Proceedings of the 2010 International Conference on Computational and Mathematical Methods in Science and Engineering

Almería (Andalucía), Spain

June 26-30 2010

CMMSE

Computational and Mathematical Methods in Science and Engineering

Editor:

J. Vigo-Aguiar (Spain)

Associate Editors:

H. Adeli (USA), J. A. López-Ramos (Spain), S. Oharu (Japan), J. Ranilla (Spain), J. Rosenthal (Switzerland), N. Stollenwerk (Germany), Ezio Venturino (Italy) and Bruce A. Wade (USA)

ISBN 978-84-613-5510-5

Register Number: 09/9851

Front Cover: "The Mathematician", Diego Rivera (1918)

Printed on acid-free paper

Contents:

Volume IV

Proceedings of the 10th International Conference
on Computational and Mathematical Methods
in Science and Engineering, CMMSE2010
Almeria, Spain, 27-30 June 2010

Wireless teleoperation system for vehicles based on automaton and secure communications

J.A. Gázquez[1], N. Novas[1] and J.A. López-Ramos[2]
[1] *Department of Architecture of Computers and Electronics, University of Almeria, 04120 Almería, Spain*
[2] *Department of Algebra and Analysis, University of Almería, 04120 Almería, Spain*

emails: jgazquez@ual.es, nnovas@ual.es, jlopez@ual.es

Abstract

We present a teleoperation system via radio for vehicles of combustion engine or electric, designed for usings in which human presence is not adequate, such as access to dangerous sites after catastrophes, spraying tasks in farming environments, road rollers, etc. The system has been developed by means of a radio modem of specific purpose that interchanges digital information of commands from the console to the vehicle and states from the vehicle to the console. A security system prevents against non-desired functioning in case of loss of communication or outsider intromissions. This system has been implemented and successfully tested in a prototype of vehicle used for spraying tasks.

Key words: Telecontrol, finite automaton, secure communications

1. Introduction

There exist several control systems of vehicles for several usings. On one hand we have autonomous functioning vehicles such as those described in [1] and [2]. This type of vehicles does not need an operator and have autonomy for the followed route. They are based on a navigation schedule. Therefore autonomous systems present as main problems the necessity of information a priori about the work environment and possible changes in such environment, taking decisions in non-expected situations and a big complexity of the sensorial system that allows the autonomous functioning, including a local computer with high capability of

 ISBN 13: 978-84-613-5510-5

calculus and information storing, usually by means of a hard disk. By the precedent, autonomous systems need a complex and delicate control system.

On the other hand, well-known classical telecontrolled systems require a permanent attention and direct observation of the behaviour of the vehicle by the operator. The solution of events such as loss of communication may cause serious consequences in these systems or in the environment. The system that we introduce and have implemented is based on that the operation console interprets what is the desired action to be developed and, by means of a dialogue of operative commands and state responses, the vehicle carries out the desired tasks, solving, automatically, possible problems of the classical case such as loss of communication and decreases the bandwidth of the communication channel. Moreover, our system allows taking pre-programmed decisions in case of non-expected events, such as automatic detention in case of loss of communication or proximity to an obstacle in its trajectory. This system is adequate for controlling vehicles that can be directly watched by the operator or monitored by video cameras in the vehicle. Security of communications is also important depending on the purposes of the vehicle. We have used a novel key selection method for real time communications based on a Linear Feedback Shift Register which allows selecting keys from a list in a pseudorandom manner.

1.1 Technology

The digital communication system has been implemented by means of bidirectional narrow band radio-modems, in the band of 400-470 MHz. The modulation is 4L-DFSK with a speed of 9600 bits/s, which is enough since the control system in the vehicle is continuously attended by a local control and the communication system only transfers operative commands from the operation console to the local control. The vehicle has incorporated as local control a system based on a microcontroller of the family MCS-51 with the embedded program in flash memory. The system has digital outputs by means of drivers of solid state, relay outputs and analogical power outputs with PWM technology to act on the elements of control of the vehicle.

The operation console has a joystick in order to input the information about motion, stop or motion directions by the operator. It also has lightning indicators that inform the operator about the state of the vehicle in what concerns to actions developed by the vehicle in real time. The console system has been implemented by means of an embedded microcontroller, taking into account a low consume in order to be supplied with batteries

 ISBN 13: 978-84-613-5510-5

2. System Design

Our system, Figure 1, is formed by two interconnected subsystems via the wireless communication device (radiomodem). The first one is constituted by the operation console and the other one is located in the vehicle and corresponds to the control system of drivers of the engines, direction control and additional functionalities, such as a spraying system control, cameras, etc.

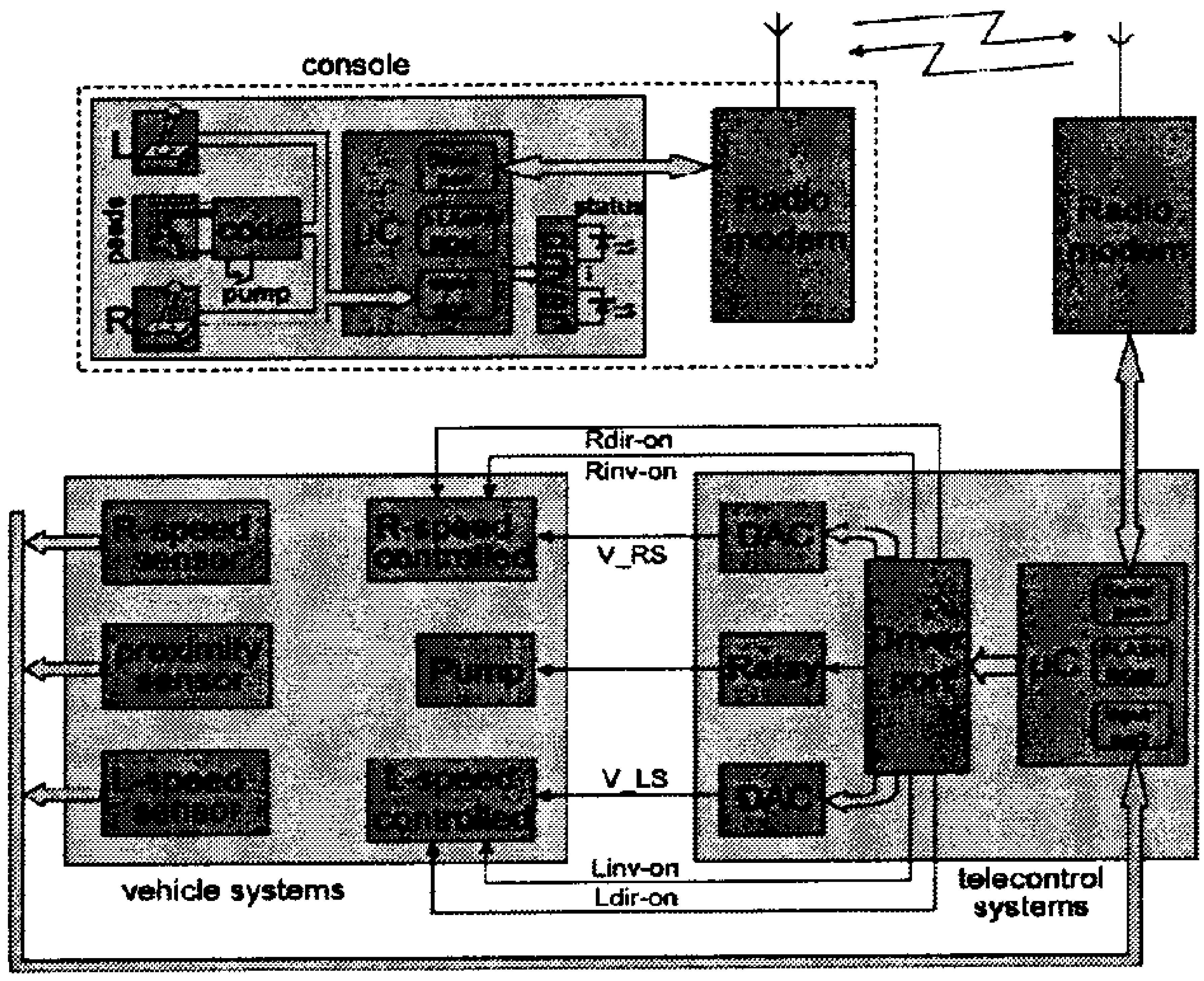

Fig. 1 *Block diagram of the system*

2.1 Console

The console is formed by a couple of joysticks, a speed selector, interrupters for activation of mechanisms in the vehicle such as spraying functions in the case of a vehicle with farming purposes, and lightning indicators of the state of the vehicle, that inform about the state of communications and actions that are being carried out by the vehicle. The system in charge of the reading of the console controls is based on a microcontroller of the family MS51 whose functioning is as follows. A finite automaton, Figure 2 implemented in the microcontroller makes the functions of reading and encodes as input all possible combinations of the console controls, that jointly with the information of the previous state, allow interpreting the action that the operator wants to carry out. This action is encoded as the output of the following state. The outputs of the states are transmitted to the

 ISBN 13: 978-84-613-5510-5

control system of the vehicle by means of the communication system (narrowband radiomodem) as packets with a ratio of two packets per second. After emitting each packet, the console receives a packet coming from the vehicle with information about its state. This state is shown on the lighting indicators. This ratio is adequate for tracked vehicles since they manoeuvre slowly. For other kind of vehicles with more speed and that require a faster response time this system allows to increase what needed the packets ratio for a right functioning

The codification system that is described corresponds to a model implemented on a tracked vehicle with spraying purposes. This vehicle moves at slow or moderated speeds and it was checked that 4 speeds (vslow, slow, middle, high) and the stop state are enough for its manoeuvre. However, from this model we can extrapolate applications to other types of vehicles considering minor modifications.
The codification of the states constitutes a finite automaton, whose entries correspond with the steering levers, the speed selector and the interrupter of the trigger sprayer pump.

The entry alphabet S possesses three subsets: the first one, with respect to the direction Sd={d11, d10, d01, d00, d0-1, d-10, d-1-1, d1-1, d-11} in function of the state of action of the drive state of steering levers. In this way the entry d11 indicates the two levers forward, d00 stop, d0-1 left lever stop y right lever backward, etc; the second one with respect to speed Ss={s00, s01, s10, s11}
s00 -> vslow, s01->slow, s->10 medium and s11->high and finally with respect to the actuator Sa={a0, a1} ao -> no action, a1 -> action.

The subset of direction entries produces a subset of states which are dependent on the direction according with the following table:

dL dR	state	Effect
1 1	S1	Straight
1 0	S2	front-right
0 1	S3	front-left
0 0	S0	Stop
0 -1	S6	reverse- left
-1 0	S5	reverse-right
-1 -1	S4	reverse-straight
1 -1	S7	turn on clockwise direction
-1 1	S8	turn on anti-clockwise direction

 ISBN 13: 978-84-613-5510-5

Not all possible transitions between states are possible for a right functioning. The next diagram defines an automaton with the set of states reduced direction of the movement.

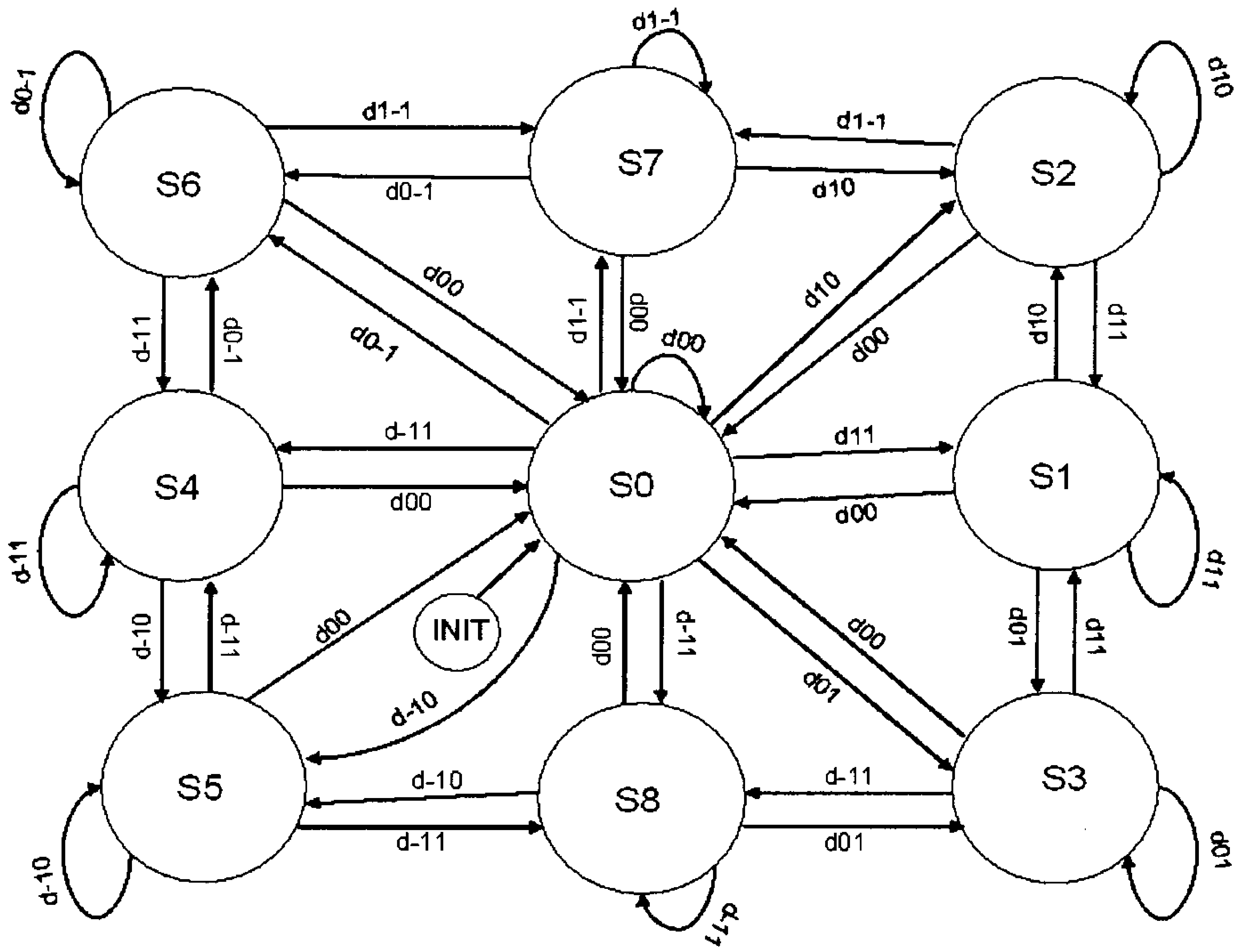

Fig. 2 *Automaton representing states and transitions*

We have taken into account that we cannot pass from entries 1 to -1 and viceversa without passing through entry 0.

For each of the states of this subset we have as a new subset the speed and the actuator system, which produces a total number of 72 possible states, although not all of them will be considered in practice because of the following exceptions:
- rotational states on its axis S8 and S7 only admit the lowest speed, ignoring other speed entries.
- in the states which imply a turn S2, S3, S5 and S6, the band corresponding to stop, what it is carried out in practice is to decrease one degree in the speed and it will only be stop when the speed selector is in vslow.

 ISBN 13: 978-84-613-5510-5

2.2 Vehicle control

The controller of the actuators of the engine of the vehicle has been implemented in a microcontroller of the same type of the console by means of another automaton. This automaton receives as inputs the packets that are sent by the console and jointly the sensorial information about direction, speed and proximity to obstacles of the vehicle, determine its next state that contains the outputs towards the actuators and the state information to be sent back to the console.
Proximity detectors in the vehicle generate the entries Sp = {p0, p1}, where p0 indicates free way and p1 that an obstacle has been detected and detention is needed.
Communications state generates the entries Sf = {f0, f1}, where f0 indicates that the last two packets have been recieved with a right checksum and f1 indicates that two consecutive errors of checksum in the packets o that they have not been received (see Figure 5). In case that the vehicle does not receive two packets of orders consecutively (fail transmission), the automaton goes to an inactivity state.
Figure 3 represents transitions between states of speed that are mapped on the states of direction Sj, depending on the codified selector on the console Ss, the proximity detectors Sp and the state of communications Sf.

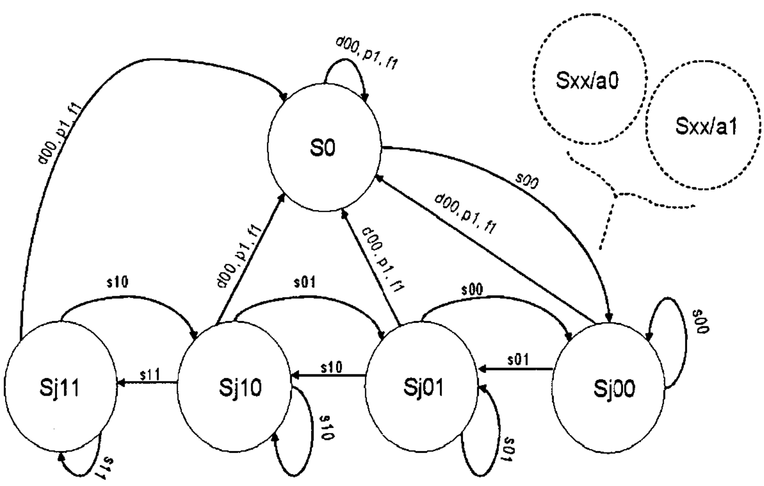

Fig. 3 Transition of states in the vehicle corresponding to speed

Each state Smn is duplicated in function of the estate of the actuator a0 to a1. The diagram of states of the vehicle does not shows differences of speed in each rolling band that is inherent to changes of direction indicated in the console automaton. We are assuming that such information is codified in each state Sj

 ISBN 13: 978-84-613-5510-5

3. Communication System

We have used a method that allows encoding the actions that at any time the vehicle can carry out using four ASCII characters. Figure 4 shows an example of the encoding used for some states in the case of tracking vehicles with a spraying system. Other vehicles with a more complex functionality can also use this system by adding some characters to the states encoding. This system of states encoding allows notorious saving in band width with respect to classical telecontrol systems and so a bit-rate of 4800 b/s is enough to the bidirectional communication (orders sending/receiving of states). Narrow band communication systems by radio are the most adequate for this type of telecontrol operations by the high ratio distance/power with low consumption, their stability and reliability and a lot of operation channels to be used. We have used a radiomodem with bit-rate 9600 b/s and F.E.C. ¾ in the UHF common used band 433 MHz.. The power of 250 mW are enough to a long distance control of the vehicle. Other communication systems such as Bluetooth or Zigbee can be used to implement this system for telecontrol in short distance, substituting the narrowband radiomodem, but with possible collisions with other users given the more extended use of these types of communications. Moreover this system increases the reliability of the control of vehicle. In case of a packet is mismatched in the communication process and F.E.C. does not detect and correct the error, this does not produces any action unless it coincides with some of the expected packets related with the state of the automaton at that time.

4bytes	1bit	1bit	1bit	1bit	1bit	2bytes	
COM	Rdir	Rinv	Ldir	Linv	pump	speed	action
0000	0	0	0	0	0	00	stop
AA01	1	0	1	0	0	01	run forward slow speed
BB23	1	0	1	0	1	23	run forward normal speed pump
GG17	0	1	0	1	0	17	run reverse normal speed
AD07	1	0	0	0	0	07	run turn left slow speed
AB07	1	0	0	1	0	07	turn on its axis slowly

Fig.4 *Example of state encoding*

One example of chronogram of the interchange of information between the vehicle and the console of control is given in Figure 5. It can be observed the messages transmitted by the console and the corresponding answers by the vehicle. In this case after a series of commands that order the running of the vehicle, all of them answered by the vehicle with its state, two consecutive fails occur due to interference or any other cause, recall that all the radio communication systems are susceptible of loss of information. In this case the vehicle goes to a stop state, restarting the running after receiving another valid command from the console.

 ISBN 13: 978-84-613-5510-5

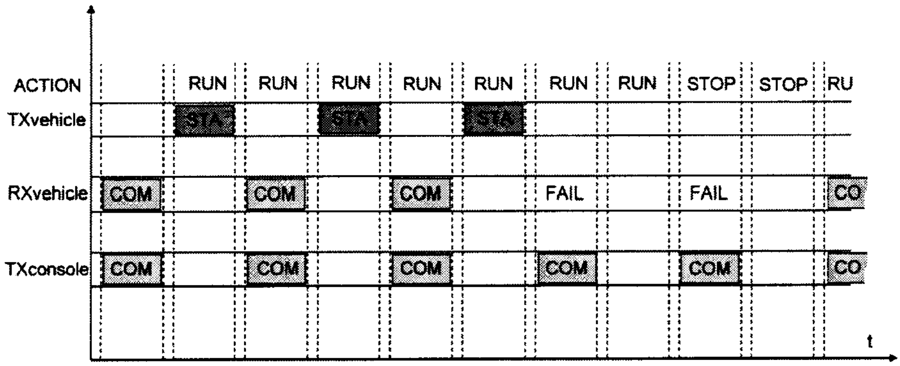

Fig. 5 *sequence of communications packets*

3.1 Security of communications

The fact that communication between the vehicle and the console takes place in real time is of a great importance. There exists a class of algorithms, known as stream cipher algorithms such that all of them treat the information bit-to-bit, usually binary digits and in real time and are very appropriate when buffering is limited some telecommunications applications as could be a radio modem. They are based in Linear Feedback Shift Registers (LFSR), which give an encryption sequence and are very suitable for hardware implementation (cf. [4] for details).
We use good properties of LFSRs to give an efficient selection key method which allows generating sequences of key identifiers. Source an destination share a list of keys and an easy algorithm to generate sequences of identifiers and therefore, these are not sent, which solves questions relative to possible compromised pairs of key-identifier and only some additional information bits about the initial state of the system that generates the sequence of identifiers is required to encrypt/decrypt a big number of blocks of information.

3.1.1 The key selection method

In this case, the source A (console or vehicle) and the destination B (console or vehicle) use a b lock cipher and share a list of l keys and an algorithm to generate a sequence of positions (identifiers) of the list of keys. The algorithm that we use consist in a binary LFSR (stages store one bit) with k stages, such that $2k \geq l$ and a Boolean function whose input is the state vector of the LFSR at some moment and its output is a number in the range 1- l.
Now if A wants to send a message to B then A proceeds as follows:

 ISBN 13: 978-84-613-5510-5

1. A divides the plain text into packets Pj, j=1,…,n of blocks Bj,i, i=1,…,r of appropriate length .

2. For j=1,…,n, A generates, by means of a Real Time Clock, a random number of k digits, Sj, which is taken as initial state of the LFSR.

3. Using the LFSR and the Boolean function, A generates a sequence of numbers j,i for i=1,…,r in the range 1-1 and consider the key whose position in the list is j,i ,kj,i.

4. A encrypts every block Bj,i of the packet Pj, j=1,…,n, using the key kj,i, obtaining packets of blocks Cj, for j=1,…,n.

5. A sends Sj and Cj for j=1,…,n to B.

When B receives Sj and Cj, he uses Sj to generate the sequence of keys necessary to decipher the message.

In case we do not want to send Sj as plain text, we can use some of the characters of the first encrypted block of the packet Cj to get a new seed for the LFSR and so, generate a pseudorandom number which gives an identifier of a new key k to encrypt Sj. In that case, when B receives the message proceeds as follows:

1. B takes selected characters of Bj,1 to get a seed for the LFSR and gets the identifier of the key k.

2. B uses k to get Sj.

3. B uses Sj to get the sequence of keys kj,i and decrypts packet Cjj=1,…,n

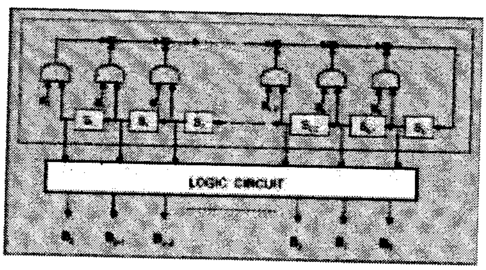

Fig 6. Key selection method

Figure 6 shows a diagram composed by an LFSR whose state vector is taken as input of a logic circuit given by a Boolean function, which produces keys kj,i. This method has been also used in [2] and [3] for telecontrol and telemetry applications.

4. Conclusions

We have introduced a novel teleoperation system for vehicles based on a finite automaton and with a secure communication system which allows to handling vehicles for different purposes in an easy and safe way. This system was

 ISBN 13: 978-84-613-5510-5

implemented on a platform for greenhouses spraying [5]. The functioning given by the designed automaton shows an easily operable vehicle and with an acceptable level of security, in what concerns to possible loss of control and with a high security level of communication in what concerns to possible interferences or outsiders as evidenced after a long testing period [6].

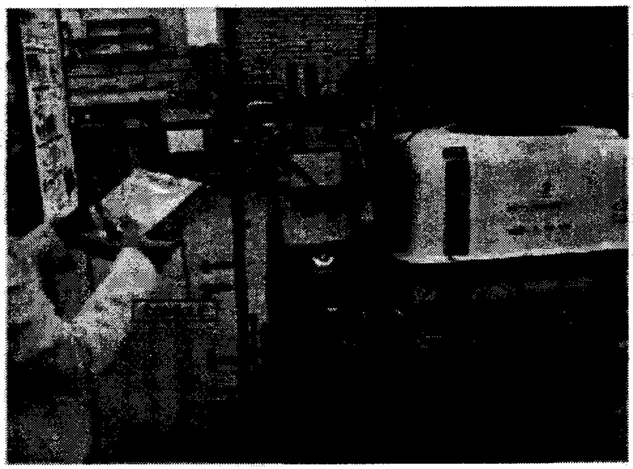

Fig 7. Vehicle and console

4. Acknowledgements

This paper was supported by TEC2009-13763-C02-02. First and second authors are also supported by TIC019. Third author is supported by FQM0211.

5. References

[1] A. MANDOW, J.M. GOMEZ, J. MARTINEZ, V. MUÑOZ, A. OLLERO AND A. GARCIA, *The autonomous mobile robot AURORA for greenhouse operation, vitiation*, IEEE Robotics Automation Mag. **3**(4) (1996) 18-27.

[2] M. DEVY, R. CHATILA, P. FILLATREU, S. LACROIX AND F. NASHASHIBI, WITTEN, *On autonomous navigation in a natural environment*, Robotics and Autonomous Systems **16**(1) (1995) 5-16.

[3] N. NOVAS, J.A. LOPEZ-RAMOS, J.A. GAZQUEZ AND J. PERALTA, *Unidad cifradora/descifradora de mensajes con informacion digital,* Spanish Patent P200402603 (2004).

[4] A. MENEZES, P. OORSCHOT AND S. VANSTONE, *Handbook of Applied Cryptography,* CRC Press (1996).

[5] J. SANCHEZ-HERMOSILLA, F. RODRIGUEZ, M. BERENGUER, D. MORALES AND J. GUZMAN, *Mobile Robot for spraying in greenhouses,* RWorkshop on Spray Application Techniques in Fruit Growing, Barcelona (2006).
[6] http://www.ace.ual.es/~jgazquez/icons/televeh1.MPG

 ISBN 13: 978-84-613-5510-5