Integration of TCP/IP Based 802 Networks into SCADA Systems

J.I. Escudero, J.A. Rodríguez, M.C. Romero
Dpto. Tecnología Electrónica, ETSII, Universidad de Sevilla
ETSII, Avda. Reina Mercedes, s/n. 41012 Sevilla (SPAIN)
ignacio@us.es

Abstract

Supervisory Control And Data Acquisition (SCADA) systems have traditionally been based on proprietary, low transmission speed networks, due to the special requirements that such systems imposed in terms of network reliability. This is a consequence of the tight temporal needs of real-time applications, which suppose an obstacle when trying to integrate new technologies into them; also, SCADA systems tend not to adopt new technologies until they have been tested enough.

But, over the last decade, a lot of effort has been spent in developing new fast and reliable network standards, reaching such a development level that SCADA systems are beginning to adopt them.

Within this paper we analyze the possibility of using IEC 802 based solutions for the deployment of real-time SCADA information together with typical non time critical enterprise information such as multimedia or database data.

1. Introduction

The main goal of every SCADA [1] system is the remote supervision and control of the facilities' devices, typically sensors and actuators. The information provided by these devices, in example the mediation of the current in a power line is short, not longer than some dozens of bytes. As a result from this, the traditionally used technologies are still suitable for the delivery of devices data, and probably will be in the future.

However, transmission and networking technologies are not the only fields which have dramatically been improved over the last years: multimedia compression techniques have evolved in such a way that digital video and audio can now be processed by cost-effective personal computers, obtaining good quality displays using relative low bit rates. Modern codecs such as MPEG-4 [2] allow compressing both video and audio signals so they can be meaningfully represented using less than 1 Mbps.

The Human Machine Interfaces used to easier the management of the SCADA network operators, typically display the status data as text strings, and in some cases, in the form of symbols representing device state. Complementing that information with video or audio can be of much help when operating wide SCADA networks, where there is usually no staff at remote stations. Security surveillance or videoconference are also another bonus features multimedia information could bring to SCADA systems.

Typical transmission links and protocols used on SCADA networks do not fulfill the bandwidth requirements multimedia data deployment impose, but newest technologies such as Ethernet do.

Ethernet has some characteristics that make it an appropriate candidate to be used not only for such purposes but also for the deployment of device information:

- The high flexibility when choosing the physical medium where the data will be transmitted, and the different transmission speeds available, which allows finding solutions to nearly all needs.
- The low cost and high availability of Ethernet hardware, which can lower the global maintenance spends in the medium run.
- Additionally, using TCP/IP opens the door to client/server architectures such as the OPC industrial standard.

2. SCADA networks

Typical network topology of SCADA systems (as shown in Figure 1) comes in the form of buses, organized into hierarchies, depending on the temporal requirements of the data they have to manage.

Although there is a wide variety of different buses and protocols, we can group them into 3 different bus types [3], [4]:

i) Field buses

Also known as device buses, they usually use serial protocols to transmit few bytes (bits in some cases) per device within a bus cycle, being the info gathered from all devices in the field bus by programmable logic controllers (PLCs). The bus cycle is typically lower than 10 ms.

ii) Control buses

Links the different PLCs with sensors and actuators that make up the field bus. They usually use the same protocol than field buses but have higher cycle times than them, typically 100 ms.

iii) Information buses

They host enterprise services' data, usually not time-critical. These buses were the first that begun adopting Ethernet technology.

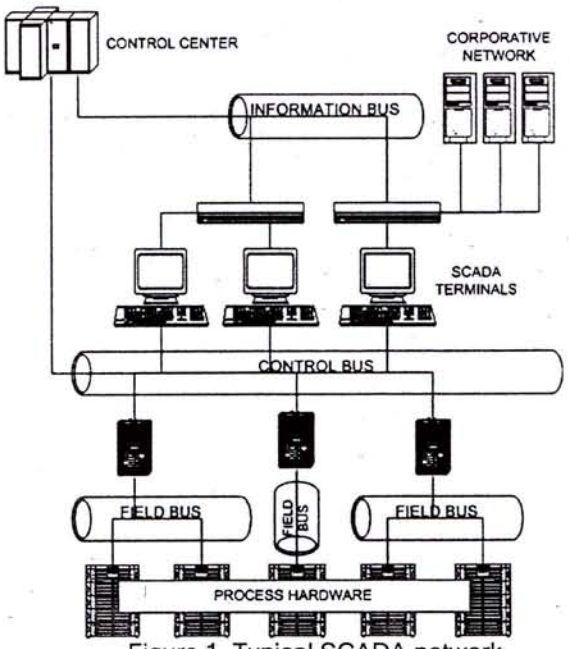

Figure 1. Typical SCADA network

Communication between devices in the same facility is used performed using RS232 links, although power line or fiber optic links are also common.

For long distances, low-speed radio links have traditionally been the common choices.

3. Drawbacks of mass-market Ethernet hardware

The benefits of using Ethernet are undoubtful, but typical commercial Ethernet products are not adequate to work on tough-environment conditions as those present on factories or remote electrical facilities: the higher temperature and the exposure to electric-magnetic and/or radio frequency disturbances could cause dysfunctions to Ethernet devices. Although the effect of perturbations can be partially solved using fiber optic links, chasing of common commercial devices is not usually adequate to work on industrial environments.

Another important inconvenience of common Ethernet 802.3 [5] compliant hub devices is the lack of determinism. Usual Carrier Sense Multiple Access with Collision Detection (CSMA/CD) medium sharing techniques used by Ethernet, due to packet collision, do not assure the device to immediately access the medium. This variable, unpredictable delay makes devices not to be suitable for real-time transactions.

To avoid these drawbacks, a new industrial standard for 802.3 networks has been defined: Ethernet/IP [6] or Industrial Ethernet, which is gradually replacing the existing proprietary networks:

- Devices built under this standard reduce the probability of packet loss to nearly 0%. Full-duplex switches devices overcome this problem)
- They have adequate chasing and components allowing them to work on harsh conditions. Devices supporting a temperature range from 0°C to 70°C conform to industrial standards.
- They also have a higher Mean Time Before Failure than their mass-market counterparts, being this feature of great importance in SCADA systems, as temporary losses could cause a big impact to the system integrity.

4. Network design

The proposed solution is based on a mixed Ethernet & Ethernet/IP core: Ethernet/IP solutions to be used for field devices placed on tough environments, and mass-market Ethernet switching equipment for the remaining network devices.

Proper network segmentation is recommended, which allows improving performance by reducing possible collisions, and, at the same time, separates time critical information from enterprise data such as video-conference, e-mail and other non time critical, network-based services. This segmentation can be performed physically, using different repeaters (e.g. switches) for each type of data, or using same devices and links for all data but having devices that support packet prioritization, as some routers do.

In respect to adequate transmission mediums, the usage of unshielded twisted-pair links is possible on short distance links, although care must be taken with regard to disturbances. The use of triaxial, shielded twisted pair (STP) or fiber optic cabling is the usual solution when working on harsh conditions.

Fiber optic based on 802.3 and/or wireless 802.11 [7] links are the recommended solutions for communicating long distance nodes.

On new facilities, the current trend when choosing the transmission medium between remote stations and control center(s) consists in the usage of fiber-optic links. These high-speed links could be used as main backbones for

transmitting all SCADA's hardware data as well as enterprise data to control centers.

Old remote facilities which use low-speed radio links to communicate with control center could easily be migrated to use the 802.11 technology.

If distance to control center is too long, remote facilities could be connected to their nearest facility in the network. This latest facility's link should be capable of managing all his data as well as the data that comes from facilities that use it as a gateway to the control center.

5. Integrating proprietary devices into 802 networks

A major obstacle for the adoption of Ethernet technologies in SCADA systems is that they usually are large-scale systems, so migrating existing devices to Ethernet suppose huge expenses that only few enterprises are willing to invest. Therefore, a gradual migration is the best solution in such cases.

Main candidates to be the latest being migrated are sensors, actuators and/or PLCs present on remote installations, as there are few of them that support Ethernet.

Among other tasks made on the IDOLO project, we have performed some lab tests where the signal transmitted by a Multitrans device (which gives data about the voltage and intensity of a powerline among other features) was injected in a Ethernet network, and received by a remote computer running iFIX SCADA/HMI system. Multitrans device transmits its data using Procome protocol (based on IEC870 protocol [8]) using a multimode fiber optic output. We used a fiber optic<->RS232 medium converter to connect it to the IS-SERVER device.

Figure 2 shows how this integration can be performed in a transparent way to both the Multitrans data acquisition device and the remote supervision station.

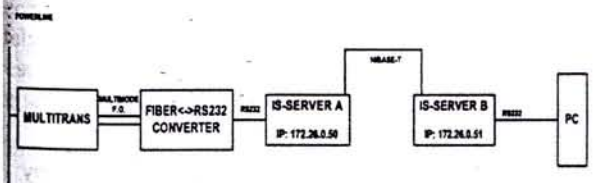

Figure 2. Basic SCADA device integration

Following Ethernet/IP specification we avoided the use of hubs in favour of the more determinist switches; in our tests we used two 4-port 10BASE-T switches connected via uplink ports using multimode fiber optic cabling, being the data received by the remote monitoring-PC using an RS-232 communications port.

To do so, the SCADA device needs a MAC hardware address so switches or other networking devices can handle it; consequently, additional hardware is needed, and the solution comes by the hands of a bi-directional serial to Ethernet converters, which add the needed hardware addresses.

To do so, we used the previously mentioned IS-SERVER device, which performs bi-directional RS232<->10BASE-T medium conversion, packing the serial data into TCP/IP packets. This device is fully configurable, allowing setting packets source and destination IP addresses and TCP ports. Latency introduced by all devices and cabling along the packets way through the network is vital on time-critical transactions, so we have measured the latency between both endpoints obtaining results smaller than 1 ms (the maximum resolution of MS-Windows timers).

The basic structure of our test system can be seen in Figure 3.

In our preliminary tests, we detected delays of about 100 ms when receiving some packets, which after a careful analysis showed to be caused by the IS-Server devices. This strange behavior was caused by the fact the devices were prototypes, still in an early stage of development. Such a behavior in any of the network devices would endanger correct deployment of real-time data on SCADA systems, so special care must be taken with the latency introduced by devices within the network.

These problems have been solved with newer, more reliable versions of those IS-Server devices, so we were now able to proceed with new lab tests. These new tests will consist on analyzing the normal behavior of the SCADA data streams in our test scenario, then injecting large amounts of data in the form of video streams, to study the effect network congestion might cause due to packet collisions and bandwidth usage.

6. Conclusions

Within this paper we describe our attempts to integrate the widely spread Ethernet arquitectures into SCADA systems. Due to the high development level reached by current network technologies such integration is now possible, but it's not a trivial task due to the tight temporal requirements imposed by real-time SCADA systems.

A careful network design has been proposed to avoid potential perturbations that could affect network reliability, which could compromise SCADA system integrity.

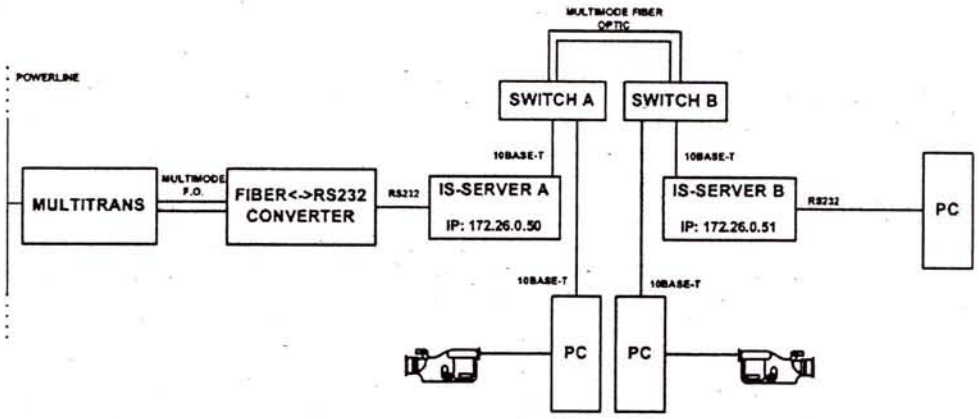

Figure 3. Basic test network

It's absolutely unwise to use hubs because of their non time-determistist nature, which could end in delays not suitable for sending real-time data. Switches are nowadays the most cost-effective network devices that meet all the requirements needed to interconnect the different subnetworks that make up the entire SCADA network; they solve the determinism drawback of hubs and own a MAC address.

One of the main problems we have faced with is how to encapsulate SCADA data, which usually is sent using serial proprietary protocols. The solution comes in the hand of bidirectional Serial/Ethernet converters, which also must have a MAC address so communication can be performed between them and other Ethernet devices.

Our preliminary tests showed (although more tests are needed in order to analyze the effects of network congestion) that such integration is possible, opening then door to substantial improvements in the functionality and usage of traditional SCADA systems, thanks to a more generic structure and the higher amounts of bandwidth available for enterprise services.

The usage of Ethernet into SCADA systems can decrease the maintenance costs as well as improve the adaptability of systems to future standard technologies.

7. References

[1] S. A. Boyer, "SCADA: Supervisory Control And Data Acquisition, 2nd Edition", ISA – The Instrumentation, Systems and Automation Society, New York (United States), 1999.

[2] "Information technology – Coding of audio-visual objects – MPEG-4", ISO/IEC 14496, 1999

[3] J. Aiza, and R. Safont, "Buses y dispositivos para comunicaciones industriales", *Automática e Instrumentación*, Cetisa Editores, Barcelona (Spain), June 2000, pp. 93-129.

[4] P. Dillon, "Fieldbus and Control Network Technologies", Research Studies Pr., 2001.

[5] "Information technology – Local area networks – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification", IEEE/IEC 802-3, 1996.

[6] "Ethernet/IP Specification 1.0", ControlNet International and the Open DeviceNet Vendor Association., http://ethernet-ip.org., 2001.

[7] "Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification", IEEE/IEC 802-11, 1997.

[8] "Telecontrol and equipment systems – Part 5: Transmission protocols", IEC 60870-5, 1990.

8. Acknowledgements

The work described in this paper has been funded by the Ministerio de Ciencia y Tecnología thorugh the project reference number TIC2000-0367-P4-02.

We'd also like to thank ISIS Engineering (Seville) for providing us with IS-SERVER prototypes.