A TCP/IP BASED COMMUNICATION ARCHITECTURE FOR DISTRIBUTION NETWORK OPERATION AND CONTROL

Mikael NORDMAN, Matti LEHTONEN
Helsinki University of Technology, Espoo – Finland
Mikael.Nordman@hut.fi, Matti.Lehtonen@hut.fi

John HOLMSTRÖM, Kenneth RAMSTEDT, Pekka HÄMÄLÄINEN
Ajeco Oy, Helsinki – Finland
john.holmstrom@ajeco.fi, kenneth.ramstedt@ajeco.fi, pekka.hamalainen@ajeco.fi

INTRODUCTION

Perhaps the most significant new development in data communication of our time is the TCP/IP protocol, which offers the first worldwide accepted standard of data transmission between computer systems. The main attractiveness of this protocol is the availability of cheap infrastructure equipment and protocol software.

However, the practical applications of TCP/IP in power distribution network monitoring and control have still been rare. One reason for this is that due to different type of physical transport media the TCP/IP protocol is difficult to implement in a system requiring deterministic behaviour. This is especially the case in geographically widespread network control systems. Concern has also been present about the data security, integrity and reliability.

The perhaps most cost-efficient way to globally transport data today, is by using networks based on the TCP/IP protocol e.g. Internet-, or intranet-type of WAN-networks. However, the nature of these networks present problems in terms of overall reliability. These problems are crucial especially when considering control system applications. If the problems in terms of reliability, timeout-management, determinism, automatic re-routing and security could be solved, these network-types would be attractive also in geographically widespread control system applications.

If the above mentioned problems could be solved, and if the new solution also would allow for taking old installations of hardware and software into account, in a seamless and modular way, the attractiveness would increase further.

This paper presents a solution called Distributed Systems intercommunication Protocol - DSiP, which aims to mitigate the above mentioned problems. The solution allows for integrating various manufacturers devices and software packages into a common automation system, covering geographically large areas. The DSiP provides a uniform and deterministic communications method between distributed equipment and software modules. In addition to this, DSiP addresses issues such as security, data integrity, reliability, controlled multicasting of data, automated re-routing and optimization of network bandwidth. DSiP was developed by Ajeco Oy.

Furthermore, special interest is paid in combining various physical telecommunications media into one automation system. These telecommunication media may have large differences in performance and throughput, making their intercombined operation a very challenging task. The paper also discusses general issues of providing a TCP/IP interface into distribution automation equipment. Two common approaches on how to integrate TCP/IP in a device are presented.

TCP/IP FOR DISTRIBUTION AUTOMATION

The communication solutions provided for distribution automation has for a long time been a mesh of different protocols on different physical media. Some typical examples are ModBus, ANSI X3.28, RP570, IEC 870-5-X and DNP 3.0. In addition, substation communication has had its own standards and the control center communication its own. By deploying TCP/IP the divergence on the network and transport layers may be removed and it is easier to build and configure the communication equipment. However, TCP/IP does not remove the divergence on the application and presentation layers. This can be seen by the fact that the standardization organizations have quite rapidly come up with adaptations of the well-known distribution automation protocols to TCP/IP. Examples of this is ModBus TCP/IP (also called Open ModBus [1]), DNP 3.0 TCP/IP and IEC 870-5-104 where the remote protocol IEC 870-5-101 is ported on top of TCP/IP [2].

Today there are also standardization efforts to converge the different information models on top of TCP/IP. The two most known standards that are based on TCP/IP and incorporating the protocol as well as the data model are Utility Communication Architecture (UCA 2.0) and IEC 61850 (actually mainly based on UCA 2.0). IEC 61850 is intended to be the worldwide standard covering the whole communication and data representation structures needed by a utility [3].
The benefit of using TCP/IP as a common transport protocol is obvious. Services are more easily integrated and the overall costs of the network can be minimized in a flexible way. The protocol allows seamless utilization of a broad number of different access technologies, e.g. radio networks, xDSL links, fiber optics switching by ATM or Frame Relay, etc. This is an important aspect for utilities having their equipment geographically widely distributed with different communication requirements and constraints.

Another big benefit of TCP/IP communication is that the communication does not have to be of master – slave polling nature anymore. TCP/IP allows a client/slave to initiate data transfer itself. Hence, in distribution automation the impact is that less data must be sent over the network and that data will immediately be sent to the SCADA. The slow and bandwidth consuming polling scheme is not needed anymore.

The obvious benefits of TCP/IP does however not solve compatibility issues on application and hardware levels. Various equipment and software modules provided by different vendors may remain incompatible regardless of the fact that they would feature physically compatible TCP/IP interfaces. DSiP is an standardization effort to solve incompatibility issues by providing uniform service interfaces for software and hardware equipment rather than plain transport of data.

By following a set of logical rules within the DSiP-protocol and by using TCP/IP as means for transport, applications, equipment and software from different vendors may intercommunicate transparently i.e. applications may respond to and ask for services without needing to know about physical implementations.

TCP/IP also wakes some concerns among utilities. The first issue of concern is security. This is an especially important feature if the communication link is shared, e.g. for commercial users as well. This is typically the case whenever a utility wants to use the equipment and links already installed by telecommunication operators. One possible solution for easing security concerns is to purchase a Virtual Private Network (VPN) link from the operator. The VPN link is protected by means of encryption and authentication providing rather reliable and secure data transmission paths. [4] The DSiP-routing and node objects utilize Secure Socket Layer (SSL) connections which relieves the necessity of using VPN for security and thus facilitates the implementation of DSiP also in open network topologies. Additional security may be achieved by tunneling the DSiP SSL communication through a VPN.

The second issue of concern is the expected quality of service. Utilities are used to know quite exactly what communication links are capable of in terms of performance, reliability and response times. If the communication media is shared, such performance guarantees can not be given anymore. The Internet Engineering Task Force (IETF) has developed means to provide a certain degree of quality of service. Differentiated Services (DiffServ) is e.g. one technique that has been proposed. [5] A problem today is, however, that installed networks do not offer such services and there are uncertainties on how the service level agreements will be negotiated and the services guaranteed (i.e. which degree of trust in the agreement can be achieved).

DSiP addresses quality issues in several ways. DSiP ensures immediate re-routing of information if a connection is lost. In addition to this, the DSiP router objects maintain an automatically updated routing list to nodes, thus removing undetermined network connection timeout issues. A specific DSiP node may or may not be present in the DSiP network at a time. Information of node existence is automatically passed and shared between DSiP routing objects. If a connection to a node is lost, information about the loss is immediately passed throughout the DSiP network enabling (automatic) countermeasures to be taken. The DSIP router objects will automatically re-route DSiP packets via (several) secondary routes if the primary connection is lost.

The TCP/IP protocol contains acknowledgement of successful transmission. This acknowledgement does however not guarantee that the actual physical target application has received and acted upon the intended transmission. DSiP contains methods for ensuring reliability in control system environments through the possibility to request acknowledgement information from the physical target application. TCP/IP acknowledges data transcieving on a “stack-to-stack” basis, whereas DSiP acknowledges on “application-to-application” basis. Furthermore, it is a known fact that TCP/IP packets will occasionally disappear real-world networks and networks might have intermittent failures. To address these issues, the DSIP contain keep-alive and heartbeat mechanisms for ensuring data-link integrity. The DSIP packet data itself is equipped with checksums helping to discriminate communication bit-errors.

A third issue of concern is the physical implementation of TCP/IP based networks to be used with old distribution...
automation equipment. It is not feasible to assume that existing investments i.e. installed equipment, will automatically be replaced by new, plainly as a result of taking new communication protocols into use. There is a demand for making upgrading of systems as seamless as possible. Old distribution automation equipment can for example be connected to a TCP/IP based DSiP network using low-cost protocol converters. A protocol converter may contain a DSiP node performing device specific communication downwards with the old equipment and uniform DSiP specific communication upwards, towards the DSiP network. This option will be considered more closely in Section 4 of this paper.

A fourth aspect of concern in TCP/IP is the distribution of information (data) especially in a heterogeneous network. DSiP reduces the amount of redundant information through an in-built multi-cast mechanism. Furthermore DSiP provides means for controlling how much data a specific node may transmit through a connection. This is useful in systems where the transmitter is located in a high bandwidth network segment and the receiver is located in a low bandwidth segment of a network. The transmit rate may need to be restricted in order to maintain overall performance.

DATA SECURITY ASPECTS

Data security is one of the most discussed topics related to open networks like TCP/IP. There has long been a debate on what services which may reliably and safely be provided in TCP/IP network environments. A typical example of service is network banking (e-banking). When TCP/IP is used as transport in distribution automation networks, similar concerns will prevail.

Distribution automation functions have different levels of criticality. Let’s study the main function groups, monitoring data, control data and parameterization.

Monitoring mostly concerns the transmission of trend data, equipment condition data and metering data. Is this information valuable to a third party? Trend data can e.g. in some cases give valuable information regarding the behavior pattern of a customer. Trends may inform an intruder whether there is activity in the building or not.

Tampering with metering data may cause harm to consumers through incorrect billing. An intruder may theoretically change the metering data and resend it at a later time creating possibly lost revenues or generally harm as wrong billing must be investigated and sorted out. Generally, however, monitoring data is sent rather frequently and it may feel infeasible to equip this process with a huge computational overhead. Hence, encryption is to recommend for this type of service and if the data is more sensitive, strong encryption can be used.

The DSiP features strong encryption with replaceable keys at all connections.

Another critical function is control. The main threats are faulty control data or control data which is stored and resent after a while (reproduced with new timestamp). Faulty or repeated control data can potentially cause harm to the power system (e.g. shut down the power supply when a circuit breaker is opened with a reproduced command from a former operation). Hence, this data can generally be regarded as needing encryption and checksums for ensuring data integrity. Furthermore, it is valuable to be able to verify the origin of data. A proper authentication/password scheme is needed for the control data. Generally, authentication is valuable for monitoring functions too but the overhead of authentication data exchange and resource management (passwords and password verification) could be rather high and inconvenient in systems without a uniform password and security management. DSiP nodes may implement several layers of security and must authenticate themselves to the nearest DSiP router object using passwords and strong encryption. Nodes cannot appear in the DSiP network unless they authenticate themselves. The router/node structure results in minimal overhead in resource management and virtually no overhead in the traffic. Furthermore, DSiP command and data packets always contain information on initiator and target which means that the origin of a packet is always known.

Parameterization is the most valuable information in the power system. If the operator wants to use an open TCP/IP network for configuration, special care must be taken. If a third party gets the possibility to reconfigure the power system and its threshold values, a dangerous situation may occur. Therefore, it is not enough with strong encryption and passwords/authentication. Security architecture is best suitable for this purpose. This architecture helps to manage the security objects in a secure and trusted way, i.e. it verifies the trusted part that is allowed to distribute management and key information. In addition, digital signatures are used to sign the parameterization data being exchanged. The architecture is shown in Fig. 2.
especially if the system contains a lot of small, embedded devices. All devices are not capable of taking part in the whole security infrastructure (e.g. a power meter in AMR) so the security services should be adapted to the capabilities and the needs. Only then can a system be designed that is acceptable to those involved in distribution automation.

DSiP nodes may support third party digital signatures. Even though a DSiP node authenticates itself correctly into the nearest router object, it has no implicit rights to perform anything in the system except attempting to get control over another node which again may require further authentication, passwords and digital keys.

A GENERAL ARCHITECTURE

A scheme of a general TCP/IP architecture for distribution automation is given in Fig. 3. It contains a core access network, which presumably is based on fiber optics and a number of IP switches. The core is extended so that it reaches the locations by means of radio links, copper links or some other medium. Fig. 3 shows four different utility items that are linked to the TCP/IP core network. These are:

- the Network Control Center, where TCP/IP is the communication interface to the SCADA system (interface ‘1’),
- an Remote Terminal Unit in a substation having a direct connection to the core network (interface ‘2’),
- a Power Monitoring Unit that is connected to the core network via radio links, e.g. TETRA IP or packet radio (interface ‘3’) and
- a customer with Automatic Meter Reading capabilities provided over an xDSL link that is connected to the meter via a gateway and a PLC network (interface ‘4’).

Interface ‘1’ is an example of a system where the TCP/IP protocol integration is rather straightforward. It is feasible to presume that the SCADA software is running in a standard PC environment. Hence, the TCP/IP networking capabilities are available and what is needed is a mapping of TCP/IP to the application protocol supported by the SCADA. Today such protocols are e.g. IEC 870-5-X or DNP 3.0 and the protocol stacks/interfaces are commercially available.

Interface ‘2’ is a communication interface between an RTU and the core network so that the physical interface is implemented using a fixed link (twisted pair or fiber optics) and Ethernet. This is a typical solution in a primary substation that is located near the core network. There are two ways how to implement this type of interface. It can either be done by an external component, a box with Ethernet interface and serial port connected to the serial port of the RTU, or by an integrated solution. These options are shown in Fig. 4.

In the right-hand side solution, the connection box functions as a protocol converter as well as the physical interface integrator. For example, if the RTU is configured to run ModBus over the serial interface and the TCP/IP Ethernet runs some other protocol, the connection box is responsible for doing the protocol conversion. This type of architecture is common in the case that the TCP/IP interface is provided to an already installed component. The left-hand side is more appropriate for new equipment. The Ethernet interface can be implemented as just another port in parallel to e.g. the serial interface. The TCP/IP protocol runs as another protocol option sharing the processor and memory resources of the main board.

Interface ‘3’ is a connection of a PMU to the core network via a radio link. Today there are a lot of different radio
solutions, e.g. GSM, GPRS, TETRA and packet radio which all can be used to connect distribution automation equipment to another host unit. The radio modem can be connected to the PMU (or other unit) in the same fashion as described in Fig. 4, the difference is only that the Ethernet interface is changed to a modem. Hence, a connection box can be used to provide the necessary modem interface logic and commands, or the modem can be directly connected to the serial port of the device while the modem handling logic is implemented as part of the system software.

Interface ‘4’ shows the utilization of an xDSL link to connect a building AMR. An xDSL link is necessarily not the primary choice of technology, equally well can the radio technologies discussed in the previous paragraph be used. In this case it is assumed that the household has an xDSL link already installed by a telephone operator and the same link can be used to transfer AMR data as well. The xDSL link is a copper version of the TCP/IP Ethernet. Today, the primary solution is to have the TCP/IP link connected to the energy meter via a gateway and a Power Line Carrier or alternatively short-range radio network. Hence, the meter itself communicates over e.g. a LonWorks power line communication network and the gateway manages the conversion between LonWorks messages and TCP/IP xDSL messages.

SUMMARY

Transmission Control Protocol (TCP) and Internet Protocol (IP) have during the last years gained a bigger interest from the distribution automation community. Traditional distribution automation communication has been based on proprietary solutions that have made system integration and configuration a very cost intensive and demanding task. With a common transport and network protocol the integration work will become simpler.

TCP/IP is already taken into account in the new standards that are under consideration. The two most important standards for information modeling of distribution automation systems that are being developed are IEC 61850 and UCA 2.0. Both of these recommend TCP/IP as a common communication protocol. In addition, there is an ongoing work to adapt the existing standards, e.g. ModBus, IEC 870-5-101 and DNP 3.0, to TCP/IP.

This paper discussed the general issues of providing a TCP/IP interface to distribution automation equipment. The two common means how to integrate TCP/IP in a device were presented. An embedded TCP/IP protocol stack sharing the resources of the controller is one alternative. The other possibility is an extension to the controller via a connection box that on the one end has a TCP/IP interface and on the other end connects to e.g. the serial interface of the device. In addition, the security aspects and market trends regarding the widespread use of TCP/IP in distribution automation were discussed. The biggest trends seem to be that TCP/IP will first be used in conjunction to a Web interface for possible configuration operations. Later, when new equipment based on the new standards are in place and when the needs for a telecommunication networks connecting automation, markets and end users together, have grown, TCP/IP seems to be the choice that seamlessly will bind all services together.

In distribution network control cases, TCP/IP packages have to be transported in a multitude of physical media. Due to the variable characteristics of different media type, deterministic communication behavior is difficult to achieve by using plain TCP/IP. Hence, it is necessary to ensure packet transmission up to application level. The DSiP protocol was developed in order to provide a uniform and deterministic communications method between distributed equipment and software modules. DSiP addresses issues such as security, data integrity, reliability, controlled multicasting of data, automated re-routing and optimization of network bandwidth. DSiP provides a solution for deploying modern communication methods allowing for integration of old and new equipment and software into a single, modular and expandable control system.

REFERENCES


