NASA TECH BRIEF

Lyndon B. Johnson Space Center

NASA Tech Briefs announce new technology derived from the U.S. space program. They are issued to encourage commercial application. Tech Briefs are available on a subscription basis from the National Technical Information Service, Springfield, Virginia 22151. Requests for individual copies or questions relating to the Tech Brief program may be directed to the Technology Utilization Office, NASA, Code KT, Washington, D.C. 20546.

A Fault-Tolerant Clock

The problem:

In many applications, computers must be fault tolerant. They must continue to operate correctly even though one or more of the components have failed. Such computers must have, among other things, a fault tolerant clock to insure that all operations occur in the proper sequence.

The solution:

An electronic clock has been designed to be insensitive to the occurrence of faults. It is a substantial advance over any known electronic clock.

How it's done:

Let A_1, A_2, and A_3 be three independent determinations of the same quantity; then the value of a simple majority voter function

$$A = (A_1 A_2 + A_1 A_3 + A_2 A_3)$$

will change if only one A_i, say A_3, fails as long as $A_1 = A_2$. But, without accurate timing it is possible for A_3 to fail and for A_1 and A_2 to be out of step so that $A_1 \neq A_2$. In this case $A = A_3$, and the failure is propa-

gated; since the clock is itself the timing mechanism, the majority voter function will not insure fault tolerance.

Instead, quorum functions are used. The quorum function Q_i^n is defined to be logical "1" if at least i of the variables A_1, A_2 ,..., A_n are "1", and logical "0" otherwise. For example:

$Q_1^4 = A_1 + A_2 + A_3 + A_4 = $ "1" when at least one $A_i = $ "1"

$Q_2^4 = A_1 A_2 + A_1 A_3 + A_1 A_4 + A_2 A_3 + A_2 A_4 + A_3 A_4 = $ "1" when at least two A_i's = "1"

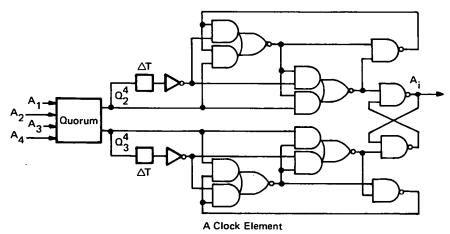$Q_3^4 = A_1 A_2 A_3 + A_1 A_2 A_4 + A_1 A_3 A_4 + A_2 A_3 A_4 = $ "1" when at least three A_i's = "1"

$Q_4^4 = A_1 A_2 A_3 A_4 = $ "1" when all four A_i's = "1".

A change in the value of Q is represented by $Q_i^n +$ for a "0" to "1" change and by $Q_i^n -$ for a "1" to "0" change.

A general fault-tolerant clock can be understood from the design of a single-fault-tolerant clock with i=1,2,3, or 4 (see figure). The first element generates Q_2^4 and Q_3^4. Each A_i is the output of one of four R-S flip-flops. The events

$$Q_2^4+, \quad Q_2^4-, \quad Q_3^4+, \text{ or } Q_3^4-$$

A Clock Element

may occur. The signals from these events will drive the differentiators which set and reset each flip-flop corresponding to an A_i in the following manner:

Q_2^4+ will set the A_i to logical "1".

Q_2^4- will be delayed by ΔT and then set the A_i to "1".

Q_3^4- will reset the A_i to the logical "0".

Q_3^4+ will be delayed by ΔT and then reset the A_i to "0".

The normal mode of operation is as follows:

When two of the four A_i's become 1, the event Q_2^4+ occurs.

The event Q_2^4+ sets the remaining A_i's to "1".

The setting of the third and fourth A_i to "1" causes Q_3^4+ to occur.

The signal from Q_3^4- is delayed ΔT and then resets A_i to "0".

When any two A_i's become "0", Q_3^4- occurs and resets the remaining two A_i's to "0".

The resetting of the third A_i to "0" causes Q_2^4- to occur.

The signal from Q_2^4- is delayed ΔT and sets the A_i to "1".

When two of the four A_i's become "1", the event Q_2^4+ occurs.

With a single fault one A_i is replaced with an indeterminante quantity. The behavior of the four-variable quorum function may, in this case, be described in terms of three-variable functions of the nonfailed elements.

For instance, the event Q_2^4+ will occur at Q_1^3+ (if the indeterminante A_i happens to be "1") or at Q_2^3+ (if the indeterminante A_i happens to be "0"). In this way, four- and three-group functions are related as below:

Q_2^4+ will occur between Q_1^3+ and Q_2^3+;

Q_3^4+ will occur between Q_2^3+ and Q_3^3+;

Q_3^4- will occur between Q_3^3- and Q_2^3-; and

Q_2^4- will occur between Q_2^3- and Q_1^3-.

A cycle of events occurs as in the unfailed case. Since however, only three of the A_i's are known, the cycle is defined in terms of the three-group functions.

The sequence of events is unchanged in the failed mode because the interval in which Q_2^4 is indeterminate does not overlap the interval in which Q_3^4 is indeterminate. Because the sequence is unchanged, the frequency is unchanged.

A general fault-tolerant clock, which will tolerate r faults, can be made by using functions Q_x^n and Q_y^n where x and y are chosen as follows:

$$n \geq 3r + 1, \, x \geq r + 1, \, \text{and} \, y \geq 2r + 1.$$

The modes of operation are essentially the same as in the single-fault-tolerant clock. A system element can generate a valid clock signal by a simple majority vote among any $2r + 1$ of the $3r + 1$ A_i's.

Note:

Requests for further information may be directed to:
Technology Utilization Officer
Lyndon B. Johnson Space Center
Code JM7
Houston, Texas 77058
Reference: TSP73-10218

Patent status:

This invention is owned by NASA, and a patent application has been filed. Inquiries concerning nonexclusive or exclusive license for its commercial development should be directed to:
Patent Counsel
Lyndon B. Johnson Space Center
Code AM
Houston, Texas 77058
Source: W. P. Daley and J. F. McKenna, Jr., of
Massachusetts Institute of Technology
under contract to
Johnson Space Center
(MSC-12531)