Mechanics Transport Communications
Academic journal

ISSN 1312-3823
volume 12, issue 3/2, 2014
article № 1020
http://www.mtc-aj.com

ON THE RELIABILITY AND SAFETY OF THE MICROCOMPUTERS AND THEIR RAILWAY APPLICATIONS

Assen Krumov, Borislav Boiadjiev
assenkrumov@hotmail.com, bboiadjiev@vtu.bg

Todor Kableshkov University of Transport,
158 Geo Milev Str., 1574 Sofia,
BULGARIA

Key words: *Reliability, Safety, Microcomputers, Embedded Computer Systems, Real Time, Railway Signalling Systems*

Abstract: *For the computers and microprocessors, working in a real time environment, like railway systems, the most important characteristics are the reliability and safety. In the paper the reliability characteristics of some of the widely used microprocessors and microcomputers are given. Since their safety and reliability values are not high enough for application in the safety critical systems, like railway control systems, a redundancy method using logical circuits is applied. As result a significant improvement of safety is reached and in some extent – improvement in reliability. The block diagram of the redundancy method using logical IC is shown. In the paper concrete applications of microcomputers in the railway systems are suggested, corresponding to their reliability and safety characteristics.*

For the computers and embedded systems, working in a real time environment, the most important characteristic is their dependability. The notion of dependability is broken down into six fundamental properties [1]:

(1) reliability;
(2) availability;
(3) safety;
(4) confidentiality;
(5) integrity;
(6) maintainability.

The most important theoretical characteristic between (1) and (6) is reliability. In words reliability can be described with the probability P of an item operating for a given amount of time t without failure. The probability that the system or the component will work without failure for a time τ, less than the argument t is:

(1) $$q(t) = P(\tau < t)$$

Exponential distribution is widely used for investigation of reliability in the technical and electronic fields - software and hardware. The analytical description of this distribution is:

(2) $$f(t)=\lambda . e^{-\lambda t} = (1/m).e^{-t/m},\ t \geq 0,\ \lambda > 0,\ m > 0\ ,$$

where: λ is constant failure rate, in failures per unit of measurement, *e.g* failures per hour, per cycle, etc.; $\lambda = 1/m$, where m = mean time between failures. Obviously, as $t \to \infty$, $f(t) \to 0$. Graphically this distribution is shown in the Fig.1.

When λ is constant can be proven that $q(t) \approx t.\lambda$:taking into account that:

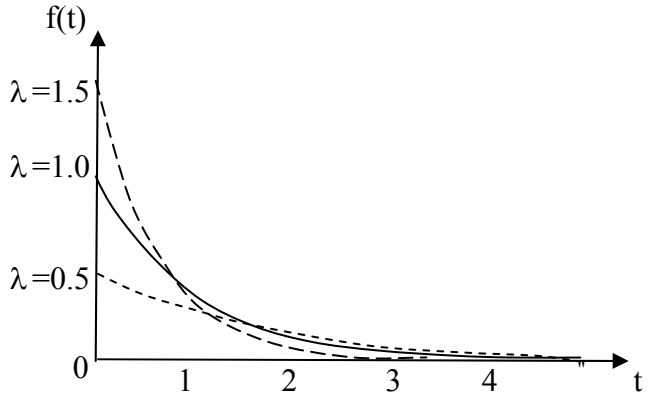
(3) $$e^x = 1 + \frac{x}{1!} + \dots$$

(4) $$q(t) = \int_0^t f(t)dt = \int_0^t \lambda.\exp(-\lambda t)dt = 1 - e^{-\lambda t} \approx 1 - (1 - \lambda t) \approx \lambda t,$$

As a result he cumulative distribution function of failures q(t) is approximately:

(5) $$q(t) \approx t.\lambda$$

Fig.1. Exponential distribution



This is the reason why the requirement for safety in the railway systems and aviation are given with λ [1/h].

The reliability characteristics [2] of some of the most popular microprocessors an memory chips are shown in Table 1.

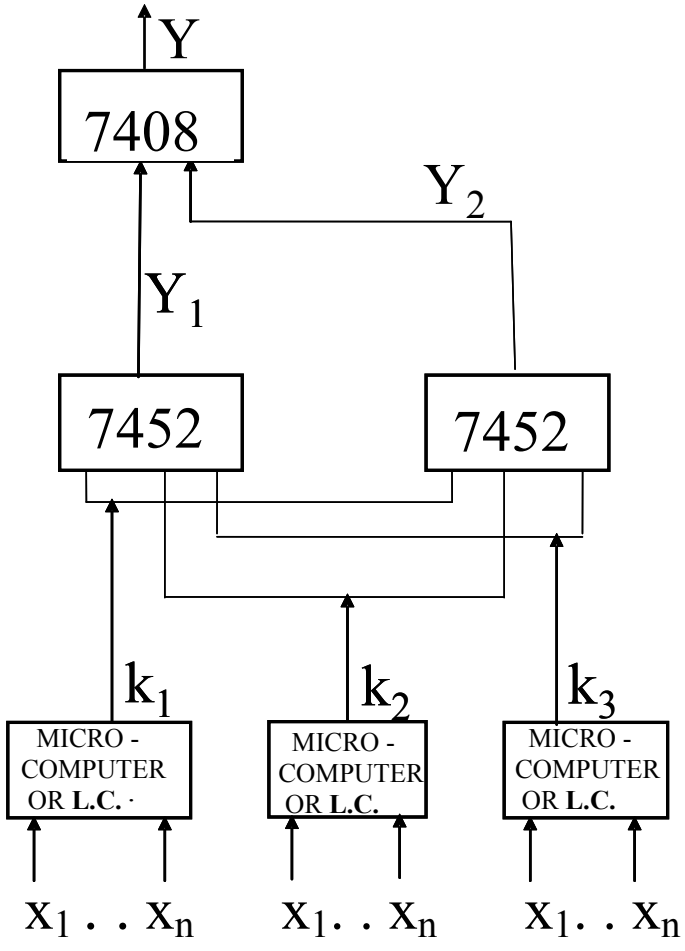
Table 1. Failure rates of IC and microprocessors

Type of IC	Function	λ [10^{-9} failure/hour]
74LS00	4 elements "NO AND"	10
2764	EPROM	9400
8085	8 bit microprocessor	190
8086	16 bit microprocessor	990

In paper [3] the dependability assessment of three cores, a PIC and an 8051 microcontroller, representative of microcontrollers commonly used in embedded applications were investigated, applying fault emulation. They present a Reduced and Complex Instruction Set Computer architecture, respectively. The third core is a custom design of a specific-purpose DSP(digital signal processor)-like architecture. The results are shown for different types of faults. For flip/flop faults **Mean-Time-To-Failure (MTTF)** is: DSP = 1/1105λ, PIC=1/721λ, 8051=1/641λ , where λ is the standard failure rate $\lambda=10^{-11}$ [faults/hour] for **flip-flops (FFs)**. Obviously the flip/flop faults can not give the total estimation of reliability. According to the experimental emulation data 8051 core presents the lowest failure rate (22.98%) and thus it could be a suitable candidate for its integration in a highly available system. However, when dealing with the system's safety, the PIC core presents the lowest probability of reaching an unsafe state (71.9%).

The data shown in Table 1 means that reliability (and as consequence safety) of the microprocessors and microcontrollers are not high enough for safety critical applications. That's why the well known [4], [5] redundancy method, applying for the first time logical circuits is suggested in [6]. This results is increase of reliability and **especially safety** of the embedded microcontrollers. The redundancy model is shown in Fig. 2.

Fig.2.Control system configuration with redundancy 2 of 3



where $x_1 \ldots x_n$ are input signals to the 3 identical microcomputers and logical circuits L.C.

In [6] probability analysis is performed on the bases that erroneous logical "1" is dangerous and concerns safety, while erroneous logical "0" reduces only reliability. The obtained results are:

(6) $$Q_{DAN} \approx 3(0.5Q_{LC})^2 + 0.5Q_{08}$$

for the probability of dangerous failure Q_{DAN} and

(7) $$Q_{REL} \approx 3(Q_{LC})^2 + Q_{52} + Q_{08}$$

for the probability of any failure Q_{REL} (dangerous and non dangerous).

For the case of dangerous failures (6) it is obvious that it depends mainly on the probability of failure of IC 7408, which is approximately the same as that of 74LS00 , λ [10^{-8} failure/hour], because Q_{LC} is to the power of 2. This means that if microprocessors 8085 or 8086 are applied, the probability of dangerous failures will be reduced 38 times (8085) and 198 times (8086) if the redundancy method is applied.

It can be expected that the obtained probability Q_{REL} of any failure (7) will be in most cases less then the probability of failure of the logical circuit Q_{LC} (or microprocessor), because Q_{REL} depend mainly on the reliability of relatively simple IC- 7452, 7408.

The conclusion is that the suggested method of redundancy reduces significantly the probability of dangerous failures Q_{DAN} and in most cases the probability of any failure Q_{REL}.

The redundancy methods with different majorities are widely used in the railway signalling systems like electronic interlocking systems for stations, block systems, automatic train protection systems (for instance European Train Control System – ETCS), etc.

Above mentioned redundancy method can be used also in different types of railway signalling equipment, as follows:

1. Signals. Railway signals are the combination of different coloured lamps. These lamps are divided in two types:

- Vital – all permissive signal lamps and
- Non vital – all stop signal lamps.

Majority method can be used for controlling of the vital lamps. For them the required value of λ is 10^{-9}. For increasing of the safety, the switching of the lamps can be separated for each of the power supply poles.

2. Point machines. In this case the required value of λ is 10^{-9}. The majority method can be used for monitoring of the point position and also for the control part of the point equipment. By reason of high amperage of the machine currents, the relays shall be used for the switching equipment of the point machines.

3. Level Crossing Safety Installations (LCSI). The required value of λ is 10^{-8} . LCSI can be separated in two main types:

- For station level crossings – in this case the control of the LCSI is from the corresponding interlocking system;
- For open line level crossings – in this case the control of the LCSI is executed from the LCSI equipment.

LCSI controls signals and half barriers if they are available. For the level crossing signals, the same methods like the vital signals (case 1 above) can be used and for the barriers the same methods like the point machines can be used.

4. SCADA systems. They are:

- For traffic control with required value of $\lambda = 10^{-9}$;
- For control of the power substations with required value of $\lambda = 10^{-8}$.

In common, for these systems the safety requirements are less strict then other signalling systems, but in some cases the redundancy method can be used too.

When microprocessors or microcomputers are applied the redundancy method described in this paper have to be used, because their values of λ are less then 10^{-8}. When the

required value of λ is 10^{-9}, than logical IC 74LS00 with increased reliability or special safety relay should be used to fulfil this requirement.

For instance in some traffic control systems, the vital commands are used and redundancy methods can be used for these cases.

The conclusion is that the suggested in the paper method of redundancy reduces significantly the probability of dangerous failures and in most cases the probability of any failure.

REFERENCES

[1]. John C. Knight "Dependability of Embedded Systems", ZCSE'02, May 19-25,2002, Orlando, Florida, USA.

[2]. Palo Sauli "Reliability Prediction Of Microcircuits", Microelectron. Reliability, vol.23, No.2, pp.283-294, 1983.

[3]. David de Andrés, Juan-Carlos Ruiz, Daniel Gil, Pedro Gil "Dependability Assessment for the Selection of Embedded Cores", Seventh European Dependable Computing Conference, 978-0-7695-3138-0/08 $25.00 © 2008 IEEE DOI 10.1109/EDCC-7.2008.19.

[4] E. Moore, C. Shanon " Reliable circuit using less reliable relays", J. Franklin Inst. ,1956, 262, p.191., p.281.

[5] J. von Neuman "Probability logics and synthesis of reliable organisms from unreliable components", Automata Studies, Prinston University Press, 1956.

[6] A. V. Krumov "Dependable computer systems", AMAZON, 2012. ISBN-13: 978-1484949504, ISBN-10: 1484949501.

НАДЕЖДНОСТ И БЕЗОПАСНОСТ НА МИКРОКОМПЮТРИТЕ И ТЯХНОТО ПРИЛОЖЕНИЕ В ЖЕЛЕЗОПЪТНИТЕ ОСИГУРИТЕЛНИ СИСТЕМИ

Асен Крумов, Борислав Бояджиев

assenkrumov@hotmail.com, bboiadjiev@vtu.bg

ВТУ "Тодор Каблешков"
София, 1574, ул. „Гео Милев" 158,
РЕПУБЛИКА БЪЛГАРИЯ

Ключови думи: *Надеждност, Безопасност, Микропроцесори, Микрокомпютри, Вградени компютърни системи, Работа в реално време, Железопътни осигурителни системи*

Резюме: *Използването на микропроцесорни и микрокомпютърни системи в областта на железопътната осигурителна техника, изисква осигуряване на висока степен на надеждност и безопасност на тези системи. В доклада са разгледани методите с използване на излишък, за осъществяване на изискванията за надеждност и безопасност, както и тяхното приложение в железопътните осигурителни системи. Предложени са някои конкретни приложения на микрокомпютри за железопътни осигурителни системи.*