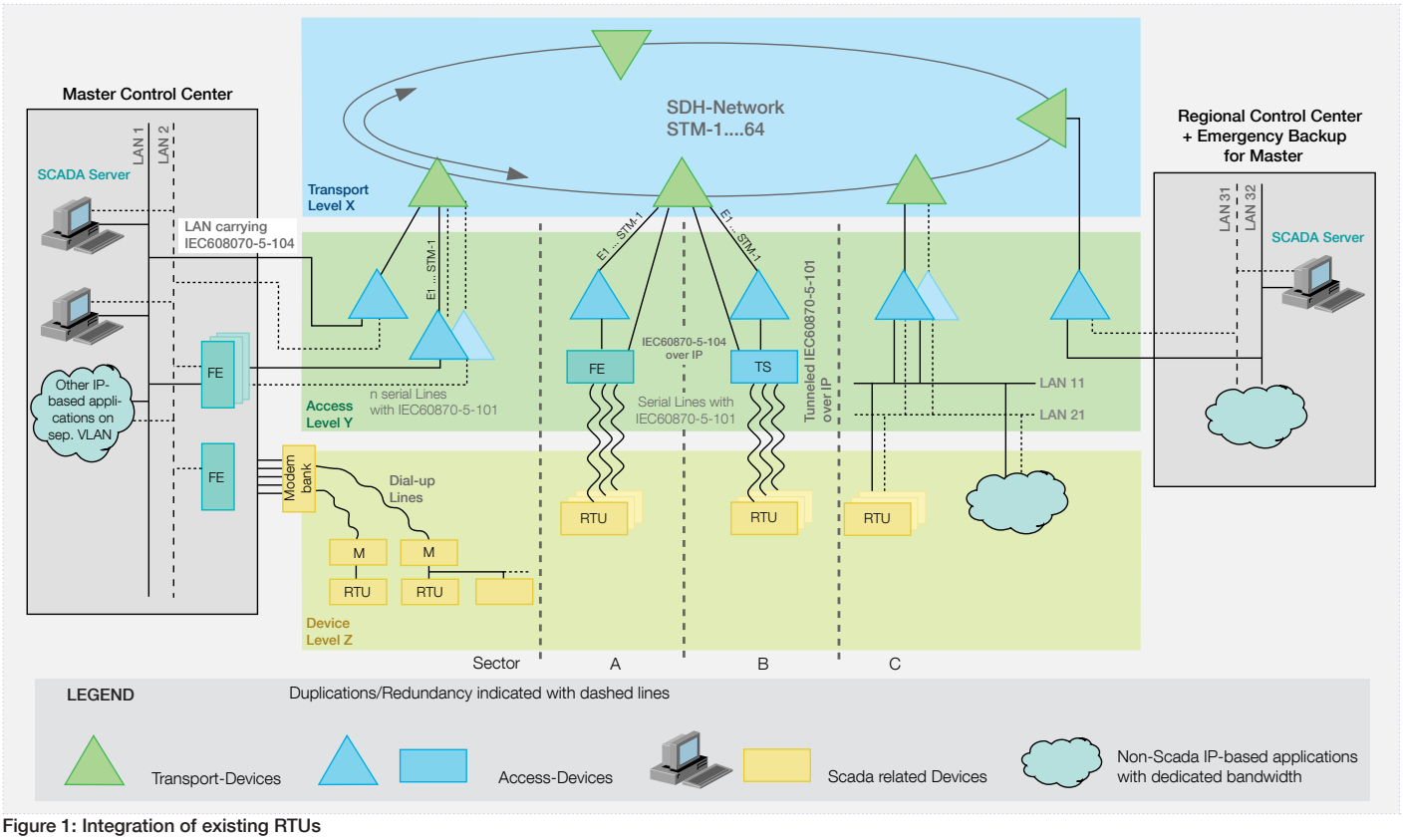


Figure 1: Integration of existing RTUs

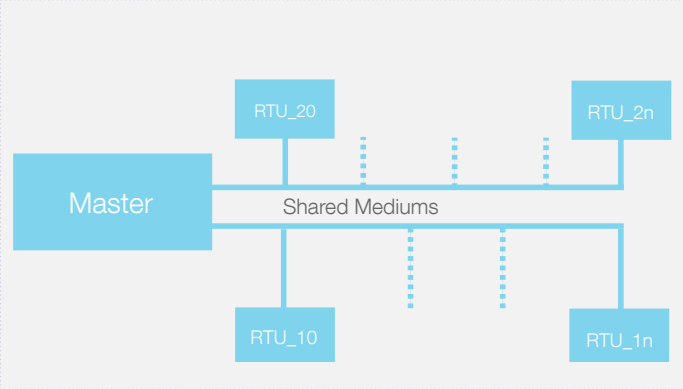


Figure 2: RTU Connections

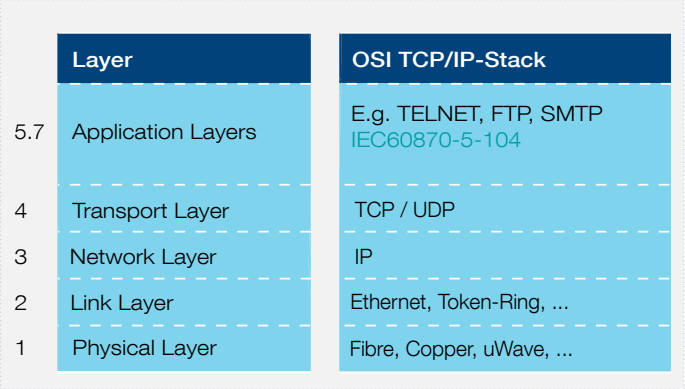


Figure 3: Layer 1-4 as vehicle for transport of higher layer protocols, eg. IEC60850-5-104

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 processer (FE) either directly, via dial-up modern, or any other devices supporting transparent serial communication (see fig. 2). 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 e.g. 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. 3 indicates how the stack can 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 (e.g. fiber-optic backbones or TDM-based access solutions)

Communication and SCADA systems used

FOX family: The family of fibre-optic utility multiplexers covers the full range of traditional legacy interfaces on the process side as well as trunk capacities up to 10 Gbit/s / STM-64. Dedicated, integrated teleprotection interfaces and latest LAN-features for SCADA and IEC61850 applications make FOX the perfect choice..

AFS / AFR / AFF family: Utility hardened switches, routers and firewall solutions

Wireless solutions: Smart radio solutions (GPRS / UMTS / EDGE; UHF/VHF) where connectivity via copper or fiber is an issue

ETL-family: Power line carrier systems providing comfortable bandwidths for LAN- as well as TDM-traffic

NMS-suite: Like an electrical or pipeline network, a communication networks needs to be managed. ABB's NMS-suite provides exactly the integrated network management solution that allows utilities handling their communication system in an efficient and highly reliable way.

RTU560 family: Highly flexible and modular remote terminal units, 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, many front-end devices are no longer required; a lot of hardware, spares, and cabling can be saved and maintenance costs are reduced.

Abbreviations	
E1	2048 kbps PDH Signal
EoS	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
IEC60870

For more information please contact:

ABB Switzerland Ltd
Power Systems
Brown Boveri Strasse 6
5400 Baden, Switzerland
Phone: +41 58 589 37 35
or: +41 844 845 845 (Call Center)
Fax: +41 58 585 16 88
E-Mail: utilitycommunications@ch.abb.com

www.abb.com/utilitycommunications

Power and productivity
for a better world™

1KHA - 000 802 - REN 1000 - 3.11 - Printed in Switzerland