INTRODUCTION
Utility companies are exposed to new threats. Deregulation and privatization lead to increased challenges in terms of cost efficiency and to high customer demands with respect to delivery quality and reliability. At the same time, today’s increased security risks demand countermeasures. Therefore a utility communication system must offer a minimal cost of ownership and maximum reliability and availability, supporting operational tasks, business activities and security. In order to accomplish this a number of requirements have to be fulfilled by the communication network.

Legacy systems as used in transport and distribution of electricity will typically use only limited communication resources. Cost reduction tends to increase the automation efforts, in substations, metering and in the management of the service crew. The computerization of administrative tasks for efficiency reasons causes additional data traffic.

Cost reductions also drive towards a maximal use of transport grid capacity, increasing at the same time the probability of hardware failures and the need to limit their impact on delivery. There is therefore a need for highly reliable, minimal delay communication for protection.

Newly emerging applications supporting video surveillance and access control are used as an answer to security threats and require relatively important communication bandwidth.

Strategies to lower operational costs include the collection of above data on one communication network. Part of the network resources can also be used by third parties for revenue generating applications. This is a strategic decision that has to be made with the choice of the network. In order to be fit for its task the communication system must show a number of characteristics.

The network must be extremely reliable and show predictable behavior. It must be guaranteed that the various applications that are served do not interfere. In order to preserve priority for the critical operational tasks it is necessary that these have their dedicated bandwidth.

SCADA and other legacy applications must be supported by the communication system both in terms of hardware interfaces and in software protocols. This will protect earlier investments both in terms of equipment and with respect to personnel training. The traditional applications used to be rather closed for a potential hostile outside world. Integration on a digital network must be accomplished with full data protection and network security.

Digital systems today show a high pace of renewal. Any system to be used by a utility company is by definition a long term investment. The adoption of newly emerging equipment therefore has to be supported by offering the necessary hardware interfaces and open software protocols.

In order to prevent human error in emergency situations or when physical security is at risk tasks have to be automated where possible. This means that the system must have knowledge about the environment, the threats and the required reactions.

A system is described that offers seamless integration of the legacy control, data acquisition and fire detection systems with video surveillance and access control equipment. Some real life examples will be presented where the integration of legacy systems with the newly emerging technologies has been successful.

Further details to the projects and implementation can be found at www.otn.be/cired.

Figure 1. Threats in a changing environment and the answers provided to the utility by technology.
THE CHANGING ENVIRONMENT

Competition
The proceeding liberalization of the electricity market is causing enhanced competition that drives the utility companies to increased cost efficiency and search for extra revenue outside their traditional activities.

Cost efficiency is sought both in the interaction with the customer and in the company’s own business administration. Automation of metering, lean customer relation procedures and strict management of the service force are examples of cost reduction efforts. The transport grid is exploited to the rated capacity in order to maximize revenue per invested dollar. Co-generation is increasing because of the pressure to use renewable energy sources. This increases the complexity of the grid and the difficulties for protection.

In an attempt to increase the revenue for the electricity utility, the network resources are partially used by third parties. Those can offer services like TV-distribution or broadband access.

Public Demand
Consumers are becoming ever more demanding with regard to delivery quality and reliability. The offers from various competitors, including supply guarantees, can be compared. The public and the society are also more dependent on the electricity supply. Consequences of blackouts today are very destructive both for our private lives and for our companies [1].

The public demand is especially hard to satisfy in an environment where competition drives utilities to operate the grid at its limits as discussed above.

Security (Physical and Network Security)
After the events of 9/11 more attention is given to security issues. It is clear that terrorists might regard our electricity supply as a target. Solutions offering perfect availability while neglecting external threats would not be satisfying the above public interest. While equipment failures can be foreseen and reacted upon by providing measurements, redundancy and standard procedures, the human factor in terrorist activity makes this much more difficult.

Infrastructure must be protected by video surveillance and access control systems. In the protection against, for example, theft or vandalism it might be sufficient to have recorded images of malicious acts: suspects can be identified afterwards and this on itself is a deterrent. Protection against terrorist acts must be immediate in order to prevent fatal damage to the installations.

The communication network itself must be safe from malicious software access attempts that are evolving into a serious threat today [2].

TECHNOLOGY ANSWERS

Integration on One Network
Today’s optical networks have the possibility to accommodate high speed applications that require lots of bandwidth. This bandwidth can be used for Gigabit or Fast Ethernet networks and CCTV (Closed Circuit Television).

It is very cost effective to use the same network for these high speed applications and for the data communications serving the substation switchgear, the SCADA system (Supervisory Control and Data Acquisition) and other legacy applications. The realized cost reduction is not only one of equipment but also the result of efficient maintenance through a unified management system.

Video Surveillance and Access Control
Modern security concepts are built with a number of integrated subsystems. The heart of the security system normally is a control room where live images form various locations can be watched and recorded. This enables the surveillance of unmanned substations. Multiple control room are sometimes provided to make sure there is a backup in case of emergency. On the network the images are transported as digitally encoded video streams.

Generally, the number of cameras is much larger than the number of monitors in the control room. Therefore it must be possible to switch cameras to any monitor at any moment. This can be accomplished by manual actions or by automatic switching, triggered by door contacts or fence guarding systems based on motion detection. Logging of events in a database is common practice.

Integration of access equipment and proximity readers has a long way to go to include also personnel databases to enable automatic access without human intervention [3].

Automation
The emerging IEC 61850 standard for substation automation is meant to enable the integration of equipment from different manufacturers by standardizing substation communication. The standard assumes the availability of Ethernet as a physical communications network in the substation, with VLAN capability to make sure that the priorities of the various information types are respected[4].

Grid Protection
Teleprotection schemes are used more often and with success to limit the size of the grid section that is affected when hardware faults occur. Faults localization and isolation are essential in order to limit the equipment that is put out of order.

With the maturity of the optical fiber technology, today’s digital transmission equipment has reached a level of reliability and availability that make it suitable for the transmission of teleprotection signals.
COMMUNICATION SYSTEM REQUIREMENTS

Reliability and Predictability
Because essential data is transported by the network, the first requirement is that this data is available at all times. The same network can be used for administrative data, for CCTV and for other high speed applications but no matter what happens, the data to support the operation of the grid has to be given first priority. Availability of connections is a function of equipment reliability and of the concepts used to separate different types of data.

Network reliability is typically implemented by having redundant equipment and redundant communication paths. The switch over from faulty to operational parts and equipment require a network configuration that has to be fast in order to fulfill the requirements for teleprotection signals. A hardware reconfiguration will offer a speed advantage over concepts based on software negotiations.

How data of different priorities is separated depends on the type of communication networks. It is essential that each connection in a network has at its disposal its own dedicated bandwidth in order to avoid competition between applications, especially at times of occurring emergencies when a lot of subsystems try to access the communication system.

SCADA Included
Because in today’s electricity network SCADA systems are extensively used to supervise and control the equipment, it is of vital importance that any communication network offers a seamless integration with these SCADA-systems. This allows the company to retain the capital that has been invested in equipment and training of personnel [5].

SCADA systems show a variety of interfaces that can be included in communication systems. Efforts have been made to standardize software interfaces by providing OPC (OLE for Process Control). Communication systems that are aimed at integrating with SCADA and PLC equipment must therefore not only offer the applicable hardware interfaces but also the expected standards in software.

Behavioral Knowledge Embedded
Integration is about providing the necessary hardware interfaces but also requires the possibility to make systems “talk” to each other by enabling adaptation of software protocols. It is also essential that the system has built-in knowledge about the procedures that have to be followed whenever something happens. In safety critical systems the human-machine interface must account for human error[6].

Figure 2. Principle of integration between SCADA and video switching. Switching commands can be given manually but are mainly initiated by PLC’s that are connected to fire detection systems and access control equipment. The video streams from the camera’s are automatically switched to the monitors while on the SCADA screens the alarm is displayed and waiting to be acknowledged.

Figure 3. Typically, only the communication network has sufficient knowledge of the environment to facilitate a high level of automation. Integration is necessary on three levels: hardware, software and behavioral.

As an example, consider a CCTV system and a detection of intrusion. First of all, the alarm should be based on automatic detection. Then, the reaction has to be executed by the system by, for example, warning security, closing extra gates, taking precautions for emergency situations that might follow.

The automation of detection and reaction is important in order to guarantee a predictable behavior. Emergencies events are by definition rare events that are difficult to train upon. Furthermore operator attention may be endangered when during long time no action is required. The fact that the system reacts automatically does not prevent the operator to have the possibility to overrule the system.

Network Security
When selecting a system to bring all applications together, it is essential to take network security in account. Today’s open systems sometimes also open doors to computer attacks. This can only be prevented with adequate security measures.
EXAMPLES

SCADA and Video Surveillance Integrated

The first example is a project in a gas winning field. It is presented as an example of the integration of communication and security networks on one resilient fiber optic backbone.

In the context of a new gas field development in the area of Qatif (Saudi Arabia) a project was implemented to connect cameras, recorders, monitors and SCADA and PLC controls to a backbone network [7]. The purpose of the network is to have surveillance from one control room of more than 15 offshore platforms. Additional applications include Fast Ethernet (100Mbps) for remote terminal units (RTU), telephony and low speed data.

Analogue video matrices are replaced by the built in distributed video capabilities of the communication system. Typical CCTV functionality, behavioral knowledge, is embedded in the software of the system. A universal protocol handler in software translates CCTV commands between the SCADA system and the CCTV equipment. This allows connecting cameras or video multiplexers of various manufacturers. This way the customer has the opportunity to have the equipment of his choice (for example explosion proof cameras) while still retaining the full functionality of digital video transmission.

Not only does this approach bring significant cost savings when compared with having separate operational, security and administrative networks, but also true vendor independence. On top of the collection of visual information, SCADA and PLC control and voice communications the system also takes care of legacy applications: low speed RS422/232 for corrosion detection, 4-Wire E&M signaling for radio and modem links and party lines.

Furthermore, the electricity company uses the same communication network to implement teleprotection of a number of cogeneration gas plants. This equipment uses dedicated G703-type connections.

Electricity Distribution Communication Network

Electrabel, a major utility company, has integrated all communication needs for electricity distribution in the southern part of Belgium onto one optical network. Activities of the Belgian utility provider in this region include the production, transport and distribution of electricity, the distribution of gas, drinking water and cable television.

The meshed communication network consists of a number of interconnected optical rings that scale from 2.5Gbps for the backbone to 150Mbps bandwidth for the access rings. The double optical rings have a built in hardware reconfiguration mechanism, ensuring maximal availability. Every connection on the network has its own dedicated and guaranteed bandwidth. This allows to use part of the network resources to third party utility suppliers without the risk of interference.

On the hardware level, integration is facilitated by a number of interfaces allowing physical connection of equipment. These connection types include classical serial data and telephony interfaces, broadband LAN and audio and video. Connection can be either point-to-point, point-to-multipoint or networked.

REFERENCES

[7] “Siemens sets milestone in pipe communication”, Oil and Gas News magazine OGN Vol.20 nr.37, Manama, Bahrain www.oilandgasnewsworldwide.com