„Aurel Vlaicu” University of Arad
Faculty of Engineering

Scientific and Technical Bulletin

Series: **Electrotechnics, Electronics, Automatic Control and Computer Science**

Vol. 4, No. 1, 2007

ISSN 1584-9198

Aims & scope

The *Electrotechnics, Electronics, Automatic Control and Computer Science* series of the Scientifical and Technical Bulletin of the „Aurel Vlaicu” University of Arad will devote it self to the dissemination of the original research results, technical advances and new items in Electrical and Computers Engineering and in Knowledge Engineering.

The team of the *Automate Control and Applied Software Department* of the above denominated academic institution is intending to build mutual benefic interactions with researchers and institutions in the field.

Published 4 times a year

All papers are refereed through a double blind process. A guide for authors, sample copies and other relevant information for submitting papers are available at **http://uavsb.xhost.ro**

Please send the submitted paper via e-mail to:
Dr. Valentina E. Balas
http://www.drbalas.ro/uav_scientific_bulletin.htm

ISSN 1584-9198

Table of Contents

SWITCHING CONTROL BY PHASE TRAJECTORY *7*
Marius M. BALAS, Jean DUPLAIX

ANALYZING SECURITY MECHANISMS IN WLAN *19*
Anton POLICEC, Gheorghe MÜLEC, Eugen MÂRZA

SECURITY COST OF IEEE 802.11 WIRELESS LAN *29*
Anton POLICEC, Gheorghe MÜLEC

EDUCATIONAL ASPECTS IN CONTROL SYSTEM DESIGN TECHNOLOGY *41*
Sorin NANU

IMPLEMENTING OF A CONTROL SYSTEM FOR PNEUMATIC PROCESS *53*
Sorin NANU

PROLOG EXPERT SYSTEM: THE DIAGNOSIS OF KIDNEY DISEASES *63*
Eugene ROVENȚA, George ROŞU

Marius M. BĂLAŞ
„Aurel Vlaicu" University of Arad,
Engineering Faculty
Bd. Revoluției nr. 77, 310130, Arad, Romania
E-mail: marius.balas@ieee.org

Jean DUPLAIX
Université du Sud Toulon-Var
Toulon
B.P. 20132
83957 LA GARDE cedex, France
E-mail: duplaix@univ-tln.fr

SWITCHING CONTROL BY PHASE TRAJECTORY

NOTE: This paper was presented at the International Symposium "Research and Education in an Innovation Era", Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

-

ABSTRACT:

The paper is discussing the instability that can occur in the case of switching controllers. The qualitative analyze of the switching phenomenon is performed by means of the phase trajectory of the difference between the controllers outputs. The significant regions of the phase plane are investigated. The second and the fourth quadrants are recommended for switching, while the first and the third quadrants must be avoided. An analogy with the sliding mode method is proposed

KEYWORDS:

Switching controllers, phase trajectory, qualitative control, fuzzy interpolative controller, sliding mode.

1. INTRODUCTION

The switching controllers problem

The limits of the frequency analyze methods are showing in control problems for which the initial values are playing important roles. Such a case appears in the switching controllers' applications. Two relevant conclusions, proved by specific benchmark studies and an extended overview of the existing literature are presented in [1]:

- a switching system can be potentially destabilized by an appropriate choice of the switching signal, even if the switching is between a number of Hurwitz-stable close loops systems; this possibility exists even in the case of identical switched systems;
- the implementation particularities of the control system can produce the same effects.

There are applications where the switching controllers instability can produce fatal consequences. For example, in particular circumstances, the instability produced when switching between automate pilot and manual pilot may cause airplane crashes. In fact these kind of effects may appear in each technological process, when automate and manual controls are switching.

This paper is continuing a previous work [2] with new arguments that were partially discussed in [3].

2. POSSIBLE EXPLANATIONS FOR THE SWITCHING CONTROLLERS INSTABILITY

Detailed and precise studies of the switching linked phenomena were reported mostly for the linear systems [4]. For the nonlinear systems it is more difficult to draw precise conclusions because of the huge diversification of the problem and of the lack of a unified theory.

The frequency analysis (using the transfer functions) has few chances to produce positive results in this case, taking in consideration the fact that this theory is essentially founded on the hypothesis of the null initial conditions. That is why Hurwitz-stable systems can be destabilized by perturbations.

There are some possible explanations for the quasi unpredictable instabilities that appear occasionally in the switching controllers systems:

- a commutation represents a discontinuity by itself, transitory effects are inherent;
- control algorithms need a perfect state initialization for the moment of the switching;
- the digital control systems are fundamentally affected by the digitization operation (sampling and encoding); that is why most of the time the digital control systems are actually working in open loop and odd unexpected dynamic effects are always possible.

In [2] and [3] we analyzed the switching controllers' problem with the help of the phase trajectories. The phase trajectory can fully support the design of switching controllers for linear systems [4]. Our aim is to move this technique towards nonlinear, replacing the precise control of the phase trajectory that can be achieved in linear systems by the Clocksin-Morgan qualitative analysis [5]. The method was already used for self adaptive control [6] and can be easily implemented with fuzzy-interpolative expert systems [7].

3. A BENCHMARK STUDY: A PI TO PD SWITCHING CONTROL FOR A DC DRIVE

Let us consider the case of a d.c. electric drive (P = 12kW, U_{nom} = 220 V, n_{nom} = 685 rpm) whose speed is controlled either by a PI controller (proportional gain = 25, integral = 10 gain) or by a PD one (proportional = 25 gain, derivative = 0.1 gain) [1]. The main window of the Matlab-Simulink model is presented in fig. 1. This configuration is taking advantage of the precision of the PI controller in steady regimes and the robustness of the PD controller in transient regimes.

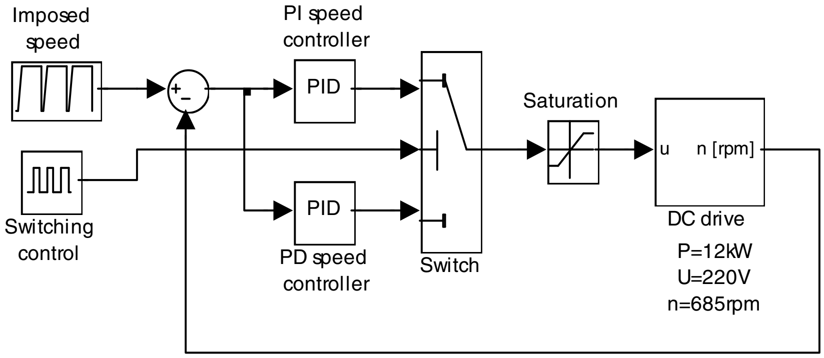


Fig. 1. The d.c. driver and the two switched PI and PD controllers

The scenario of the simulations is the following: we will impose a 600 rpm speed step that should be accomplished in one second and we will introduce a loading torque at t = 5s. The basic idea is to switch from the PD controller to the PI one after 5s, for instance at t = 7s. The resulting performance for the previous scenario is the expected one.

Now let us change the PI to PD switching and the moment of the switching before the loading of the drive, for instance at t = 3s. The system becomes unstable as one can see in **fig. 2**.

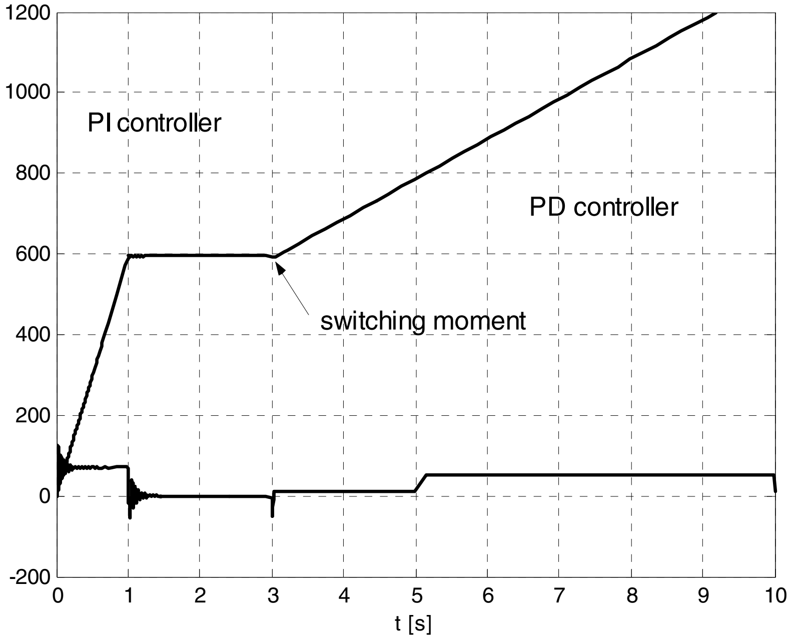


Fig. 2. Instability induced by a PI to PD commutation at t = 3s

Analyzing the state variables one can easily notice that the outputs of the two controllers are very different in the moment of the commutation (see **Fig. 3**). It is natural to assume that the origin of the instability is connected to this difference.

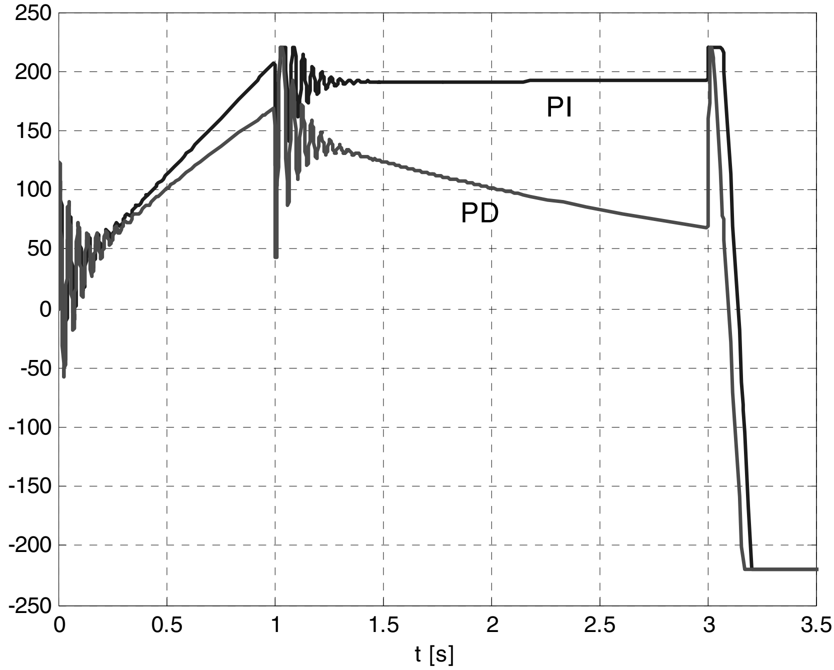


Fig. 3. The outputs of the two controllers

Other empirical observations drawn from simulations [2]:

- the instability may evolve in both senses: positive as in fig. 3 but also negative;

- the instability appears as well in the case of same type controllers;

- the instability is finally producing the saturation of the controller, but its causes are not necessarily linked to the saturation;

- changing the parameters of the integration used for the simulation is producing significant changes and even the disappearing of the instability; in a correct perspective we can conclude that the instability is appearing only in digital systems and it is linked to the sampling operation and the integration method.

Based on these observations one can conclude that the switching controllers' instability is linked to the initial conditions, as well as to the very essence of the numeric calculus.

4. THE QUALITATIVE ANALYSIS OF THE PHASE TRAJECTORY OF THE ERROR

Since the Laplace operational calculus is useless as a tool in this case, we will replace it with the *phase trajectory of the error* (PTE). Originally PTE refers to the control error in close loop control systems. In this case the error *er* will be defined as the difference between the outputs of the switching controllers PI(t) and PD(t) [2]:

$$er(t) = \mathrm{PI}(t) - \mathrm{PD}(t) \qquad (1)$$

er and its derivate *cer* corresponding to the fig. 6 simulation are shown in fig. 4.

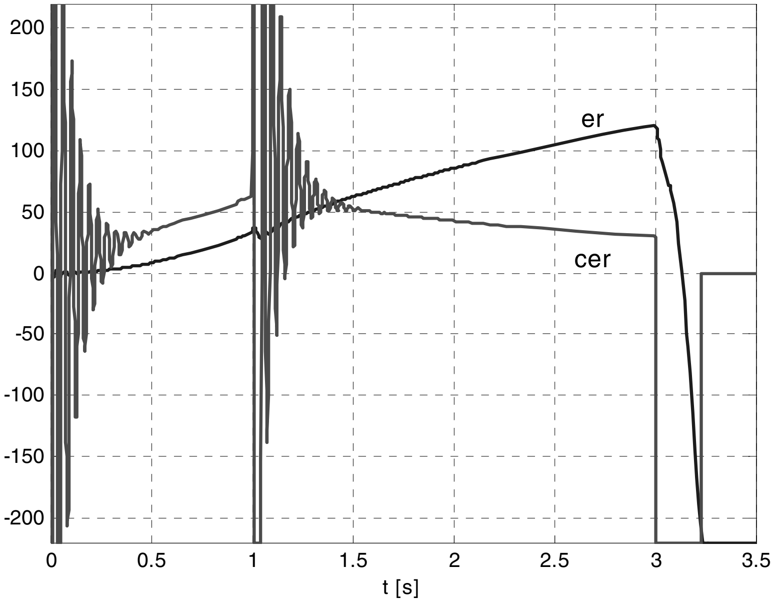


Fig. 4. The error and its derivate, for the case of the switching controllers

The PTE that is resulting after filtering the high frequency components (see fig. 5) can be used for analyzing the causes of the oscillatory or unstable commutations, as well as for the choice of a low risk switching moment. The technique is identical for the case of nonlinear controllers and/or processes. The option for this linear example is made rather for methodological reasons: the time responses are very simple and easy to interpret.

A first observation is that the commutations executed while the PTEs are located into the first or the third quadrants presents high risks for instability, while the second and the forth quadrants are recommendable for commutations. The risk of producing instability decreases massively according to our experience if we have in mind this primary criterion when choosing the switching moment. Our observations are pointing to a particular high risk zone in the first (third) quadrant: the one limited by max(*cer*) and max(*er*) [2].

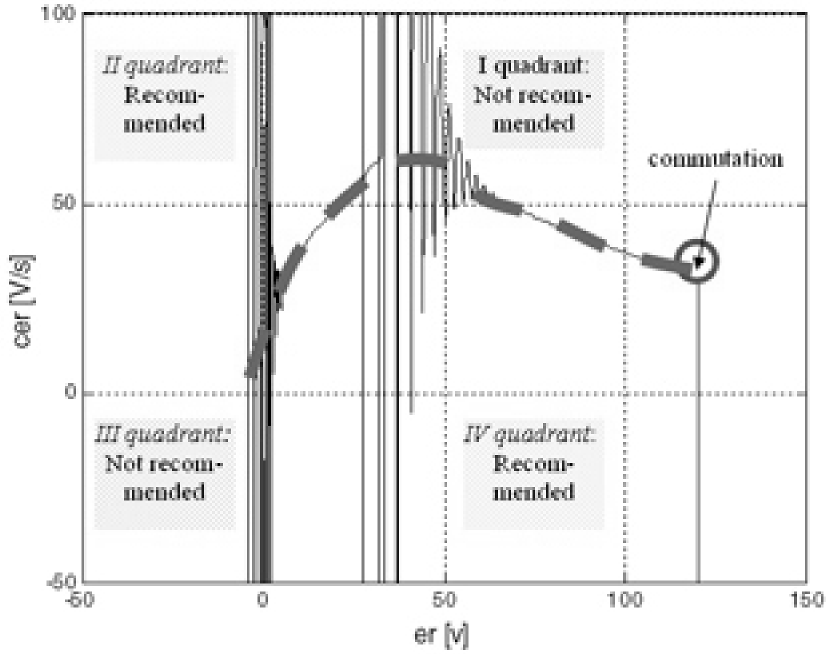


Fig. 5. The PTE and the not recommendable switching in the first quadrant

5. THE CONTROL OF THE SWITCHING

A further step after pointing the high risk zones would be to recommend the best possible commutation methods. The commutation methods can be *passive* or *active*.
a) **The passive commutation** is choosing the best possible commutation moments. In this matter we are proposing an analogy with the sliding mode method. Although the meanings of *er* and *cer* are totally different (in the case of the sliding mode *er* is a control error while in the case of the switching controllers *er* is the difference between the outputs of the switching controllers) the idea of imposing a switching law in the II and IV quadrants of the phase plane is offering good results in the case of the switching controllers. Instead of becoming a sliding contour the switching law has only the purpose to trigger the switching action.
It is to remark that if we are accepting a precise switching criterion and if we leave the unconnected controller in open loop, we will loose the possibility to control the precise moment of the switching, since there are no guarantees that the unconnected controller, that is very often saturated, will behave by itself such way that the phase trajectory can reach the sliding contour.
b) **The active commutation** is forcing the unconnected controller to track the output of the active controller. This way the commutation can be performed in any moment. If the unconnected controller's output is to slow, one can still find a satisfactory solution by imposing to it an initial value equal to the other controller's output in the moment of the commutation. In the case of very pretentious plants (nuclear reactors for instance) the tracking control law should be sliding mode. Adaptive tracking controllers able to control the commutations with no risks may be realized using the Takagi-Sugeno controllers [8] and also by the fuzzy-interpolative methodology, because the phase trajectory analyze is similar to the one that is

performed in FSAICs (Fuzzy Self-Adaptive Interpolative Controllers) [6] by the adaptive corrector.

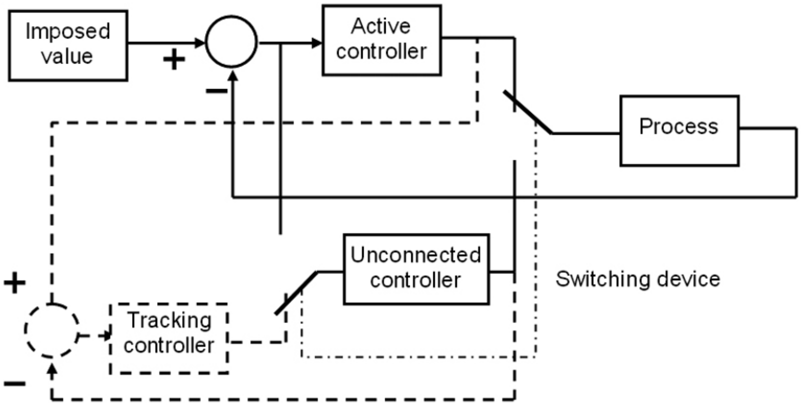


Fig. 6. The following controllers active commutation

6. CONCLUSIONS

The switching controllers' instability is caused by particular initial conditions and by the numeric calculus that is characterizing digital systems. The phenomenon is extremely dangerous and barely predictable. For this problem no rigorous theoretical apparatus is disposable for the moment, as far as we know. A common sense recommendation for decreasing the risk is to smooth as much as possible the commutations.

Among other existing methods for smoothing the commutations, a very feasible one is relying on the on-line analyze of the phase trajectory of the difference between the outputs of the switching controllers, which can be considered as a switching error. Such way one can choose the best moments for switching the controllers, in quadrants II and IV of the phase plane of the switching error, and one can avoid the risky quadrants I and III. A sliding mode law can be imposed to the unconnected controller's output in order to follow the output of the active controller.

REFERENCES

[1] D. Leith, R. Shorten, W. Leithead, O. Mason, P. Curran. Issues in the design of switched linear control systems: a benchmark study. *http://www.hamilton.ie/doug/ benchmark.pdf.*

[2] M.M. Balas, V.E. Balas, T.L. Dragomir. On the Switching Controllers' Issue and Smooth Controller Switching by Phase Trajectory Qualitative Analysis, *The 6th International Conf. on Recent Advances in Soft Computing (Abstracts + CD),* Canterbury, 10-12 July, 2006, pg. 63.

[3] M.M. Balas. Le flou interpolatif. *Conference soutenue a LSIS St. Jerome, Marseille*, 21 Sept. 2006. http://www.lsis.org/vie_du_labo/seminaire_81.html#102.

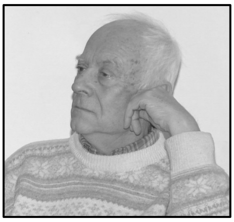
[4] E. Asarin, O. Bournez, T. Dang, O. Maler and A. Pnueli. Effective synthesis of switching controllers for linear systems. *Proc. of the IEEE,* vol. 88, no. 7, July, 2000, pp.1011-1025.

[5] L. Foulloy. Qualitative Control and Fuzzy Control: Towards a Writing Methodology, *AICOM* Vol. 6, Nrs. 3/4 Sept./Dec., pg. 147-154, 1993.

[6] M.M. Balas, V.E. Balas. The Family of Self Adaptive Interpolative Controllers, *Proc. of IPMU 2004*, Perugia, July, 2004, pp. 2119-2124.

[7] L. T. Kóczy, M. Balas, M. Ciugudean, V. E. Balas, J. Botzheim. On the Interpolative Side of the Fuzzy Sets, *Proc. of IEEE Sofa'05*, Szeged-Arad, Aug. 2005, pp. 17-23.

[8] Chih-Lyang Hwang, A Novel Takagi-Sugeno-Based Robust Adaptive Fuzzy Sliding-Mode Controller. *IEEE Transactions on Fuzzy Systems,* vol. 12, no. 5, October 2004, pp. 676-687.



Prof. Dr. Eng. Anton POLICEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania

Drd. Eng. Gheorghe MÜLEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania
E-mail: george.mulec@rdslink.ro

Ass. Prof. Dr. Eng. Eugen MÂRZA
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania
E-mail: eugen.marza@etc.upt.ro

ANALYZING SECURITY MECHANISMS IN WLAN

NOTE: This paper was presented at the International Symposium "Research and Education in an Innovation Era", Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

ABSTRACT

Because of their flexibility, affordability, and ease of installation, the WLAN have become increasingly popular and widely used. Besides these advantages, inherent broadcast nature of wireless networks has raised security concerned. In this study we analyzing WLAN security standards from point of view of implementation the major security requirements in communication systems and the features and weakness of them.

KEYWORDS:

communication, WLAN, security, standard, authentication.

INTRODUCTION

The market for wireless communications has experienced incredible growth over recent years. Wireless Local Area Networks (WLANs) have quickly found a significant place and popularity in business and the computer industry alike [1]. The major benefit of WLANs is increased flexibility and mobility [2].Security risks in wireless networks are equal to the sum of the risk of operating a wired network plus the new risks introduced due to the portability of wireless devices [3].

Starting from these security requirements, we have analyzed the security standards for Wireless Local Area Networks.

There are three security standards of WLAN:

- *WEP* (Wired Equivalent Privacy) - proposed by IEEE 802.11 Task Group.
- *WPA* – (Wi-Fi Protected Access) – proposed by Wi-Fi Alliance (The Wi-Fi alliance is an alliance of major 802.11 vendors formed with the aim of ensuring product interoperability).
- *IEEE 802.11i* – (which has also come to be known as WPA2) – proposed by IEEE 802.11i task group in June 2004.

CRYPTOGRAPHY ELEMENTS

For satisfy requirements of a secure communication network the cryptography comes in. The goal of cryptography is to design, implement, deploy, and make use of cryptographic systems that are secure in some meaningful way [4].

Authentication

There are three important requirements for achieve an authentication [5]. *Mutual authentication*, *Self protecting*, *Produces session key*. In WLAN are used three types of authentication methods.

A1. Open system authentication (**Fig. 1**) – This method permit any station (STA) which wants to join a network to send an authentication request to access point (AP).

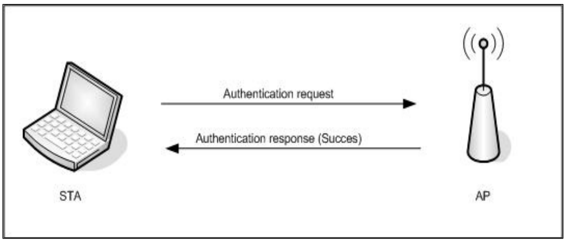


Fig. 1 – Open System Authentication

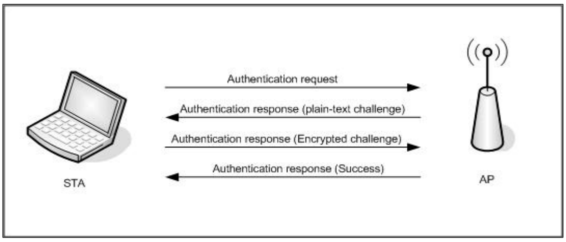

Authentication request
Authentication response (plain-text challenge)
Authentication response (Encrypted challenge)
Authentication response (Success)
STA
AP

Fig. 2 – Shared Key Authentication

A2. Shared key authentication (**Fig. 2**) – This method is based on the challenge-response system. Using this method it requires that the STA and the AP be capable of using WEP and both to have a preshared key. The method doesn't produce session key, because the session key is the same with preshared key which is achieve through manual configuration for each entities involved.

A3. 802.1x authentication – Is a different approach to authentication and authorization for IEEE 802.11 that is based on the 802.1X standard, which was originally published by the IEEE in 1999, and was revised in 2001 [6].

The 802.1X standard makes use of the *Extensible Authentication Protocol* (EAP) [7] as a way of communicating authentication information between the supplicant (STA) and the Authentication Server (AS), passing through the AP – **fig. 3**.

The 802.1x port model (**Fig. 4**) is a logical model consisting of a switch with multiple logical switches, where there is one logical switch per user. The strength of IEEE 802.1x authentication lies in other authentication mechanism that is implemented above it. (ex . EAP-TLS, EAP-TTLS, etc.). When the IEEE 802.1X authentication completes successfully, the STA and the AS will share a secret, called a MSK (Master Session Key).

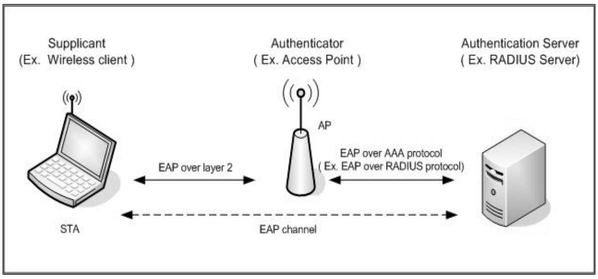


Fig. 3 – EAP protocol implementation

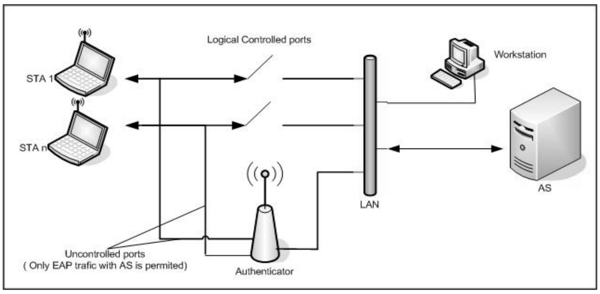


Fig. 4 – 802.1x model

Confidentiality

The confidentially is ensure by Symmetric Key Cryptography. Symmetric key Cryptography refers to the process in which the sender and the receiver use the same shared key to encrypt and decrypt messages.

Data Integrity

To ensure that a packet has not been modified in transit, WLAN uses an Integrity Check Value (ICV) field in the packet. ICV is known also as another name for Message Integrity Check (MIC). The idea behind the ICV is that the receiver should be able to detect data modifications or forgeries by calculating the ICV over the received data and comparing it with the ICV attached in the message.

SECURITY STANDARD IN WLAN

The 802.11 security architecture is compound by three security standard: WEP, WPA and 802.11i [8]. We will analyze all these standards and will accentuate on its features and weakness.

WEP – WIRED EQUIVALENT PRIVACY

It is the first security standard deployed in WLAN, when security was not very important.

Authentication with WEP

WEP support two types of authentication: Open authentication and Shared Key Authentication .Although in open authentication is no authentication at all, whoever wants to join to the network is permit. When the WEP encryption is enable, even through authentication is successful, the STA will be unable to transmit data through AP [9]. Neither has it decrypted data sent from AP.

Confidentiality with WEP

WEP uses RC4 (a stream cipher) in synchronous mode for encrypting data packets. The problem is that a stream cipher is not suitable for a wireless medium where packet loss is widespread.

Data integrity with WEP

To ensure that a packet has not been modified in transit, 802.11 use an Integrity Check Value (ICV) field in the packet. The ICV is compute with Cyclic Redundancy Check-32 bits (CRC-32) from data payload of an 802.11 packet.

The problem with the message integrity mechanism specified in 802.11 is not only that it uses a linear integrity check algorithm (CRC32) but also the fact that the ICV does not protect all the information that needs to be protected from modification.

WPA – Wi-Fi Protected Access

We consider that WPA is a bridge between WEP and 802.11i. To improve the security of 802.11 networks without requiring a hardware upgrade, the Wi-Fi alliance adopted Temporal Key Integrity Protocol (TKIP) as the security standard that needs to be deployed for Wi-Fi certification.

WPA is basically a prestandard subset of 802.11i which includes the key management and the authentication architecture (802.1X) specified in 802.11i [10].

Authentication with WPA

In a WPA environment are possible two types of authentication mechanism. The first is the same as a WEP and the second is based on the 802.1x framework.

WPA extends the two-tier key-hierarchy of WEP to a multi tier hierarchy. At the top level is still the MK, referred to as the Pair-wise Master Key (PMK) in WPA. WPA uses the PMK for deriving the Pair-wise Transient Keys (PTK) which are basically session keys. The term PTK is used to refer to a set of session keys which consists of four keys, each of which is 128 bits long.

These four keys are as follows: an encryption key for data, an integrity key for data, an encryption key for EAPoL messages and an integration key for EAPoL messages.

Confidentiality with WPA

TKIP doubles the IV size from 24 bits to 48 bits. This results in increasing the time to key collision. Actually, the IV is increased from 24 bits to 56 bits by requiring the insertion of 32 bits between the existing WEP IV and the start of the encrypted data in the WEP packet format.

Existing WEP hardware accelerators expect a 24-bit IV as an input to concatenate with a preshared key (40/104-bit) in order to generate the per-packet key (64/128-bit). This hardware cannot be upgraded to deal with a 48-bit IV and generate an 88/156-bit key. The approach, therefore, is to use per-packet key mixing, that has a key mixing function instead of simply concatenating the IV to the master key to generate per-packet key, increases the effective IV size while still being compatible with existing WEP hardware.

Data integrity with WPA

WEP used CRC-32 as an integrity check that is not a cryptographically secure integrity protocol. TKIP introduce a new ICV protocol—MICHAEL—which uses no multiplication operations and relies instead on shift and add operations. This protocol improves the CRC-32 integrity protocol. Another enhancement that TKIP makes in IV selection and use is to use the IV as a sequence counter.

IEEE 802.11i – Robust Security Network

WPA was a bridge to the final solution which was being designed by the IEEE 802.11i task group. This security proposal was referred to as the Robust Security Network (RSN) and also came to be known as the 802.11i security solution. The Wi-Fi alliance integrated this solution in their proposal and called it WPA2.

Authentication with 802.11i

WPA had also adopted the authentication architecture specified in 802.11i completely. Therefore, the authentication architecture in WPA and 802.11i is identical.

Confidentiality with 802.11i

To provide confidentiality in 802.11i, AES is used in the counter mode. Counter mode actually uses a block cipher as a stream cipher, thus combining the security of a block cipher with the ease of use of a stream cipher.

The AES cipher is then used to encrypt the counter to produce a key stream. When the original message arrives, it is broken up into 128-bit blocks and each block is XOR-ed with the corresponding 128 bits of the generated key stream to produce the cipher-text.

The main features of AES in counter mode are: Block cipher operated as a stream cipher; Key stream can be generated before the message arrives; The various blocks of the message can be encrypted in parallel; The length of the encrypted text can be exactly the same as the length of the plain text message.

Data integrity with 802.11i

To achieve message integrity, IEEE 802.11i Task Group extended the counter mode to include a Cipher Block Chaining (CBC)-MAC Operation (CCMP). CBC-MAC XORred a plain-text block with the previous cipher block before encrypting it. This ensures that any change made to any cipher-text block changes the decrypted output of the last block and hence changes the residue. CBC-MAC is an established technique for message integrity.

CONCLUSION

WEP encapsulation is flawed at many levels and WPA is designed to patch the vulnerabilities while reusing existing hardware. WPA provides an acceptable level of security in legacy WLAN devices. WPA only requires firmware or device driver updates and is fairly easy to implement and deploy.
For using IEEE 802.11i (WPA2) is required a new hardware device with new computational capabilities. The main features of 802.11i towards WPA are that replace stream cipher (RC4) with a strong block cipher (AES) and provide a stronger integrity protection AES-based CCMP.

REFERENCES

[1] Gast M. (2002).Chapter 6: Security, Take 2: 802.1 X, 802.11 Wireless Networks: The Definitive Guide. O'Reilly. ISBN 0-596-00183-5, April.

[2] Kapp S. (2002). 802.11: leaving the wire behind. Internet Computing, IEEE. Volume 6 Issue, pages 82-85 , February.

[3] Karygiannis T& L. Owens. (2002). Draft : Wireless Network Security – 802.11, Bluetooth and Handheld Devices. USA, National Institute of Standards and Technology.

[4] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 644–654, Nov. 1976.

[5] Rescorla, E., "A Survey of Authentication Mechanisms", Internet Architecture Board (IAB), work in progress, draft-iab-auth-mech-02.txt, October 2003.

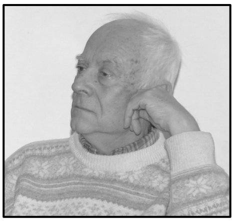
[6] IEEE Std 802.1x-2001: Port Based Network Access Control, http://www.ieee802.org/1/pages/802.1x.html, June 2001

[7] 10. B. Aboba, "Extensible Authentication Protocol (EAP)." RFC 3748 (Standards Track), June 2004.

[8] "IEEE 802 Standards", http://standards.ieee.org/getieee802

[9] Gast M. (2002), Wired Equivalent Privacy (WEP), 802.11 Wireless Networks: The Definitive Guide. O'Reilly.

[10] C. He and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," Proceedings of Network and Distributed System Security Symposium (NDSS), (San Diego, CA), Feb. 2005.



Prof. Dr. Eng. Anton POLICEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania

Drd. Eng. Gheorghe MÜLEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania
E-mail: george.mulec@rdslink.ro

SECURITY COST OF IEEE 802.11 WIRELESS LAN

NOTE: This paper was presented at the International Symposium "Research and Education in an Innovation Era", Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

ABSTRACT

Wireless network have gained popularity due to the flexibility and mobility that allow users access to the information. This research evaluated the effect of multiple security mechanisms of the performance for IEEE 802.11g wireless network using server-client architecture. The results showed that security mechanisms degrade the performance of network and we must know how much we pay for security features.

KEYWORDS

security mechanism, wireless network, topology.

I. INTRODUCTION

Since the ratification of the IEEE 802.11b standard in 1999, wireless LANs have became rifer. This is due the mobility of users by releasing the constraint of physical connections. Today, wireless LANs are widely deployed in places such as corporate office, conference rooms, airports, university campus.

Besides these advantages, inherent broadcast nature of wireless networks, the IEEE 802.11 – based wireless LANs present new challenges for information security administrators [1].

Network performance is characterized by certain parameters such as a time delay, system throughput, packet loss etc.

Wireless networks are highly susceptible to many kinds of attacks since interception and eavesdropping of data in transit is possible for anyone with access to wireless network due to their inherent broadcast nature and shared air medium [2],[3]. For maintaining a specific level of network performance it is vital to determine the performance impact caused by security services in wireless network. At the most basic level wireless security requires authentication and encryption. Wireless network use more levels of security for data protecting [4].

II. BACKGROUNDS

In the first stages of 802.11 development, the WLAN security was based on two mechanism: Service Set Identifier (SSID) and Wireless Equivalent Privacy (WEP). When the weaknesses of WEP were identified, IEEE ratified a new standard, IEEE 802.1X, that provides a way to leverage traditional strong authentication mechanisms such as RADIUS Server in a wireless network [5]. The IEEE 802.1x defines a mechanism for port-based network access control. It is based upon Extensible Authentication Protocol (EAP) to provide compatible authentication and authorization mechanisms for devices interconnected by IEEE 802.11.

There are three main components in the IEEE 802.1x authentication system: supplicant, authenticator and authentication server. In a WLAN, *supplicant* usually is AP (Acces Point) that represents an *authenticator*. Authentication, Authorization, and Accounting (AAA) server such as RADIUS server is the *authentication server*. The *port* in 802.1x represents the association between supplicant and authenticator. Both supplicant and authenticator have a *Port Access Entity (PAE)* that operates the algorithms and protocols associated with the authentication mechanisms. The authenticator's *controlled port* is in unauthorized state. Messages will be directed only to the *Authenticator PAE*, which will further direct 802.1x messages to the authentication server.

The authenticator PAE will close the controlled port after the supplicant is authenticated successfully. IEEE 802.1X specifies how to run the EAP directly over a link layer protocol. EAP is a transport protocol that can used a variety of different authentication types known as EAP methods [6],[7],[8].

In **figure 1** is illustrate the 802.1X–EAP Message Flow for an authentication process. Among the EAP methods developed specifically for wireless networks are a family of methods base on public key certificates and the Transport Layer Security (TLS) protocols. These are EAP-TLS, EAP-TTLS and EAP-PEAP.

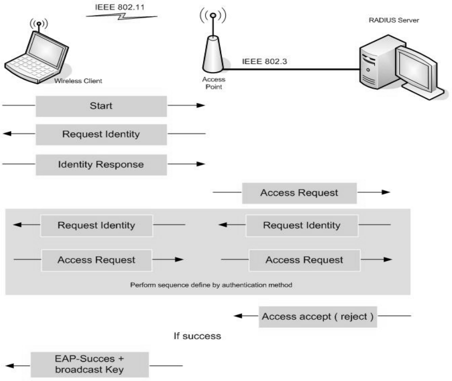


Fig. 1 - 802.1X – EAP Message Flow

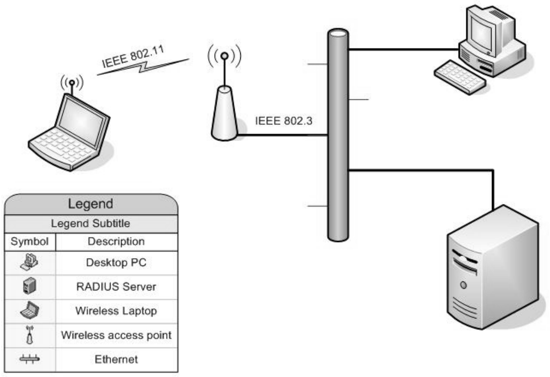


Fig. 2. Testbed architecture

III. EXPERIMENTAL PART

A. Configuration topology

Our test platform is a miniature of WLAN compound by an access point, an authentication RADIUS server, a local area network, a wireless laptop and a PC station. **Figure 2** shows the testbed architecture used on this experiment.

B. Hardware configuration

Access point (AP) used in experiment is a D-link DWL 2100AP [10]. At this access point, are wireless connected a wireless client with Laptop HP (Celeron 1.5 GHz, 256 MB RAM) and a D-link DWL G650 wireless cardbus adapter [10]. For RADIUS Server we used a desktop PC (P IV, 2.6 GHz, 512 MB RAM) and for PC station another desktop PC (AMD 1,3 GHz, 256 MB RAM). All the Ethernet adapter are fast adapter (100 Mbps).

C. Software configuration

All the system have installed Windows XP Home Edition as a operating system. We have installed following software components for various protocol used in testbed: RADIUS server is implemented with open-source software FreeRADIUS [11], X.509 Certificate (CA, Server, Client) are issued with open-source software OpenSSL [12], Capturing packets are made with Ethereal packet analyzer. [13], TCP / UDP tuning and throughput measurement are made with Iperf [14] and Qcheck [15]

D. Experimental analysis

Many factors affect network performance and some of them interact to provide overall performance results. Performance results depending on the choice of hardware device, software application, security policy and network topology. On the same conditions (hardware, software and network topology) we have measured the authentication time, throughput and response time for different types of security policy.

Authentication time is defined as the time involved in a authentication phase of security protocol.

Throughput refers to actual measured bandwidth, at a specific time of day, using specific routes, and while a specific set of data is transmitted on the network.

Response time is a measure of the delay in transmission of data between a sender and a receiver for a specific packet size.

For this experimental analyze we have used the “Iperf”, “Qcheck” and “Ethereal” software programs.

1. Security configuration

IEEE 802.11 provides two mechanism of security: authentication and encryption. Authentication may be made with Shared key authentication mechanism and with different type of authentication mechanism run over the EAP protocol.

In our research we used the EAP based on 802.1x family protocol for authentication (EAP – TLS, EAP – TTLS, EAP –

PEAP).For data encryption we used WEP (40 and 128 bits), TKIP and AES encryption protocol.

2. Measurement methods

For each security service configured, experimental data were collected in two phases, in a not congested network (normal situation). The first phase collects measurements from authentication protocols. The second phase focuses on generating different traffic and measurement the throughput and response time.

In the first phase, we used “Ethereal” packet analyzer to capture the packets exchanged during authentication process. Data obtained here were used to compare the authentication time for different authentication protocols.

On the second phase we used “Iperf” and “Qcheck “ for generate TCP and UDP traffic between Wireless Laptop and PC station for measures the throughput and response time .For all tests, the wireless link was at a constantly 54 Mbps with level of radio signal more than 95%.

IV. RESULTS AND DISCUSSION

1. Authentication Time

Figure 3 show authentication time (in sec) for EAP – TLS, EAP–TTLS, EAP–PEAP authentication protocols.

Our research is based only to the 802.1x authentication framework. The shared key authentication not achieves the mutual authentication and when the authentication is completed does not result a session key.

Authentication time for all the Certificates based protocol mention above is mostly the same. We can see that authentication process is smaller than 1 sec and appear after association phase.

2. Throughput

Figure 4 illustrates the throughput of TCP traffic for different encryption protocol. Performance measures were gathered by running seven repetitive tests at each encryption protocol. The throughput is smaller if we use the AES instead of TKIP (RC4) cipher. If we use the same protocol the throughputs decrease if increasing the secret key length.

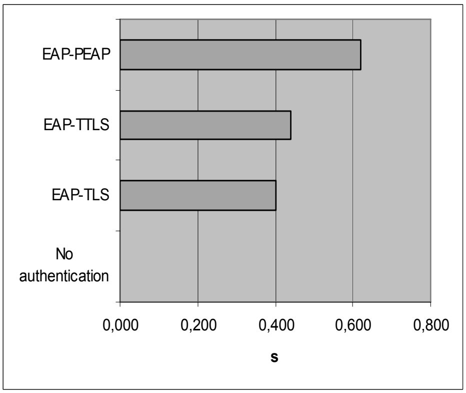


Fig. 3 Authentication time

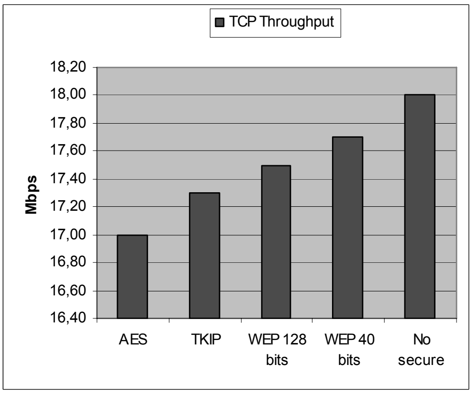


Fig. 4 Throughput for TCP

Figure 5 illustrates the throughput of UDP traffic for different encryption protocol. In this case, the "trend" is the same as in TCP traffic, but throughput is with cca. 20% lesser.

3. Response time

Figure 6 illustrate the response time for TCP and UDP traffic. In this case, we measure the response time for 1K byte packet size (in a not congested network).

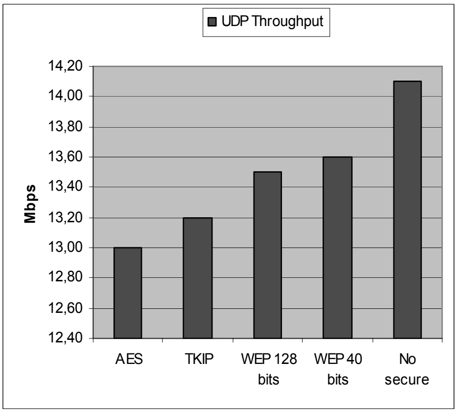


Fig. 5 Throughput for UDP

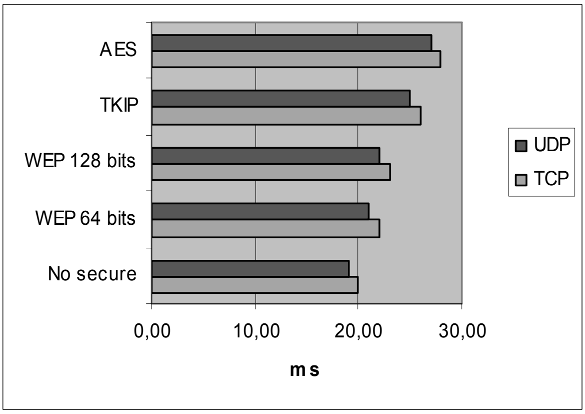


Fig. 6 Per packet response time

V. CONCLUSION

In this paper, we presented experimental results of impact incurred by security policies on system performance in a not congested network.

The results demonstrate that WEP policies cause least overhead, while AES and TKIP cause significant overhead but provide stronger security. Authentication process 802.1x with EAP-TLS cause lesser overhead than 802.1x with EAP-PEAP. The delay produce by the authentication process is smaller than 1 sec. Because the WLAN isn't very mobile (WLAN is implemented in relative limited area – college campuses, airports, shops) the need for authentication is not very frequent and the benefits of that is evident. The authentication delay is bigger for EAP-PEAP towards other authentication Certificate based protocols.

Using AES as encryption protocol we have obtained a smaller throughput and obviously the possibility of delivery less amount of data in a given time than in case of using TKIP or WEP , but this is the 'price' for having a higher security.

REFERENCES

[1] Y. Zahur and T.A. Yang, "Wireless LAN security and Laboratory design", Journal of Computing Science in Colleges, vol. 19, pp. 44-60, January 2004

[2] W. A. Arbaugh, N. Shankar, J. Wang and K. Zhang, "Your 802.11 network has no clothes", IEEE Wireless Communication Magazine, December 2002

[3] D.B. Faria and D.R.Cheriton, "DoS and authentication in Wireless Public Access Networks," pp. 47-56, September 2002.

[4] E Bertino, S. Jajodia , L. Mancini and I. Ray,"Advanced transaction processing in Multilevel secure File Stores", IEEE Transactions on Knowledge and Data Engineering, vol. 10 , pp. 120-135, February 1998

[5] "IEEE Std 802.1x-2001x: Port Based Network Access Control", http://www.ieee802.org/1/pages/802.1x.html, June 2001

[6] Blunk, L., & J. Vollbrecht. (1998). PPP Extensible Authentication Protocol (EAP), RFC2284: Internet Engineering Task Force.

[7] "IEEE 802 Standards", http://standards.ieee.org/getieee802

[8] IETF, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999

[9] Microsoft Wireless 802.11 Security Windows XP, http://www.microsoft.com

[10] http://www.d-link.com

[11] http://www.freeradius.org

[12] http://www.openssl.com

[13] http://www.ethereal.com

[14] http://www.iperf.org

[15] http://www.ixiacom.com

Sorin NANU
lecturer professor
“Politehnica” University of Timisoara
Faculty of Automation and Computers
Department of Automation and Applied Informatics
B-dul Vasile Pârvan Nr. 2, 300223 Timişoara, Romania
E-mail sorin.nanu@aut.upt.ro

EDUCATIONAL ASPECTS IN CONTROL SYSTEM DESIGN TECHNOLOGY

NOTE: This paper was presented at the International Symposium “Research and Education in an Innovation Era”, Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

ABSTRACT

Didactical technology in the field of automation implies not only the transfer of knowledges to the students, but also to create them the abilities to understand, describe, search, innovate, generate a solution for a technical problem. This paper presents a didactic activity according to the elements exposed, with a very intense impact to the students. Examples are considered only in the field of automation because this involves some particular features. Four examples are detailed. The conclusions were spectacular due to the massive involving of students in this activity.

KEYWORDS:

education, control systems, learning

INTRODUCTION

Engineering is a profession. Its members work closely with scientists and apply new and old scientific effects to produce products and services that people want. Engineers are professionally responsible for the safety and performance of their designs. The objective is to solve a technical problem with the simplest, safest, most efficient design possible, at the lowest cost [WAN01]. Design is a very important engineering activity. It involves meeting some need by applying the laws of physics and chemistry, using mathematics, and the computer [SHA01]. The purpose of this paper is to describe the educational aspects of four design projects in automation, according to the statements above, that were proposed for the first time to students in the fifth year.

During the design activity, the students will cover a wide area in the field of automation (electronics, measurement, microcontrollers-hardware and software, high technology boards, system theory), they are shown the steps of the project management, how to receive abilities, how to communicate and to innovate. The projects are rather small, hardware-ready and not very difficult, so the students can easily fulfill their tasks and see rapidly the results.

EXPERIMENTAL PART

The experimental part consists of four closed loop control systems. The structure and objectives for every application will be presented consequently.

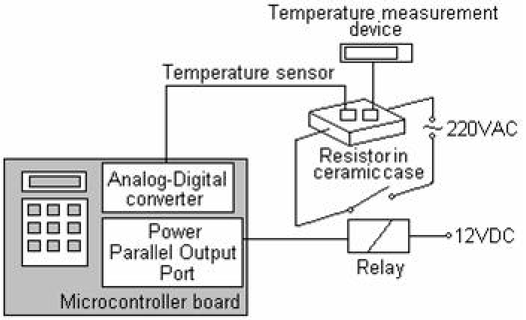
1. Temperature control system. In **Fig. 1** is depicted the block diagram and in **Fig. 2** the picture of this system. The process is represented by a 10k resistor encased in ceramic. It runs a current from a 220 VAC supply through a contact of a Relay driven by an open collector transistor from microcontroller board (Power parallel port). The temperature of the ceramic surface is read both by a LM335 temperature sensor that converts it in voltage conducted to the digital-analog converter on microcontroller board [***89] and an industrial temperature measurement device used only for monitoring purposes, with no duty in control.

The task for this application is to design a control system (the software) to control the temperature within the interval **[θ_ω-ε, θ_ω+ε]**, together with displaying both of actual and reference temperature and possibility to adjust from the keyboard of microcontroller board the prescribed temperature.

The objectives for the student are:

- to understand the electronic schematics (introducing the use of temperature sensor, relay actuation, open collector parallel output),
- to manage the signal conversion from temperature to voltage,
- to apply the knowledges of bi-positional controller (emphasizing the hysteresys) in solving the task,
- to ellaborate the structure of program for this task (is time critical?, which are the priorities between resources exploiting?),
- to practice the C programming in working with different resources (analog – digital converter, power parallel port, keyboard, display).

Fig.1



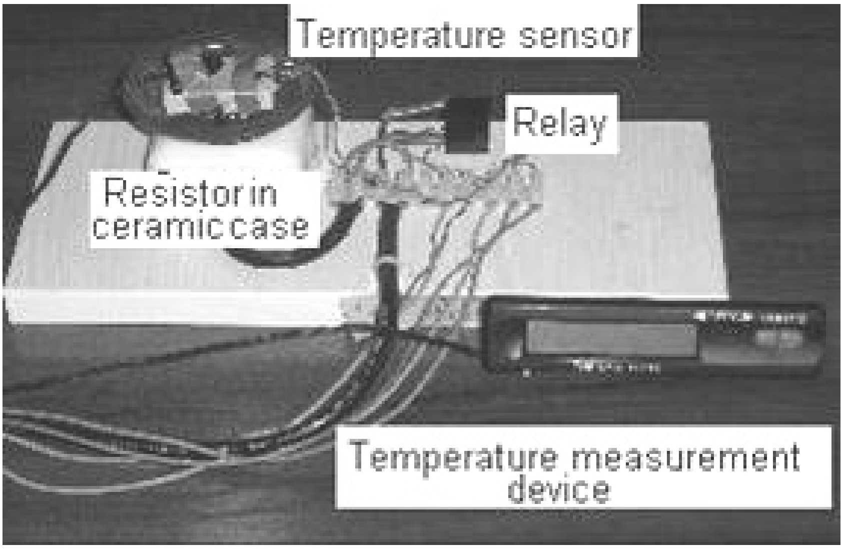


Fig.2

As this application is the easyest, the students managed very rapidly the bi-positional controller and this part was finished very quickly. Problems were encountered with signal conversion, working with display and especially with keyboard.

2. Position control system. In **Fig. 3** is represented the block diagram and in **Fig. 4** the picture of this system. The process is represented by DC motor that carries a slider along of a steel wire over two turning wheels. The cursor represents also a wiper of a long potentiometer used as a position sensor. The voltage collected by the wiper is provided to the Analog-Digital converter of the microcontroller board. The motor is actuated by a driver (BA6219 of ROHM) that has as inputs one analogic voltage in range [0, 5] V that controls the speed, and two digital signals that controls the direction of rotation. So microcontroller board receives the information about actual position and consequently provides three signals to control the motor according to a control law.

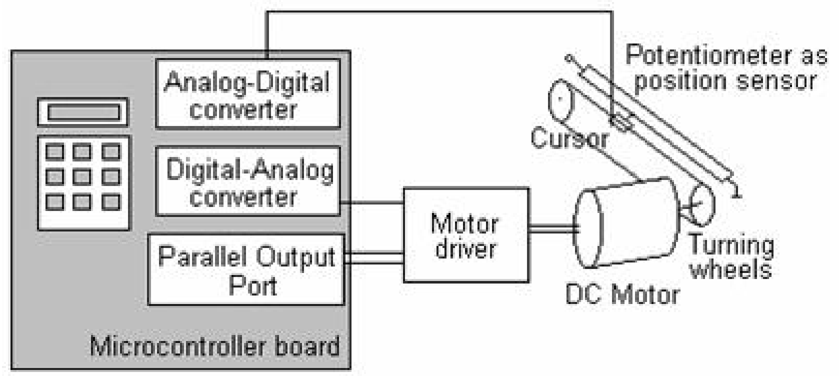


Fig. 3

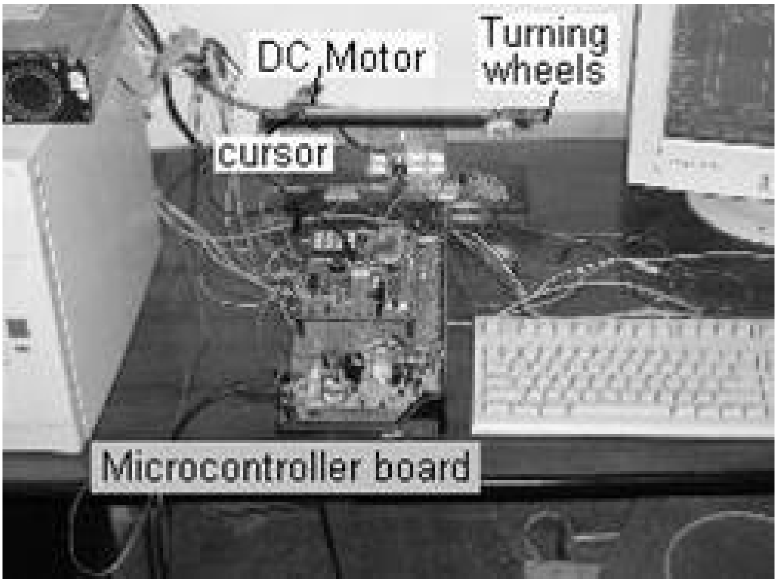


Fig.4

The task for this application is to design a control system (the software) to control the position of cursor along all path, together with adjusting from the keyboard of microcontroller board the reference position.

The objectives for the student are:

- to understand the electronic schematics (introducing the use of position sensor, motor driver, parallel output, digital-analog converter),
- to manage the signal conversion from position to voltage,
- to apply the knowledge of implementing a controller in solving the task (students were directed to implement a n-positional and a proportional controller),
- to elaborate the structure of program for this task (is time critical?, which are the priorities between resources ?),
- to practice the C programming in working with different resources (analog-digital converter, digital-analog converter, parallel port, keyboard, display).

In this application, students managed quite rapidly both the n-positional and the proportional controller. Also the working with display and keyboard run pretty fast. A particular feature was noticed regarding the proportional controller. They could appreciate quantitatively and qualitatively by watching on scope, the effect of the controller constant on the quality of control. It was a very good example for understanding the controllers.

3. Orientation after the light. This system consists of a rotating frame actuated by a 4 phases, unipolar stepper motor (see electric schematics in **Fig. 5**, functionality in **Fig. 6** and a picture in **Fig. 7**). Three light sensors oriented in proper positions (as in fig.6) sense the intensity of light.

As the light is making different angles with the sensors, the voltage issued by sensors differ consequently. A reference position (called 'closed') of the rotating frame is defined by a Hall sensor and a magnet. 4 Darlington transistors drive the motor.

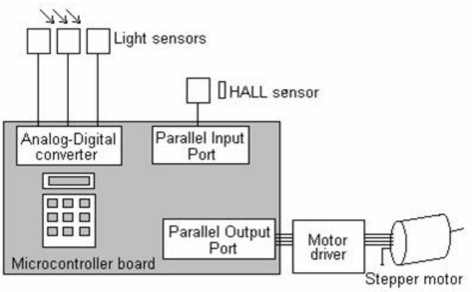


Fig. 5

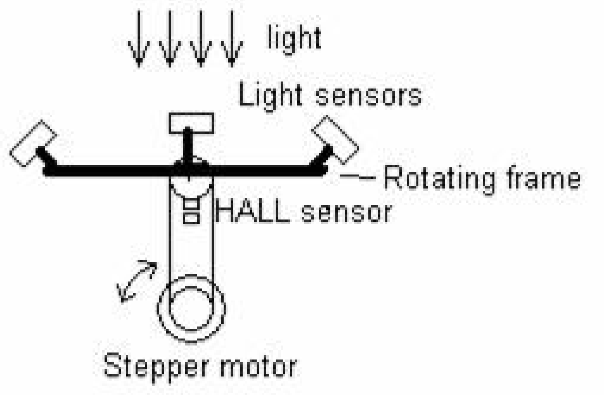


Fig. 6

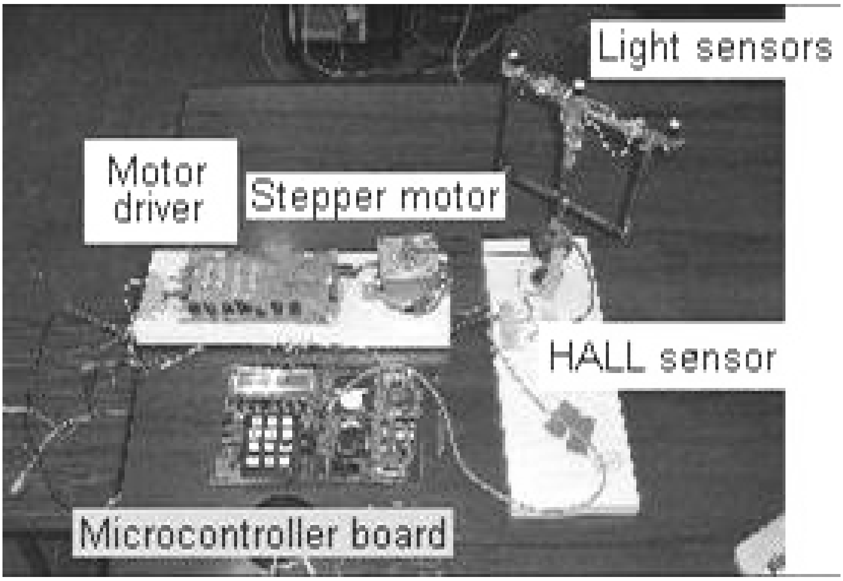


Fig. 7

The task for this application is to control the position of rotating frame in such a manner so it always stays perpendiculary on light beam. If there is no light, or the intensity stays below a certain limit, the frame has to go to the 'closed' position.

The objectives for the students are:

- to understand the electronic schematics (introducing the use of light sensor, Hall sensor, stepper motor, Darlington transistors as motor driver),
- to manage the signals coming from 4 sensors,
- to elaborate the structure of program for this task (how does the block diagram look like?),
- to practice the C programming in working with different resources (analog-digital converter, input and output parallel port).

This application is more complex than the previous, students made some experiments to understand the functioning of all sensors and stepper motor. There were some versions of structure of programme.

4. Motor speed control. This system consists of a DC motor driven by a L165 of Linear Technology amplifier, mechanically connected to a tachogenerator as transducer. To determine the absolute speed of the motor on the shaft is mounted a magnet, sensed by a Hall sensor from the base plate (see **Fig. 8** and **Fig. 9**).

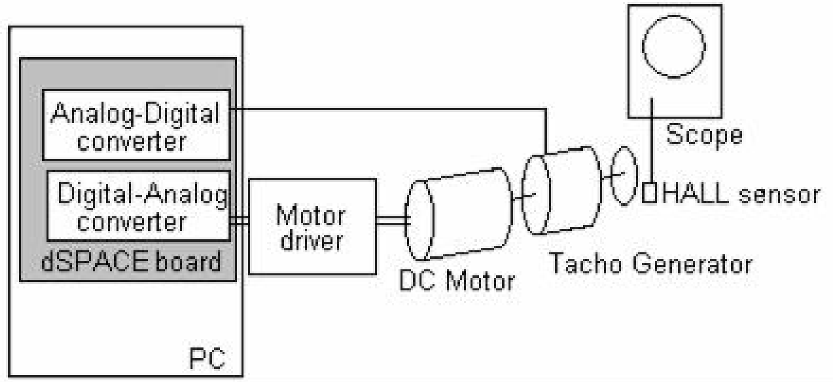


Fig. 8

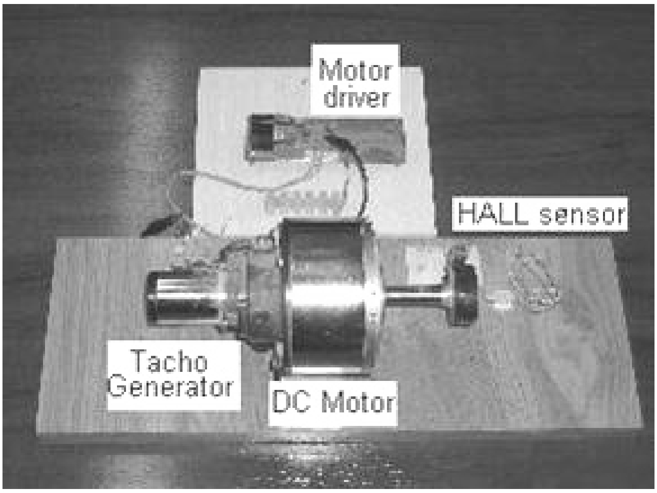


Fig. 9

The task for this application is to model the process and speed transducer and to design a control system using a dSPACE board, to control the motor speed. For modelling they had to determine the static characteristic of motor and tachogenerator and to proximate the dynamic constants. The objectives for the student are

- to be able to make an experiment to determine static characteristic of process and transducer, and to process the results,
- to design a controller,
- to understand and to implement a controller on a dSPACE board [***99],

Problems were encountered on managing the experiment for modelling. The implementation on dSPACE board was very simple, and students experienced a high technology board for rapid prototyping.

RESULTS AND DISCUSSION

During the design activity, many of the “learning principles” of [SHA01] were respected. The conclusions drawn from this intense design learning activity were spectacular.

1. Much more students (80% were extremely active) than in usual laboratory activities were deeply involved in design, after first two meetings they “fought” to be directly involved. A motivation for this could be the challenging aspect of the activity,
2. It was obvious that degree of understanding was very high, and it was seen in the questions asked after the closing of one project,
3. the degree of interest was very high,
4. one reason for efficiency was the fact that, because the students had the hard-ready projects, they had only to develop the algorithm and software, and the results were seen very fast.

Some of the students asked some things about the hardware design showing interest on it. So, can be stated that this can be the first step in a wider educational program in engineering.

CONCLUSION

This type of learning, with small, part ready design projects is very efficient. The degree of involving and understanding for students is very high, and it can prepare further more advanced items in control systems education.

REFERENCES

[SHA01] Shaw M. C. Engineering problem solving: A classical perspective Arizona State University, Noyes Publications, William Andrew Publishing, New York, 2001,

[SCH99] Schultz, T.W., C and the 8051, vol. II Building efficient applications, Prentice Hall, New Jersey, 1999,

[WAN01] Wankat P. C. Oreovicz F. S. Teaching Engineering, Purdue University, 2001,

[***89] *** 80C552 Microcontroller User Manual, Philips, 1989,

[***99] *** DS1102 Board, Real Time Workshop, User manual, dSPACE Company, Paderborn, 1999.

Sorin NANU
lecturer professor
“Politehnica” University of Timisoara
Faculty of Automation and Computers
Department of Automation and Applied Informatics
B-dul Vasile Pârvan Nr. 2, 300223 Timişoara, Romania
E-mail sorin.nanu@aut.upt.ro

IMPLEMENTING OF A CONTROL SYSTEM FOR PNEUMATIC PROCESS

NOTE: This paper was presented at the International Symposium “Research and Education in an Innovation Era”, Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

ABSTRACT

Within the research and didactical activity implementing of a control system represent a first step. Rather difficult to fulfil when every component, both pneumatic process and digital controller is new. The effort of implementation is done for connecting the elements of the process, measurement, interfaces with digital controller, software. The result is a system that can be developed according to theory, increased in complexity, with minimal changes in structure.

KEYWORDS:

pneumatic elements, control systems, learning, LabView

INTRODUCTION

Pneumatic elements are wide spread in low power positioning systems. They are very advantageous because of flexibility, but not very performing regarding the precision. The control of these systems was improved in last years by introducing of proportional valves instead of on-off valves. This paper describes the steps of building a rather complex control system for 2 degrees of freedom pneumatic system plus a suction valve. The process is provided by FESTO Company, being a part of a full control system. Weren't used the FESTO controller and interfaces, but replaced with an acquisition board from National Instruments and consequently electronics. Unfortunately, the feedback from a pneumatic element was in CAN bus format and was not processed by the built control system. The software used was LabView 7 and MAX 2.0 from National Instruments.

EXPERIMENTAL PART

The experimental part consists of a control system with one closed loop and two open loops. The block diagram is presented in fig.1.

- process PC, detailed in fig.2, is formed of one linear pneumatic piston (1), with a sliding cursor (2), a rotating pneumatic motor (5) on whose shaft (6) is mounted an arm (4) with suction valve (3),
- y1, y2 and y3 represents position of linear piston, angular position of motor respectively the air volume absorbed by vacuum generator,
- actuators EE1 and EE2 are two identical proportional pneumatic valves, while EE3 is a vacuum generator,

- measurement element EM is a potentiometer that measures the angular position of rotating motor (for linear piston the feedback is in CAN bus format and couldn't be processed in actual version),
- controller RG consists of a computer and NI acquisition board together with the LabView and MAX software.

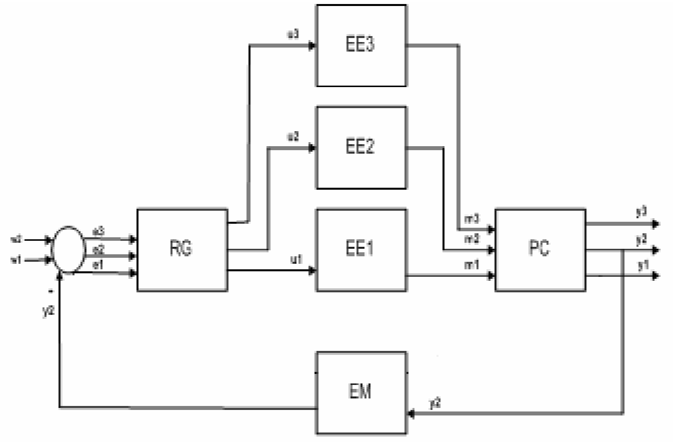


Fig.1

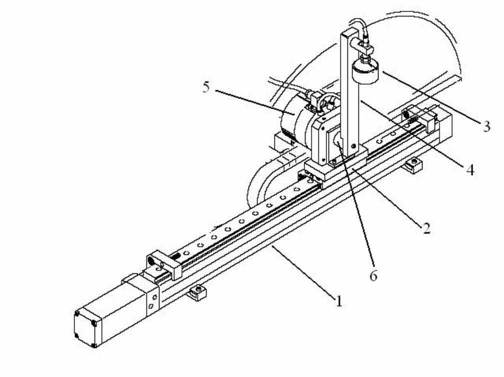


Fig.2

The whole pneumatic process is powered by a 3HP compressor that can issue 8 to 10 bars. The pressure of compressed air is regulated by a regulator that has the main task to maintain the pressure in circuit constant at 4 bars, but also the task to filter the air from impurities and humidity.

Vacuum generator. The task of this device is to generate vacuum when supplied with 4 bars air. The command signal is logic 0V for OFF and 24V for ON. Its efficiency is 85%, consumed power is 2.5W at an input impedance of 240 Ohms. It is connected through a pipe to the suction valve mounted on the arm of rotating motor.

Linear piston. (Fig.3) It consists of a metalic case (2), the piston with a mounting plate (1), the pneumatic circuit that has two inputs (3) and the measurement system with the corresponding electronics. The movement of the piston is realized by the differential pressure supplied at input 3, by the proportional valve. The ampltude of difference detremines the speed, while the sign of difference determines the direction. On the mounting plate of the piston is fixed the rotating motor.

Rotating motor. The principle is identical to that of the linear piston, but the displacement is angular. The air flow through two pipes from proportional valve determine the movement of the motor shaft.

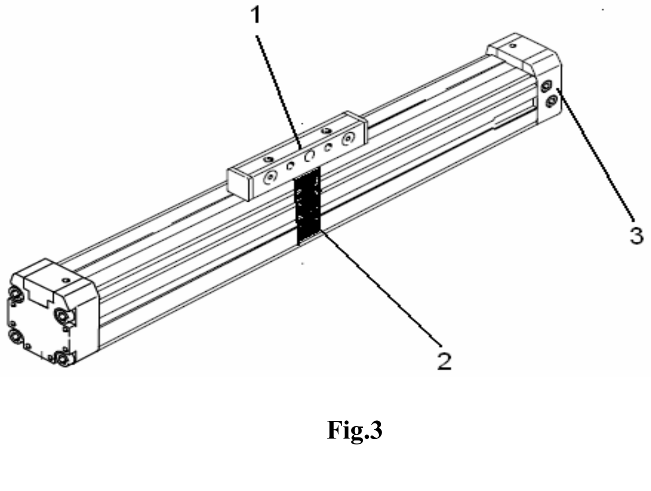


Fig.3

Proportional valves. These devices have the task to generate differential pressure to actuate the linear piston and rotating motor. The structure is presented in fig.4, where 1 is the electric converter that transforms the input voltage into the displacement of the shaft 2. The consequence is that the input air flow in 3 is distributed towards outputs 4 or 5, the excess being evacuated in atmosphere through 6 or 7. They are controlled in voltage as in fig.5. When in equilibrum status, at 5 V, the air flow on both output is null. When voltage is different from 5 V the air flow is guided towards one or another output from 0% to 100%.

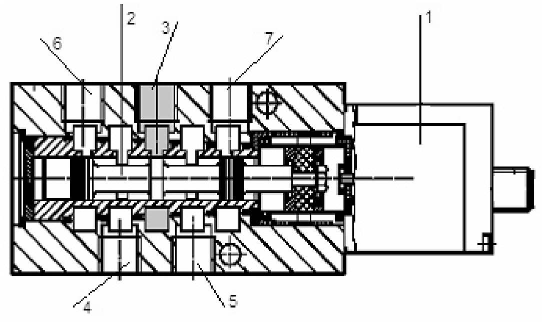


Fig. 4

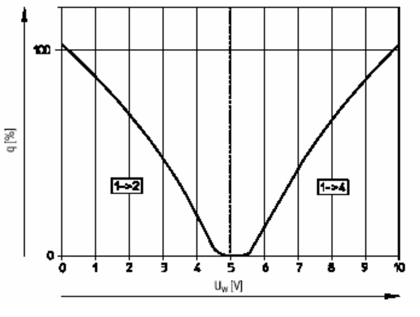


Fig. 5

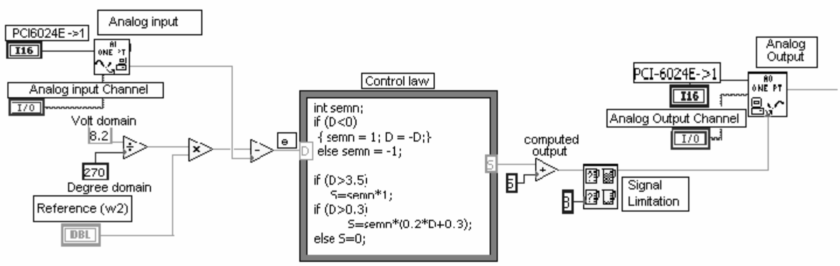
Controller. It is performed by a personal computer with NI PCI-6024E data acquisition board. The software used for development is LabView 6.0 and MAX 2.0 of National Instruments.

Control System implementation. From the hardware point of view there are 4 connection between controller and actuators and measurement elements.

- 1 analog signal from position sensor of rotating motor (voltage in range 0V- 8.2V) towards Analog Input of PCI 6024E board,
- 2 analog signals to proportional valves (voltage in range 0V-10V) from Analog Output of PCI 6024E board,
- 1 logical signal to vacuum generator (voltage with TTL levels) from Digital Output of PCI 6024E board, through a 24V relay.

From the software point of view there are three modules that deals with the three pneumatic actuators:

- *rotating motor control module* (fig. 6), has the following functions:
  - analog signal acquisition from position sensor on Analog Input,
  - generation of reference (w2),
  - computing the comand using control law (in this case was a simple proportional controller),
  - limitation and generation of the analog signal towards valve through Analog Output.

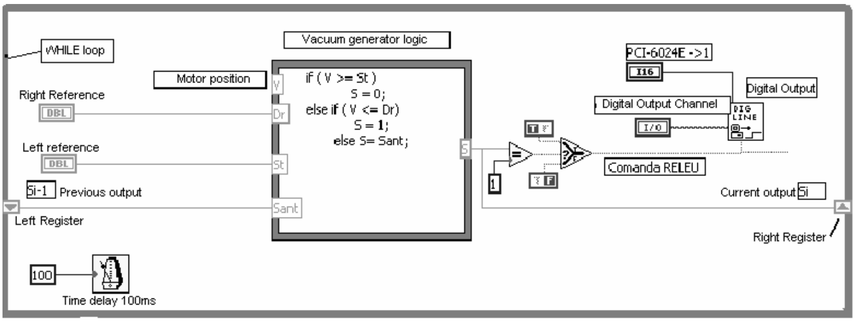


```
int semn;
if (D<0)
 { semn = 1; D = -D;}
 else semn = -1;

if (D>3.5)
   S=semn*1;
if (D>0.3)
      S=semn*(0.2*D+0.3);
else S=0;
```

Fig.6

- *vacuum generator module* (fig. 7), has the following functions:



```
if ( V >= St )
      S = 0;
else if ( V <= Dr)
      S = 1;
   else S= Sant;
```

Fig.7

- reading the position of motor, aquired by previous module,
- comparing with two limits (left and right),
- generating a proper logic signal if the position is on a certain relation with these limits

- *linear piston module*, has the following functions:
  - reading of comand signal from a user interface,
  - generating an analog signal towards proportional valve through Analog Output (open loop control).

The time diagram in fig.8 shows all the signals involved in this control system:

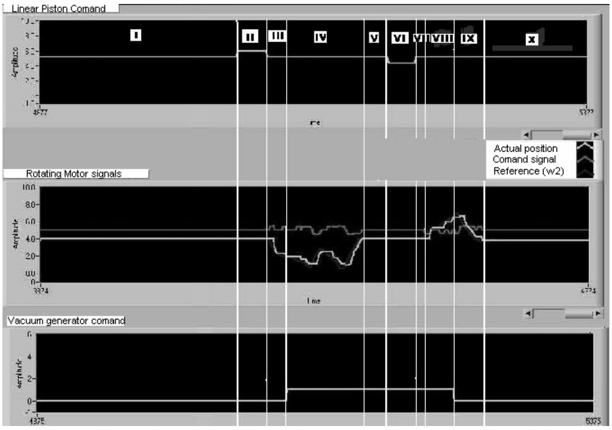


Fig.8

- diagram 1 – comand signal for linear piston

- diagram 2 – motor blue (reference signal w2), green (actual position),red (comand signal),
- diagram 3 – comand signal for vacuum generator.

Zone I- initial state, Zone II- movement of linear piston towards a desired position (manual comand), Zone III- start of rotating, Zone IV- when reaching a certain position, start of vacuum, continuing rotation (getting an object), reverse rotation (lifting the object), Zone V- stop movement (pause), Zone VI- start linear movement backwards, Zone VII- stop movement (pause), Zone VIII- start rotating (lowering object), Zone IX- when reaching a certain position, stop vacuum (release object), reverse rotating, Zone X- stop.

For this application there is a user interface that allows to set the variables, and to visualize the signals. In fig.9 is presented the whole system (on the monitor screen can be seen the signals from process).

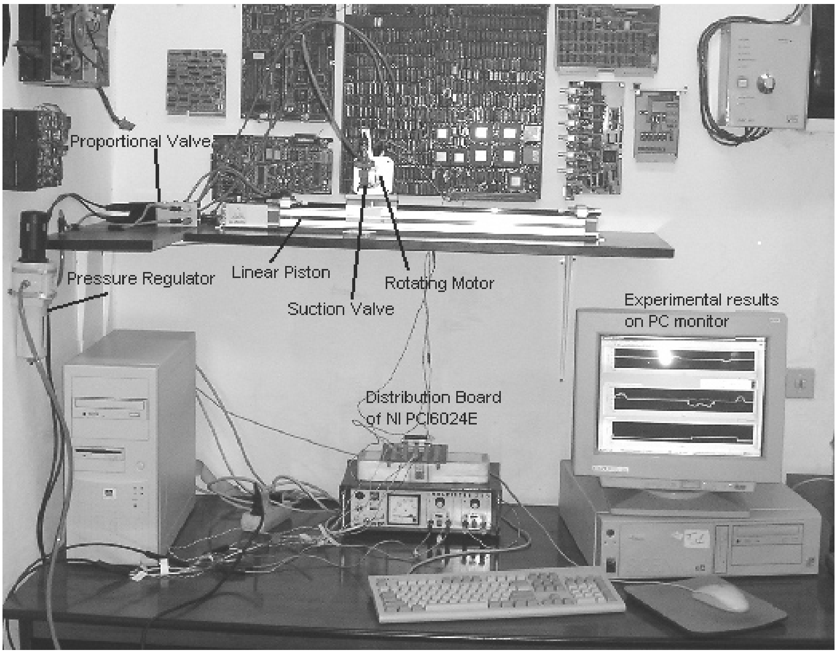


Fig.9

CONCLUSION

This application was designed and started up to create a base for future development for Control Systems design and research. From this point, with minor interventions the application can be changed. The linear piston loop has to be added by processing the can BUS signals.

REFERENCES

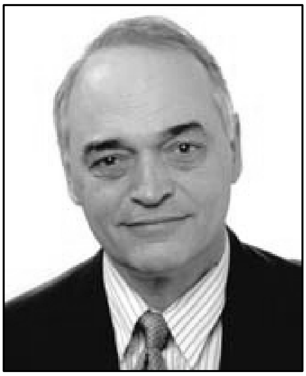
Cottet F., Ciobanu O. *Bazele programării în LabView,* Matrix Rom, București, 1998

Bishop R.H., *LabVIEW Student Edition 6,* Prentice-Hall, 2001

Festo AG & Co.KG *Assembly instructions* , 2004.

SMC, *Electropneumatica practic*a, 2004

SMC, *Introducere în pneumatica practică,* 2004



Eugene ROVENȚA
Computer Science and Engineering Department
York University, Toronto, ON
Office: CSEB 3026
Voice: 416-736-2100 ext. 33928
E-mail: roventa@yorku.ca

George ROŞU
„Aurel Vlaicu” University of Arad, Engineering Faculty
Bd. Revoluției nr. 77, 310130, Arad, Romania,
E-mail: george_rosu_s@yahoo.com

PROLOG EXPERT SYSTEM: THE DIAGNOSIS OF KIDNEY DISEASES

NOTE: This paper was presented at the International Symposium "Research and Education in an Innovation Era", Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

ABSTRACT

A Medical Expert System made in Visual Prolog is proposed. This Expert System makes a differential diagnosis among the main kidney diseases. The diagnosis is made taking into account the clinical exam (the symptoms that can be seen and felt) and the paraclinical exam (the results of laboratory tests). This system is designed to give help to a medical expert in making the appropriate diagnosis of a patient. Why would it be needed in helping a physician? Because the kidney diseases have a lot of common symptoms and many of them are very much alike, fact that makes it very difficult even for a kidney specialist to put a right diagnosis. The proposed Expert System can address that. It contains in its knowledge base twenty-seven kidney diseases from nine different categories.

KEYWORDS:

Expert System, Differential diagnosis, Clinical and paraclinical exam,

INTRODUCTION

1. MEDICAL EXPERT SYSTEMS

Artificial Intelligence is defined as intelligence exhibited by an artificial entity. AI programs that achieve expert-level competence in solving problems in task areas by bringing to bear a body of knowledge about specific tasks are called *knowledge-based* or *expert systems.* A lot of Expert Systems are build in medical domain. Their purpose is the diagnosis and treatment of certain diseases. A Medical Expert System is made out of a group of programs and a medical knowledge base with which one can have a dialogue with a computer. The information obtained from the computer is similar to the information given by an expert doctor in that certain area.

1.1. The Proposed Medical Expert System

The proposed system has in its knowledge base twenty seven kidney diseases from nine different categories. The user is asked to answer with **Yes** or **No** if a certain symptom appears or not. In the end, based on the user's answers, the name of the disease is posted up on the screen. A "minus" of this system (and usually of any other Expert System) is that only the symptoms put in the knowledge base by the programmer are available. It doesn't think and doesn't learn by itself; but the knowledge base can be updated anytime with new symptoms and new diseases.

1.2 The Sections of the Program

The „facts" section

In this section we have declared two facts:

xpositive(symbol,symbol) – for a positive answer and
xnegative(symbol,symbol) – for a negative answer

which will be used in defining the rules for the predicates „positive" and „negative", like this:

```
positive(X,Y):-
        xpositive(X,Y),!.
  positive(X,Y):-
        not(xnegative(X,Y)),
        question(X,Y,yes).
```

- if the answer to the question is affirmative;

```
  negative(X,Y):-
        xnegative(X,Y),!.
  negative(X,Y):-
        not(xpositive(X,Y)),
        question(X,Y,no).
```

- if the answer to the question is negative.
Of course that the negation of a negation is an affirmation and the negation of an affirmation is a negation.

The „predicates" section

In this section we have declared the following predicates:

```
  disease(symbol) - nondeterm (o)
  is_disease(symbol) - nondeterm (i)
  question(symbol,symbol,symbol)-    determ (i,i,i)
  remember(symbol,symbol,symbol)- determ (i,i,i)
  positive(symbol,symbol) - determ (i,i)
  negative(symbol,symbol) - determ (i,i)
```

```
clear_facts - determ ()
run - determ ()
```

The predicate „disease" will have as a parameter the name of the disease in the **clauses** section. The predicate „is_disease" will have as a parameter the category of diseases which the certain disease takes part of. This category is defined and recursively appealed each time it is met in the program.

The predicate „question" is the predicate of a „no" or "yes" answer. The clauses (the rules) for this predicate will be shown in the section „clauses".

The predicate „remember" is used by the program for remembering the answer given to a fact, before adding more facts while running the program, through the pre-defined predicate „assertz", like this:

```
remember(X,Y,yes):-
        assertz(xpositive(X,Y)).
remember(X,Y,no):-
        assertz(xnegative(X,Y)).
```

Through the predicates „positive" and „negative" we introduce the symptoms of the disease: the symptom is put as an argument at „positive" if it is available for that certain disease, respectively as an argument at "negative" if it is not available.

The predicate „clear_facts" is used for stopping the compiling of the program, and the predicate „run" is used for running the program.

The „clauses" (rules) section

In this section we introduced all the rules that define the diseases, using the predicates „disease", „is_disease", „positive" and „negative", defined in the predicates section.

For a better understanding we illustrate here the rules for one disease:

```
disease(sindromul_Goodpasture):-
       positive(se_semnaleaza,hemoragii_pulmonare),
        is_disease(glomerulonefrita_rapid_progresiva),
         positive(apare_o_infectie_a,cailor_respiratorii_superioare),
         positive(simptome_respiratorii,tuse_dispnee),
positive(anemia_este,variabila),
         positive(hematuria_este,microscopica_si_moderata),
positive(proteinuria_este,moderata),
        positive(hipertensiunea_arteriala,este_usoara),
         positive(apar_fenomene_articulare,artralgii_variabile),
         negative(complexele_imune_circulante,sunt_crescute),
positive(fractia_C3,este_normala),
         positive(ureea_sanguina_si_acidul_uric,inregistreaza_valori_crescute),
         positive(se_evidentiaza_prezenta,unor_infiltrate_pulmonare_bazale),
         positive(imunofluorescenta_evidentiaza,depozite_liniare_de_imunoglobuline_IgG).
```

In the following we present the common clause for the category “Glomerulonefrite rapid progresive” (in this case), which is called in the rules from all the diseases in this category.

```
is_disease(glomerulonefrita_rapid_progresiva):-
       positive(se_semnaleaza_inflamatie_glomerulara,si_oligoanurie),
positive(debutul_e_lent_progresiv,rar_acut),
  positive(evolutie_spre_insuficienta_renala,in_perioada_de_cateva_zile_la_cateva_luni),
       positive(leziunea_predominenta_o_reprezinta,glomerulita_extracapilara).
```

We also have the clause for „question”, using the predicate „remember”:

```
question(X,Y,yes):-!,
           write(X," ",Y,'\n'),
           readln(Reply),nl,
           frontchar(Reply,'y',_),
           remember(X,Y,yes).
   question(X,Y,no):-!,
           write(X," ",Y,'\n'),
           readln(Reply),nl,
           frontchar(Reply,'n',_),
           remember(X,Y,no).
```

Here is the clause for the predicate „clear_facts”:

```
clear_facts:-
          write("\n\nPress <<space>> to exit. \n"),
          retractall(_,dbasedom),
          readchar(_).
```

„Jumps” out of the program when pressing „space”: „retractall” (deletes facts while running) and „readchar”(reads a “char” variable) – these are pre-defined predicates in Prolog.

The clause for the predicate „run”:

```
 run:-
          disease(X),!,
          write("\nThe disease having all these symptoms is:  ",X),
          nl,
          clear_facts.
   run:-
          write("\nThis disease cannot be determined. \n\n"),
          clear_facts.
```

The program calls the predicate „disease” and posts up on the screen the name of the disease (read from the argument), and in case it cannot find all the symptoms or the disease cannot be identified it gives a certain message.

The „goal” section

Here the “run” predicate is called and also the program posts up on the screen information which the user will be able to read when running the program (the name of the system, who made it, how to use it etc.).

2. HOW THE PROGRAM WORKS

We consider for example a certain disease from a certain category. The program "thinks" like this: if it has a positive answer to a symptom, it goes on with the symptoms from that disease. If only one symptom from the disease is negative it "jumps" to the first symptom from the next disease. Of course that in takes into accounts the category symptoms also. If at least one symptom from the category is negative, the program goes to the next disease. If all the category symptoms are affirmative, it goes on to the symptoms which make the difference between this disease and the other diseases from this category.

3. FUTURE IMPROVEMENTS

The knowledge base can be improved with new diseases and even new symptoms.

An important way of improving this Expert System is using fuzzy techniques. In this case the system would establish the degree that the diagnosis is close to the reality.

Here we present some ideas for fuzzifying the Prolog rules:

p(X,a) :- q(X,u), r(X,Y,v). where:

a = degree to which „X" satisfies „p";
u = degree to which „X" satisfies „q";
v = degree to which„(X,Y)" satisfies „r".

The degree is a number between 1 and 0.

$$\mathbf{a = sup(u \wedge v)}$$

Example:

big(X,a) :- tall(X,u), heavy(X,v). which means:

X is big (with a degree a) if X is tall (with a degree u) and X is heavy (with a degree v).

In this way we could fuzzify all the rules in this program to obtain the degrees in diagnosis of the kidney diseases.

CONCLUSIONS

Taking into account the fact that we are dealing with a person's health and we have to put an approximate diagnosis on a certain disease, this system used in practice implies a great risk. In reality there are more kidney diseases than we have in this system's knowledge base. Therefore, our knowledge base is not complete, but we can update and improve it anytime with new symptoms and new diseases.

On the other hand, it is possible that the symptoms already present are not 100% right, because different experts have different opinions and there are a lot of anomalies in Medicine.

REFERENCES

[1] Bostaca, I. (1999) *Cheile diagnosticului în clinica medicală*, Editura Polirom.

[2] Gluhovschi, G. (2004) *Curs de Nefrologie*, Lito U.M.F.T.

[3] Romoşan, I. (1999) *Rinichiul. Ghid diagnostic şi terapeutic*, Editura Medicală.

[4] Luger, G.L. (2002) *Artificial Intelligence. Structures and Strategies for Complex Problem Solving,* 4ed., Addison-Wesley.

[5] Negnevitski, M. (2002) *Artificial Intelligence Guide to Intelligent Systems*, Addison-Wesley.

[6] Rovența, E. (2000) *Elements de logique pour l'Informatique*, GREF Toronto

[7] Rovența, E., Spircu, T. (in publication) *Management of Knowledge Imperfection in Developing Intelligent Systems*, Springer-Verlag

[8] Russell, S., Norvig P. (1995) *Artificial Intelligence. A Modern Approach*, Prentice Hall.

[9] Rowe, N.C. (1988) *Artificial Intelligence through Prolog*, Prentice Hall.

[10] Bratko, I. (2000) *Prolog Programming for Artificial Intelligence*, Addison - Wesley.

[11] Nilsson, U., Maluszynski, J. (2000) *Logic Programming and Prolog*(2ed), John Wiley & Sons Ltd.

[12] Reghiş, M., Rovența, E. (1998) *Classical and Fuzzy Concepts in Mathematical Logic and Applications*, CRC Press New York