# DISTANCE CONTROL OF MECHATRONIC SYSTEMS VIA INTERNET

[*]Tibor VINCE, [**]Irena KOVÁČOVÁ
[*]Department of Theoretical Electrical Engineering and Electrical Measurement, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Park Komenského 3, 042 00 Košice, E-mails: tibor.vince@tuke.sk
[**]Department of Electrical Engineering, Mechatronics and Industrial Engineering, Faculty of Electrical Engineering and Informatics, Technical University of Košice, Letná 9, 042 00 Košice, E-mail: irena.kovacova@tuke.sk

## SUMMARY

*The article presents possibilities of distance remote via Internet. The Internet protocols divided by OSI model that can be used for controlling and regulations are discussed with final focusing on TCP and UDP protocols and comparing these protocols from the controlling point of view. The paper is analyzing advantages and disadvantage of using the Internet in different level of the existing levels in the information hierarchy and the delay time problem in communication via Internet. The item compares more buses used in distance remote. It contains also some distance remote control system proposal.*

***Keywords:*** *control systems, communication protocols, Internet*

## 1. INTRODUCTION

The Internet is playing an important role not only in information retrieving, but also in industrial processes manipulation. Distance remote via Internet, or other words, Internet-based control is a new concept of controlling, which has been paid much attention in these years. IFAC has held the first workshop on Internet Based Control Education in Spain (2002). The ScadaOnWeb system funded by the European Council from September 2001 to August 2003 targets Internet-based protocols enabling process, monitoring and optimization via the web. This type of control system allows remote monitoring or regulation of plants or single devices over the Internet. With the progress of the Internet it is possible to control and regulate from anywhere around the world at any time. The design process for the Internet-based control systems includes requirement specification, architecture design, control algorithm, interface design and possibly safety analysis.

Specifying requirements for Internet-based control systems is the first task in the design process because different requirements may lead to different control architectures. Architecture design is the second step in the design process of Internet-based control systems. The requirements specification should be met in the architecture design [1].

Many requirements validation techniques involve building prototypes or executable specifications or waiting until the system is constructed and then testing the whole system. It could be too late and too expensive by that time to make any change in specification for control systems although certainly much can be learned by "testing" a specification. Very little work has so far been done on requirements specification for control systems design.

Due to the low price and robustness resulting from its wide acceptance and deployment, Ethernet has become an attractive candidate for real-time control networks. However, it is difficult to build a real-time control network using the standard Ethernet because the Ethernet MAC (Medium Access Control) protocol - persistent CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol may cause unpredictable access delay.

Our approach is to explore now days possibilities for Internet based controlling of mechatronic systems, eventual trends, compare UDP and TCP protocols from the controlling point of view, review of advantages and disadvantages of distance remote via Internet in different level of information hierarchy and possible solutions.

## 2. INTERNET PROTOCOLS

The Internet protocols are the world's most popular open-system (non-proprietary) protocol suite because they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. One common tool used for comparing different kinds of protocols is the OSI Reference Model, which is the simplistic breakdown of networking functions from the physical wiring up to the applications that run on the network. By comparing TCP/IP to the OSI Reference Model, it is easier to understand how each of the major protocols interacts with each other.

The OSI Reference Model is a conceptual model that uses seven "layers" to identify the various functions provided by a network, and these seven layers can be used to compare different protocols using a common framework. Each layer within the OSI Reference Model has a very specific function, and each layer depends on the other layers in order for the entire model to function properly. Each layer only communicates with the layers immediately above or below it. Not all networking technologies have seven layers, nor do they all match up to the seven layers in the OSI Reference Model exactly. The following text briefly describes each of the seven layers, the purpose each serve and the protocols of given layer:

*The physical layer* is concerned with the physical wiring used to connect different systems together on the network. Without strictly standardized definitions for the cabling and connectors, vendors might not implement them in such a way that they would function with other implementations. There is no defined protocol for physical layer.

*The data-link layer* defines how information is transmitted across the physical layer, and is responsible for making sure that the physical layer is functioning properly. If there are any problems with transmitting, this layer must deal with those errors, either attempting to retransmit the information or reporting the failure to the network layer. For this layer are defined Address Resolution Protocol (ARP) and Reverse ARP (RARP).

*The network layer* is used to identify the addresses of systems on the network, and for the actual transmission of data between the systems. The network layer must be aware of the physical nature of the network, and package the information in such a way that the data-link layer can deliver it to the physical layer. For this layer are defined Routings protocols, Internet Protocol (IP) and Internet Control Message Protocol (ICMP).

*The transport layer* provides the reliability services lacking from the network layer, although only for basic transmission services, and not for any application- or service-specific functions. The transport layer is responsible for verifying that the network layer is operating efficiently, and if not, then the transport layer either requests a retransmission or returns an error to the layer above it. For this layer are defined Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) [3].

*The session layer* and the presentation layer are rarely supported therefore we will not concern with.

*The application layer* provides the network's interface to end-user application protocols such as http, ftp, telnet etc.

### 2.1. Protocols UDP and TCP

All the transport-layer protocols (including TCP and UDP) use IP for their basic delivery services. The IP is an unreliable protocol, providing no guarantees that datagrams or packets will reach their destination intact. For applications that need some sort of guarantee that data will arrive at its destination intact, this uncertainty is simply unacceptable. There are two standard transport protocols that applications use to communicate with each other on an IP network. These are the User Datagram Protocol (UDP), which provides a lightweight and unreliable transport service, and the Transmission Control Protocol (TCP), which provides a reliable and controlled transport service.

The Transmission Control Protocol (TCP) provides a reliable, connection-oriented transport protocol for transaction-oriented applications to use. TCP is used by almost all of the application protocols found on the Internet today, as most of them require a reliable, error-correcting transport layer in order to ensure that data does not get lost or corrupted. This reliability is achieved through the use of a virtual circuit that TCP builds whenever two applications need to communicate. TCP provides five key services to higher-layer applications: Virtual circuits, Application I/O management, Network I/O management, Flow control and Reliability. These services make TCP an extremely robust transport protocol.

The User Datagram Protocol provides a low-overhead transport service for application protocols that do not need (or cannot use) the connection-oriented services offered by TCP. UDP is most often used with applications that make heavy use of broadcasts or multicasts, as well as applications that need fast turnaround times on lookups and queries. UDP is more appropriate for any application that has to issue frequent update messages or that does not require every message to get delivered.

In case of TCP packet, receiver to sender must acknowledge every successful delivered packet. That means TCP must be generated double amount of packet and the network could be overworked by huge amount of packets. Therefore TCP protocol is not suitable for transport of monitoring data (where data is transferred many times per second). For this transfer is much suitable UDP protocol. For other type of data transfers (for instance transfer of commands) is much suitable protocol TCP [3].

### 2.2. Network performance

There are more parameters in mutual relationship, which refer to network condition or network performance. One of performance parameters is Latency. Latency means a time required to transfer an empty message between relevant computers. It is total sum of delay introduced by the sender software, delay introduced by the receiver software, delay in accessing the network and delay introduced by the network.

Another parameter is Data transfer rate. Data transfer rate is the speed at which data can be transferred between sender and receiver in a network, once transmission has begun. The unit of this parameter is Bits/sec. For message transfer time calculating is equation 1,

$$MTT=L+(LM/DTR) \qquad (1)$$

where MTT is Message Transfer Time, L is Latency, LM is Length of Message and DTR is Data Transfer Rate

A third parameter of network performance is Bandwidth. Bandwidth is a total volume of traffic that can be transferred across the network. Maximal data rate formula is shown in equation 2,

$$MDR=CB \cdot \log2\ (1 + (S/N)) \qquad (2)$$

where MDR is Max. Data Rate (bps), CR is Carrier Bandwidth, S is Signal and N is Noise. This maximum is only theoretical, not reachable in practice [5].

The all parameters are pointing on the main disadvantage of controlling via the Internet – packets delivery delay. It is difficult to build a real-time control network using the standard Ethernet because the Ethernet MAC protocol and CSMA/CD protocol may cause unpredictable access delay. When packets are concurrently transported over an ordinary Ethernet, packets may experience a large delay due to contention with other packets in the local node where they originate and collision with other packets from the other nodes. In first case, there is "only" delay in packet transport. In second case there are damaged packets and need to be retransmitted (in case of reliable service). By data transmission, four sources of delay spring up at each hop: nodal processing, queuing, transmission delay and propagation delay. The most significant part of total delay belongs to queuing. By queuing is considered the following equation 3,

$$TI = L * A/W \tag{3}$$

where TI is traffic intensity, L is packet length (bits), A is average packet arrival rate, and W is link bandwidth (bps).

If ratio L*A/W will be very small almost 0, average queuing delay is small. If ratio L*A/W rise up to 1, delays become large (exponentially) and if ratio L*A/W is bigger than 1 average delay is infinite, more "work" arriving than can be serviced.

## 3. INFORMATION ARCHITECTURE

It is becoming increasingly necessary to think in terms of integration of information and control, across the entire plant site. In manufacturing industries this is often referred to as "Computer Integrated Manufacturing" (CIM). In process and power industries these are called "Plant-Wide Systems" (PWS). An effective PWS makes possible improved plant energy efficiency, better monitoring, manpower savings, and equally important, effective integration of the plant with the company as a whole. On the surface, it would seem that the increasing use of microprocessor-based plant level devices such as programmable controllers, distributed digital control systems, smart analyzers, personal computers, etc., would make this easy. After all, most of these devices have "RS232" connectors, which enable connection to computers. Unfortunately, the real world situation is somewhat more challenging. If we began hooking all these RS232 ports together, we would soon have an unmanageable mess of wiring, and custom software, and little or no communication. To date, this has been the usual result, where "point solutions" have been implemented without an overall plan to integrate these devices into a meaningful "Information Architecture". This Information Architecture can be separated into 4 levels with the sensor/actuator level as shown in Fig. 1, which are distinguished from each other by"4Rs" principle criteria.

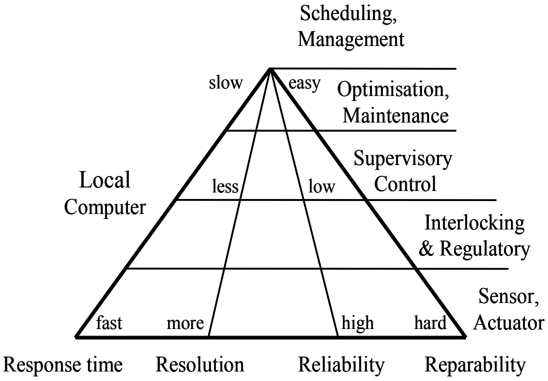

**Fig. 1** Information Architecture

The 4Rs criteria are: Response time, Resolution, Reliability and Reparability.

*Response time*: as one moves higher in the information architecture, the time delay, which can be tolerated in receiving the data, increases. Conversely, information used at the management & scheduling level can be several days old without impacting its usefulness.

*Resolution*: Abstraction levels for data varies among all the levels in the architecture. The higher the level is, the more abstract the data is.

*Reliability*: Just as communication response time must decrease as one descends through the levels of the information architecture, the required level of reliability increases. For instance, host computers at the management & scheduling level can safely be shut down for hours or even days, with relatively minor consequences. If the network, which connects controllers at the supervisory control level and/or the regulatory control level, fails for a few minutes, a plant shutdown may be necessary.

*Reparability*: The reparability considers the ease with which control and computing devices can be maintained.

Local computer on supervisory control level is able communicate with higher levels of information architecture via Internet, but there is also possibility to use the Internet also in lower levels of the Information architecture. The Internet can be linked with the local computer system at any level in the information architecture, or even at the sensor/actuator level. These links result in a range of 4Rs (response time, resolution, reliability, and reparability). For example, if a fast response time is required a link to the control loop level should be made. If only abstracted information is needed the Internet should be linked with a higher level in the information architecture such as the management level or the optimization level.

Table 1 shows a simple evaluation for the possible links. This table can be used to guide the selection of the links.

| Existing Information Level | Information Exchange | Advantages | Disadvantages |
|---|---|---|---|
| Management level | Commercial data systems | Enable the commercial data to their customers and managers | Not suitable for real time monitoring and control tasks. |
| Plant-wide Optimisation Level | Global Database | Easily achieving the plant-wide information of process plants. | Not suitable for real time monitoring and control tasks. |
| Supervisory Level | Process Database | Easily achieving the real-time status of process plants, suitable for implementing advanced control. | Missing management information. |
| Regulatory Level | PLC, Control Unit | Allowing controllers to directly talk to the Internet | Introducing a high risk of being attacked by malicious hackers, Internet delay |
| Sensor/Actuator Level | Smart-Devices | Monitoring and controlling the smart-devices directly from the Internet | Introducing a high risk of being<br>attacked by malicious hackers, Internet delay |

**Tab. 1** Links between the Internet control level and existing control levels

## 4. SYSTEM ARCHITECTURE

Suitable way for distance remote architecture demonstration could be architecture for distance remote of mechatronic system.

One of the ways of monitoring Mechatronic system is to use a virtual reality or other visualization software. However, the slow rate and instability of the Internet connection restrict the real-time control and feedback of remote tasks. To efficiently implement the teleoperation of mechatronic system, most systems apply visualization tools to simulate the environment. The main advantage is the achievement of fast response to the operator's actions because smaller data package is required to update the virtual mechatronic system and its environment. It provides the operator with a "live" virtual representation of the scene instead of the delayed video images.

It can also increase the efficiency of the operator performance because the operator can choose appropriate points of view, zoom the scenes and make some objects transparent or semitransparent, etc. The augmented reality can also be used in the system to get a better visualization and help the operator get more immersion of the virtual environment.

In the architecture design, a distance remote mechatronic system generally includes three major parts: client, server and controlled mechatronic system. The general remote mechatronic system architecture is shown in Figure 2. The client part is the interface for the operations. It includes computers, visualization software with user interface for operators. Client computer receives state information of remote mechatronic system via Internet. Received information will be processed and evaluated in remote computer.

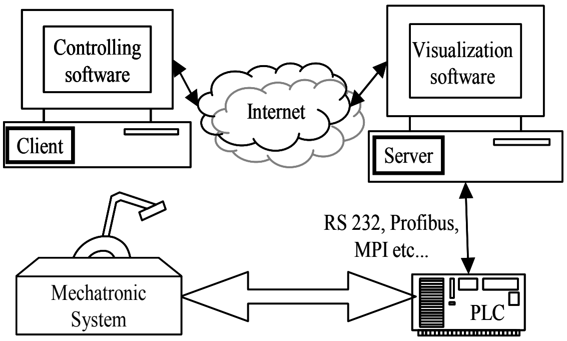

**Fig. 2** Remote system architecture

The server part contains a server computer, which is connected to the real mechatronic system. Some systems also include different sensors for different purposes or an on-site camera with an image acquisition board sometimes. The server software includes different models of data processing such as sensor data acquisition and processing. Server contains all required drivers and devices for communication with mechatronic system. Communication of server with mechatronic system could be based on several ways (RS232, Profibus, MPI etc.). Server can be connected with mechatronic system directly (server is directly connected with all sensors and actuators), or indirectly (server is connected with control unit of mechatronic system – PLC, microcontroller, etc., but these days is also Ethernet based connection possible). The third part of system architecture is mechatronic system itself. It contains all sensors, actuators and all devices with specific purpose.

Common way for distance remote is, when remote client computer has limited functions – only start/stop of mechatronic system, or choosing specific program for mechatronic system to run on server site. But Internet speed progress open possibility for real-time control from client site. So there is possibility that server would serve only as an interface between remote client and mechatronic system. This way of distance remote is possible, if the mechatronic system is “sufficient slowly” and server-client connection is sufficient fast.

### 4.1. Buses in Industry

There are more types of buses using in Industry. to connect of various devices, which are supported on the type of interface/bus [6]:

*AS-Interface* – the Actuator Sensor Interface offers many of the benefits of more powerful and expensive fieldbuses, but at much lower cost and as a much simpler installation. Transmission of analog signals via time multiplex procedure. Data and power via the same line. No termination necessary. Address setting automatically from the master or via service tool. ASI conforment power supply required. It supports 62 nodes, max 300m with 3 repeaters. Date rate is 167kbit/s. Addressing is Master/Slave.

*CANopen* – is a CAN-based higher layer protocol. It was developed as a standardized embedded network with highly flexible configuration capabilities. Node removal without severing the network is possible. Provisions for the typical request/response orientated network communications. Provisions for the effiecient movement of data framentation for moving larger bodies of information It supports 127 nodes, 25-5000m (depending on boudrate). Data rate is from 10kbit/s to 1Mbit/s, addressing is Master/Slave, Peer-to-Peer, Multi-cast and Multi-master.

*ProfiBus* – is a Multi-Master System and makes possible the mutual operation of several automation, engineering or visualizing systems at a Bus. The Masters, also designated as active devices, define the data traffic on the Bus. When in possession of the access permission (Token), they can send data without external requests. The Slaves, designated as passive devices, have no Bus access permission. They can only confirm received messages or send messages when requested by a Master. Baud rates from 9.6 kBaud up to 12 MBaud are supported. A maximum of 126 devices can be operated at the Bus. Profibus also supports Broadcast and Multicast communication. Network length is possible 100-1200m, addressing is DP: Master/Slave, Cyclic, Polling, DPV1: Cyclic, Polling + acyclic data transfer.

*EthernNet/IP* – The Industrial Ethernet Protocol (Ethernet/IP) has been developed by ODVA with strong support from Rockwell Automation. It uses the Control & Information Protocol (CIP) which is already well known from ControlNet and DeviceNet. Network size (number of nodes) is scalable and nearly unlimited. Network size can be 100m (10/100 Base-T) or 35-2000m (fiber optic). Standard layers 1-4 providing Ethernet data transmisson, bus access, internet protocol (IP) and TCP & UDP protocols. CIP "implicit" and "explicit" messaging with encapsulation technology. Message routing between EtherNet/IP, DeviceNet & ControlNet.

## 5. CONCLUSION

Nowadays, a lot of control elements have been embedded with Internet-enabled functions, for example, PLC with TCP/IP stack, smart control valves with a built-in wireless communication based on TCP/IP protocol, and process control computer (DCS) with an Internet gateway. There possibility that some mechatronic system could be connected directly to the Internet (without a necessity of a server computer). On the basis of done analysis is evident that the existence of server as a gate to the Internet for mechatronic system is still highly recommended (because of capriciousness of Internet, computer crime and many other reasons). By utilizing of UDP Internet protocol it is possible to regulate real-time systems with tenths milliseconds of feedback. When compare Ethernet as a bus with other standard types of industrial bus, there are more advantages and disadvantages. The most powerful advantage is nearly unlimited size of bus, possible huge distance, open system of the internet protocols and accessibility of the Internet. The main disadvantage stills unpredictable time delay and security (hackers).

## ACKNOWLEDGEMENT

The paper has been prepared by supports of Slovak Grant Agency as project No.1/4174/2007 and KEGA project No. 3/5227/07.

## REFERENCES

[1] Yang, S.H., Tan, L.S., Chen X: Requirements Specification and Architecture Design for Internet-based Control Systems, proceedings of the 26th Annual International Computer Software and Applications Conference (COMPSAC’02), 2002.

[2] Kweon, S. K, Cho M., Shin K. G.: Soft Real-Time Communication over Ethernet with Adaptive Traffic Smoothing, IEEE Transactions on parallel and distributed systems, VOL. 15, NO. 10, October 2004.

[3] Hall E.: Internet Core Protocols: The Definitive Guide, O'Reilly & Associates (February, 2000) USA, ISBN: 1-56592-572-6.

[4] Yang, X., Chen Q.: Virtual Reality Tools for Internet-Based Robotic Teleoperation, proceedings of the 8th IEEE International

Symposium on Distributed Simulation and Real-Time Applications (DS-RT'04).

[5] Fonda C., Postogna F.: Computer networking basics, ICTP workshop on telecommunications: science, technology and applications. Trieste, 15th September - 3rd October 1997

## BIOGRAPHIES

**Tibor Vince** - He finished his studies in 1986 at the Technical University of Košice, Department of Industrial Engineering. From this time he has been study the doctoral study program from the expert field of electrotechnical systems. Now he works as computer net supervisor at KOGER company – Dublin (Ireland). His working interest is mainly focused on the field of computer net management and Internet communication protocols.

**Irena Kováčová** - She finished her studies in 1982 at the Technical University of Košice, Department of Electrical Drives, area – Power electronics with excellent evaluation. From this time she has worked at the Department of Electrical Drives, first as an assistant lecturer and now as an associate professor. In 1988 she got her doctoral diploma. In 1991 she got the Award of the Minister of Education for the Development of Science and Technology. Her working interest is mainly focused on the field of power electronics, especially on the construction of converters and inverters with new perspective elements and computer simulation of new power semiconductor parts and devices.