Command transmission in power control centers

Joaquin Luque, Jose L. Calvo

Departamento de Ingenieria Electronica. Universidad de Sevilla.
E.T.S. Ingenieros Industriales. Avda. Reina Mercedes s/n. 41012-SEVILLA. SPAIN.

ABSTRACT

An study on command transmission security in complex systems is presented. The main objective is to garantee error rates under the limits recommended by the international organizations, keeping the communication channel occupation as low as possible.

Two methods increasing the security are analysed and compared: the redundant bits addition and the command message repetition. Using simulation techniques, the results are applied to the command transmission in the power control centers.

1. INTRODUCTION

In many control systems one of the most critical functions is the command transmission from one computer to another one. This is many times the most important function in the system and, though don't be used continously, everything must be ready in the right moment for sending the requested commands in a fast and secure way.

And even one of the most importants factors designing a control system is the security carrying out the commands. Therefore these systems are designed with a set of rules providing from specials redundancies in the man-machine interaction to hardware tests directly on the controlled element.

The communication system is not inconsistent with this security requirements and the maximum restrictions are applied to the fail probability of the command message. We say a command message has failed if the receiver understand a different command wich was sent, carrying out an unwanted action on the system.

For the electric power control centers an international recommendation exists due to CIGRE (Conference International de Grand Reseaux Electrique) wich says that the failing probability of a command message must be under a limit wich depends on the channel error rate, anyway lower than 10^{-12}.

2. FORMULATION

Let us suppose the command transmission message M is constituted by n bits: m data bits and r redundant bits computed by the algorithm A. Among the data bits there are k critical bits that in case of being changed and not detected will lead to the reception of a different valid message wich was sent: a fail in the command transmmision.

In the other side there are c non-critical data bits that in case of being changed and not detected, will lead to not carrying out the command but not carrying out a different command wich was sent. We can write

$$m = c + k \qquad\qquad n = c + k + r \tag{1}$$

It is called residual error probability in the command transmission, the probability of a command transmission fail, that is to say, the probability that a change in any critical bits occurs not being detected by the algorithm A. If we call p the channel error rate, we can write

$$P_r = f(A,M,p) \tag{2}$$

and if we fix A and M

$$P_r = f(p) \tag{3}$$

 CH2484-4/87/0000/1016$01.00

If we call Bi the number of valid messages with i erroneus critical bits, and calling $q = 1 - p$, we can write

$$P_r = \sum_i B_i \, p^i \, q^{n-i} \tag{4}$$

formula in wich the coefficients Bi depends on the message M and the error detection algorithm A. The standard error detection algorithms (for instance the CRC-CCITT) do not fit the severe restrictions imposed to the command transmission security. To solve it two approach can be choosen: the redundants bits addition, and the command message repetition a times before its execution. For the last case the Pr formula should be modified in the following way:

$$P_r = \sum_i B_i \, p^{ai} \, q^{a(n-i)} \tag{5}$$

To study the performance of both methods we have been based on the command transmission in an electric power control center in the south of Spain. With a command message standard structure we have simulated several methods for error detection. We also supose the transmission security is provided using the CRC-CCITT in every message type.

3. REDUNDANTS BITS ADDITION METHOD

In first place different algorithms with redundants bits addition has been tried. 16 and 32 bits CRC's, checksums, parities, critical bits repetitions (single, double or triple) and many others combinations (up to a total of 32) can be found among the tested algorithms. The figure 1 depicts some of thems, being the one labeled with B wich has better performances/occupation ratio with only 4 bytes of additional redundancy. This algorithm is the checksum, the parity and the CRC-16 on the critical bits plus the CRC-CCITT on the full message.

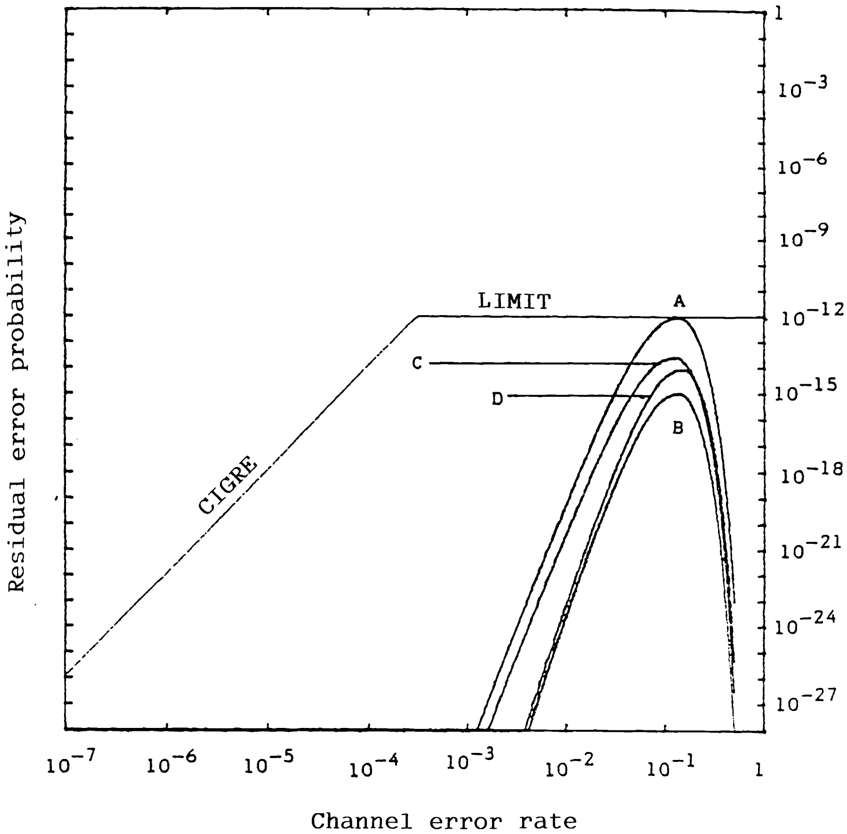

Fig. 1.- Redundant bits addition

4. MESSAGE REPETITION METHOD

The second approach lead us to the command message repetition with standard error detection algorithm. The command is not carried out until the last message has arrived without errors. The figure 2 depicts the results in the simulation of this method with different number of message repetitions and the CRC-CCITT as the error detection algorithm. The line E is the one selected previously. We can see that at least 3 commands messages are required to get an internationally accepted security.

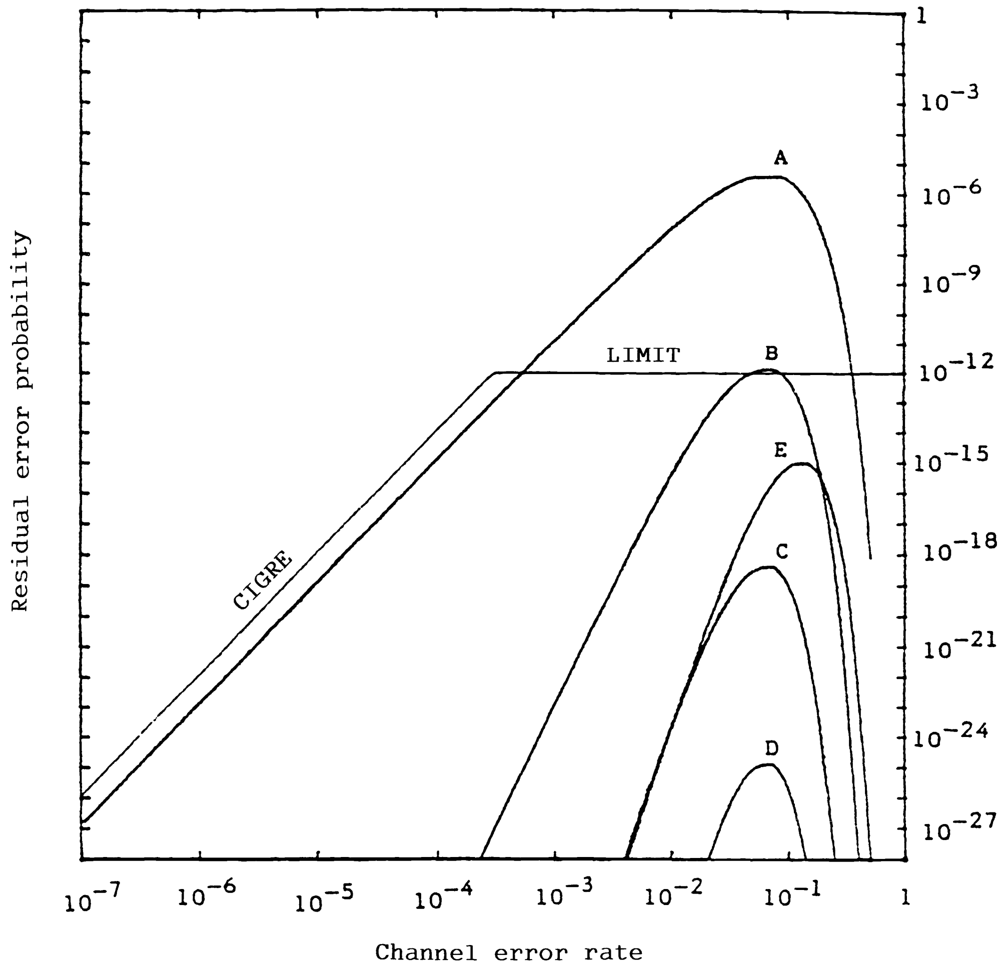

Fig. 2.- Command message repetition

5. METHODS COMPARISON

Once both messages fit the security requirements, the comparation criterion between them must be the minimum channel occupation. Developing the differents factors affecting the transmission we have obtained the following expression:

$$O = \frac{a - 1}{2\, q^{2n}} (2\, n + 2\, W) + \frac{1}{q^{n+m}} (\, n + m + 2\, W) \qquad (6)$$

where $W = V + I$, $q = 1 - p$ and

O: Channel occupation (in bits)

a: Number of transmited messages

n: Number of bits in a message

m: Number of data bits in a message

p: Channel error rate

V: Channel communication speed (bits/sec)

I: Delay times inherent to a transmission

Based on this expression, and in the tested system, the redundants bits addition method present a lower channel occupation: about 60% of the channel occupated by the command message repetition method.

6. CONCLUSIONS

Two methods ingreasing the security on command transmission in complex systems has been analysed and compared. Adding the checksum, the parity and the CRC-16 on the critical bits plus the CRC-CCITT on the full message, the best performance/occupation ratio has been obtained.

7. ACKNOWLEDGMENTS

The authors wish to thank the Compañia Sevillana de Electricidad for allowing us to use one of theirs power control centers to verify our results. We would also thank Josep M. Selga of ENHER for his helpful cooperation.

8. REFERENCES

1. CIGRE, "Operational and functional requirements for telecontrol systems". 1.980.
2. CIGRE, "Telecontrol communications protocols". 1.980.
3. J. Luque, "Estudio y optimizacion de las comunicaciones entre procesadores para el control de sistemas complejos en tiempo real". Tesis doctoral. Universidad de Sevilla. 1.986.