INFORMATICA, 1993, Vol.4, No.3–4, 267–276

REALIZATION OF FAIL-SAFE SEQUENTIAL MACHINES BY USING INVERSION OF INPUT VARIABLES

Romanas ANDRUŠKEVIČIUS

Lithuanian Energy Institute
3035 Kaunas, Breslaujos St.3, Lithuania

Abstract. A fail-safe sequential machine is one that produces error signal when failures occure in the machine. This paper presents a new method of realization of fail-safe sequential machines under the following assumptions: 1) failure is caused by faults of logical and memory elements in the machine, 2) output of faulty elements is stuck at one or zero.

A feature of this method is that an input inversion is used for additional state assignment and this additional state is used for detection of faults of elements.

Key words: fail-safeness, sequential machine, state assignment, state transition function.

1. Introduction. A fail-safe sequential machine is one that produces error signal when failures occur in the machine. A number of investigations (Sapoznikov and Sapoznikov, 1984; Thoma, Ohyama and Sakai, 1971) have dealt with the careful encoding of the secondary state assignments of sequential machines or finite automata, often directly using the properties of error-correcting codes. These machines are encoded redundantly (hence, they have redundant states) and, if properly designed, can posses any of a number of several error-tolerant properties. The assumption of a redundant state may signal an error-detection circuit that an improper transition has occured. These investigations have dealt with the cases in which the failure is caused by a single fault of element in the machine and erroneous signal may take value one or zero. A

new method of realization of a fail-safe sequential machine for all kinds of fault of element is presented in this paper.

Let us consider a Moore-type sequential machine $\mathrm{M}(A, S, Z, \delta, \kappa)$ in Fig. 1, where in normal operation A, S, Z, δ, κ are as follows:

A – set of input alphabets;

S – set of states;

Z – set of output alphabets;

δ – state transition function, $\delta: A \times S \to S$;

$\varkappa$ – output function, $\varkappa: S \to Z$.

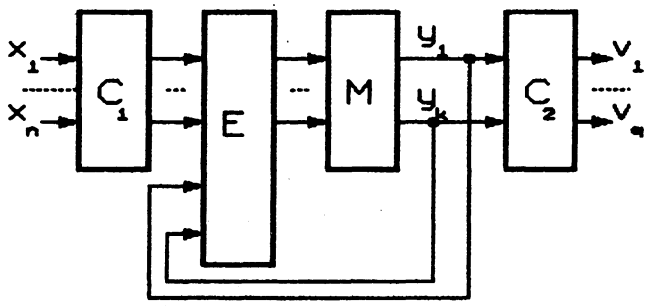

Fig. 1. Moore-type sequential machine.

Sequential machine operation is determined by the following equations:

$$s(t) = \delta(a(t), s(t-1)), \tag{1}$$

$$z(t) = \varkappa(s(t)), \tag{2}$$

where t is the number of clock time, $t = 1, 2, 3, \ldots$.

The state at clock time t is completely determined by the state transition function, by the previous state at clock time $t-1$ and by the input variables at clock time t. Output is determined only by the output function and by the state at clock t. This means that the output variables is completely determined by the state of memory elements. If a high speed operation is not required, this property can be used for fault detection.

From the point of view of fail-safeness, it is necessary to consider failures that occur in input circuit C_1, excitation circuit E, memory elements M and output circuit C_2 separately. Since the output circuit C_2 in Fig. 1 is combinational, it must be realized using a fail-safe combinational circuit (see, for example, Sogomonyan and Slabakov, 1989). Let us consider only failures that occur in the C_1, E and M circuit. Furthermore, we assume the following conditions.

1. Failure is causing by faults of logical and memory elements in the machine.

2. Fault is stationary, that is, output of faulty element is stuck at one or zero.

2. Conditions of state assignment. Let S_r be a set of states that occur under failure condition. States of S will be called normal states and states of S_r will be called erroneous states in the sequel. These states are represented by vector of n state variables $y_1, y_2, \ldots,$ and y_n.

If state transition function is modified by some fault, the state is not s but s_r. The previous state of state s is state s'. The next state of state s is state s^*.

State transition from a normal state is specified by δ, while state transition from an erroneous state at any input is not specified. After the excitation circuit is constructed the state transition from any possible state is completely determined. Let Δ be a completely specified state transition function such as

$$\forall a \in A,\ \forall s' \in S, \quad \Delta(a, s') = \delta(a, s') \in S, \tag{3}$$

and let Δ' be a modification of Δ by a failure condition. Then the above closure condition of the state transition is expressed by the following equations:
under normal condition

$$\forall a \in A,\ \forall s' \in S, \quad \Delta(a, s') = \delta(a, s') = s \in S, \tag{4}$$

$$\forall a \in A,\ \forall s \in S, \quad \Delta(a, s) = \delta(a, s) = s^* \in S, \tag{5}$$

under failure condition

$$\forall a \in A,\ \forall s' \in S,\quad \Delta'(a, s') = s_r \in S_r, \tag{6}$$

$$\forall a \in A,\ \forall s_r \in S_r,\quad \Delta'(a, s_r) = s_r^* \in S_r. \tag{7}$$

The object of this paper is to show that we can construct sequential machines that generate error signal under any failure condition.

The state s^*, if defined in special mode, can be used for erroneous state's s_r identification. We must assign such a code to each s^* that satisfies the following condition.

$$\forall s, s^* \in S,\quad s^* = \bar{s}. \tag{8}$$

State transition from state s to state s^* satisfies the following equation:

$$\forall \bar{a} \in A,\ \forall s \in S,\quad \delta(\bar{a}, s) = s^* \in S. \tag{9}$$

The erroneous state s_r can be identified by the comparison with the state s^*. It is possible if:

a) the state variables of state s are fixed in memory M,

b) before the arrival of the next clock signal the new state transition to the next state s^* take place.

The state s^* is temporal. It is changed by leading edge of new clock signal. The values of each state variables of state s^* can be compared in the special control circuit with the values of corresponding state variables of state s, which are stored in memory.

Realization of sequential machine is shown in Fig. 2.

Circuit FDC generates error signal F, if $\bar{s} \neq s^*$. As shown in Fig. 3, error signal is stuck at one $F \to 1$, if $\bar{s} = s^*$ and stuck at zero $F \to 0$, if $\bar{s} \neq s^*$.

Fault detecting circuit FDC can be constructed by using self-testing and self-checking comparison schemes which are represented in (Gossel and Sogomonyan, 1992).

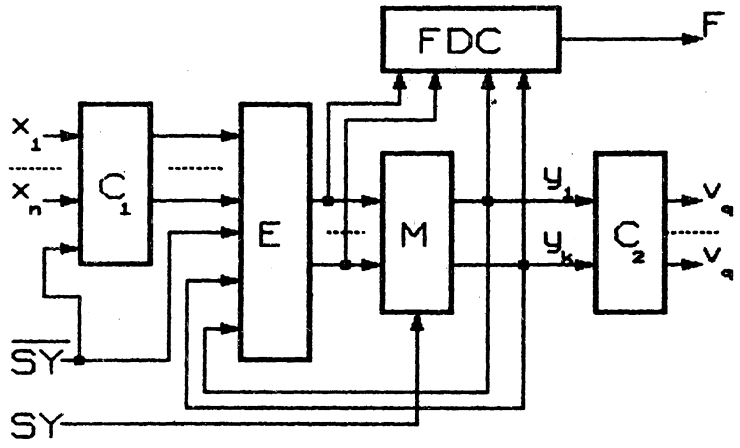

Fig. 2. Fail-safe sequential machine.

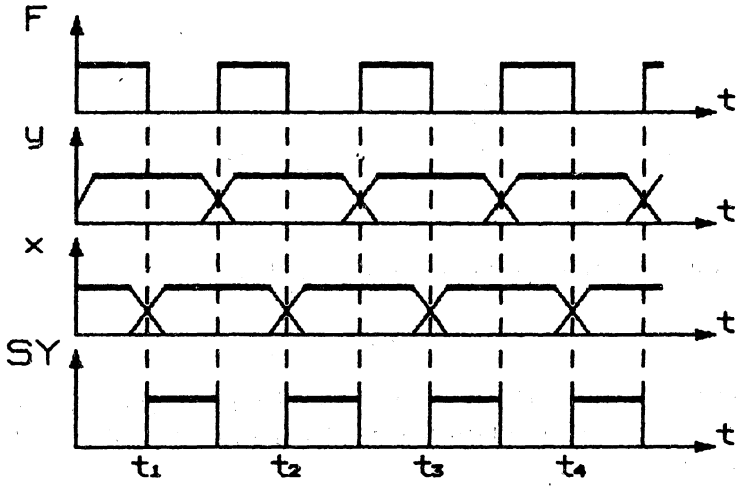

Fig. 3. Timing relation.

3. Construction of input circuit. In common the set of input alphabet A is pre-assigned. It is necessary to complement input alphabet by new elements. Let assume the set of new elements A'. For convenient fault detection, it is necessary that A and A' are disjoint.

$$A \cap A' = \varnothing. \tag{10}$$

According to equation (9) we must assign a new code to each element of A', which satisfies the following condition:

$$a'_i = \overline{a}_i, \tag{11}$$

where $i = 1, 2, \ldots, m$.

In order to satisfy these conditions, let us assume the clock signal SY (Fig. 2) as an input variable $(x_1, x_2, \ldots, x_n, SY)$. Relation between a and a' is shown in Table 1, where SY, $\alpha_{ij} \in \{0, 1\}$.

Table 1. Input alphabets assignment

x				
x_1	x_2		x_r	SY
α_{11}	α_{12}	...	α_{1n}	0
α_{21}	α_{22}	...	α_{2n}	0
...	...	...	...	...
α_{m1}	α_{m2}	...	α_{mn}	0
$\overline{\alpha}_{11}$	$\overline{\alpha}_{12}$	...	$\overline{\alpha}_{1n}$	1
$\overline{\alpha}_{21}$	$\overline{\alpha}_{22}$	...	$\overline{\alpha}_{2n}$	1
...	...	...	...	...
$\overline{\alpha}_{m1}$	$\overline{\alpha}_{m2}$	...	$\overline{\alpha}_{mn}$	1

Input function we can express as follows.

$$x'_i = \overline{x}_i \; SY \vee x_i \; \overline{SY}. \tag{12}$$

From this equation it is evident that input circuit can be constructed by using standard logical elements that realise Exclusive Or function.

4. Construction of excitation circuit. For convenient fault detection according to Eq. 8 and 9 it is necessary to complement set of states by new states $s_1^*, s_2^*, \ldots, s_m^*$.

$$s_i^* = \overline{s}_i, \tag{13}$$

where $i = 1, 2, \ldots, m$.

The state assignment of excitation circuit of normal sequential machine is shown in Table 2, where state s_{ij} belongs to set of states S. The number of different states s_{ij} is m.

Table 2. State assignment

s	a			
	a_1	a_2		a_r
s_1	s_{11}	s_{12}	...	s_{1r}
s_2	s_{21}	s_{22}	...	s_{2r}
...	...	...	...	...
s_m	s_{m1}	s_{m2}	...	s_{mr}

For convenient fault detection Table 2 must be complemented by states s^* according to Eq. 9 and condition 13, as shown in Table 3. From this table we can obtain completely definite state transition function δ that is used for transition to state s and transient state s^*.

Table 3. States and complement states assignment

s	a				a'			
	a_1	a_2		a_r	$\overline{a}_1$	$\overline{a}_2$		$\overline{a}_r$
s_1	s_{11}	s_{12}	...	s_{1r}	$\overline{s}_1$	$\overline{s}_1$	...	$\overline{s}_1$
s_2	s_{21}	s_{22}	...	s_{2r}	$\overline{s}_2$	$\overline{s}_2$	...	$\overline{s}_2$
...	...	...	...	...	...	...	...	...
s_m	s_{m1}	s_{m2}	...	s_{mr}	$\overline{s}_m$	$\overline{s}_m$	...	$\overline{s}_m$

Let us examine the behavior of sequential machine under failure condition that occure in the input circuit. If output of faulty element is stuck at one or zero it is evident that output of input circuit will be stuck at one or zero. This means that some input variables can not be changed in accordance with (11) and the error signal will be generated, because next state s^* will not satisfy condition (13).

The same result will be obtained if such a failure will occur in the excitation circuit or in memory element. In both cases the condition (13) will not be satisfied and the error signal will be generated.

In order to detect failures if erroneous state occur in the cause of memory malfunction, it is desirable that S and S_r are disjoint

$$S \cap S_r = \varnothing. \tag{14}$$

Equation (14) and the definition of S_r require that an erroneous state should go over to a state that must belong to S_r when an arbitrary input is applied. Now let us consider state transition from an erroneous state s_r at input a. When no fault exists the next state s_r^* is, of course, determined by δ (9).

$$\delta(a, s_r) = s_r^*. \tag{15}$$

If $s_r \in S$ the state transition satisfies condition (13) and failure can not be detected. If s_r did not belongs to S, but $s_r \in S_r$ the state transition from erroneous state results to an erroneous state and condition (13) will not be satisfied. Logic gates in the E circuit and memory elements (Fig. 2) are not used in common for many state variables. According to this proper construction of the E circuit and the assumption of occurrence of single fault, the Hamming distance $d\{s, s_r\}$ between state assignments of s and s_r is one. Therefore, in order to make S and S_r disjoint, we must assign such a code to each normal state that satisfies the following distance condition:

$$\forall s_1, s_2 \in S, \quad d\{s_1, s_2\} \geqslant 2. \tag{16}$$

5. Illustrative examples. In order to illustrate the above method, let us consider a sequential machine which state transition function is specified by Table 4 and 5.

Table 4. State assignment

s	a	
	a_1	a_2
1	1	3
2	1	4
3	4	2
4	3	1

Table 5. State assignment

s	a	
	0	1
100	100	111
010	100	001
111	001	010
001	111	100

Sequential machine (Fig. 2) has one input represented by input variable x_1 and four states represented by three state variables y_1, y_2, y_3. According to (12) the set of input alphabets $A\{0,1\}$ will be transformed in to the set of input alphabets $A'\{00,10,11,01\}$, as shown in Table 6. Assigning a code to each additional state, which satisfy condition (13) we obtain the following logical functions of exitation circuits.

$$y_1 = a_1(y_1\bar{y}_2\bar{y}_3 \vee \bar{y}_1y_2\bar{y}_3 \vee \bar{y}_1\bar{y}_2y_3) \vee a_2(\bar{y}_1\bar{y}_2y_3 \vee y_1\bar{y}_2\bar{y}_3) \vee (\bar{a}_1 \vee \bar{a}_2)(\bar{y}_1y_2\bar{y}_3 \vee \bar{y}_1\bar{y}_2y_3), \tag{16a}$$

$$y_2 = a_1\bar{y}_1\bar{y}_2y_3 \vee a_2(y_1\bar{y}_2\bar{y}_3 \vee y_1y_2y_3) \vee (\bar{a}_1 \vee \bar{a}_2)(y_1\bar{y}_2\bar{y}_3 \vee \bar{y}_1\bar{y}_2y_3), \tag{16b}$$

$$y_3 = a_1(y_1y_2y_3 \vee \bar{y}_1\bar{y}_2y_3) \vee a_2(y_1\bar{y}_2\bar{y}_3 \vee y_1\bar{y}_2\bar{y}_3) \vee (\bar{a}_1 \vee \bar{a}_2)(y_1\bar{y}_2\bar{y}_3 \vee \bar{y}_1y_2\bar{y}_3). \tag{16c}$$

Table 6. States and complement states assignment

s	a'			
	00	10	11	01
100	100	111	011	011
010	100	001	101	101
111	001	010	000	000
001	111	100	110	110

6. Conclusion. A new method of realization of fail-safe sinchronous sequential machines has been presented. A feature of

this method is that input variables inversion in time between two clock signal is used. New state transition into transient state is determined by inverted input variables. This state is used for fault detection.

REFERENCES

Gossel, M., and E.S. Sogomonyan (1992). Self-testing and self-checking comparison scheme (Comparator). *Avtomatika i Telemexanika*, **10**, 135-141 (in Russian).

Sapoznikov, V.V., and Vl.V. Sapoznikov (1984). *Diskrete Automatona with Fault-Checking.* Energoatomizdat, Leningrad. 109pp. (in Russian).

Sogomonyan, E.S., and E.V. Slabakov (1989). *Self-Checking Devices and Fault-Tolerant System.* Radio i sviaz, Moscow. 207pp. (in Russian).

Thoma, Y., Ohyama Y.and Sakai R. (1971). Realization of fail-safe sequential machines by using a k-out-of-n-Code. *IEEE Trans. Comp.*, **20**, 1270-1275.

Received November 1993

R. Andruškevičius received the Degree of Candidate of Technical Sciences from the Kaunas Polytechnic Institute, Kaunas, Lithuania, 1975. He heads the Department of Automation of ThermoPhysics Experimental Research. His research interests include fault-tolerant systems.