1 Analysis for a restarting method

Definition. *A state graph consists of $<V, S, T>$ where V is the ordered set of signals where $1 \leq k \leq n$ indexes into V and gives the signal v_k. S is the set of all states in the state graph and s(k) denotes the (binary) value of the state at signal v_k. T is the set of all transitions in the state graph $T \subseteq SXS$ where (s_i, s_j) denotes a transition from the state s_i to s_j with a single transition in some variable.*

Definition. *Two state graphs G_A and G_B are similar if there exists a one to one mapping function f: $V_A \rightarrow V_B$. So that for all $s \in S_A$, $\exists$ $s' \in S_B$ such that for all i in n_A, $s(i) = s'(f(i))$, for simplicity we write $s \rightarrow s'$. And for all pairs of $(s,t) \in T_A$, $\exists (s', t') \in T_B$ and also for all pairs of $(s', t') \in T_B$, $\exists (s,t) \in T_A$ with $s \rightarrow s'$, $t \rightarrow t'$.*

Claim. *Given some graph G_A if we insert a signal that is a constant value (ie. 0 for all states) to form G_B then G_A is similar to G_B*

Proof. If we add the new signal to the beginning of the set of signals, $V_B = v_0 \cup V_A$ then the function f is just f(i)=i+1 for $1 \leq i \leq n$. And for all $s \in S_A$, we have $s \rightarrow s'$ where $s' \in S_B$. Also the transitions in G_B occur between (s',t') if and only if there is a transition (s,t) in G_A with $s \rightarrow s'$, $t \rightarrow t'$. Thus G_A is similar to G_B □

Starting with a circuit that is a valid implementation of state graph G, we modify the circuit as follows, we add a $Restart_A$ signal, for every input A to the set or reset logic of some gate, we replace with A or $Restart_A$. The $Restart_A$ gate is implemented with a $0 \rightarrow 1$ restartable generalized C-element with no set signal, and a reset logic that is a copy of the reset logic of A. If we allow a 0 signal being reset as staying in the 0 state then if we start at some state s0 from the original state graph G and assign $Restart_A$ an initial value of 0 then the new state graph G' we build from the new circuit starting at state $<0, s0>$, the $Restart_A$ signal is a constant 0. For all states $s \in S$ and corresponding state in the new state graph s'=$<0, s>$, then for every t such that $(s,t) \in T$, then $(s', t') \in T'$ where t'=$<0, t>$ and since adding the new logic of A or $Restart_A$ while $Restart_A$ is a constant 0 does not add new transitions to the new state graph that does not exist in G, this is an if and only if relation for all transitions starting from state s and s'. Then by induction since there is an initial state s0 in G and $<0, s0>$ in G', the rest of the states and transitions remain the same as in the original state graph G with only an addition of the constant $Restart_A = 0$ signal. By our earlier claim, this new state graph G' is similar to the original G.

In the case of a stuck at fault in signal A, so that the $0 \rightarrow 1$ transition does not happen even when A is being set, then when enough time elapses the $Restart_A$ signal will go high. We build the resulting state graph from the circuit starting from this new state. Since the new logic is A or $Restart_A$, with A now a constant 0 signal, and $Restart_A$ has the same reset logic as A, use the same argument as in the above paragraph but switch the signals so that we view $Restart_A$ as A and A as $Restart_A$, then the new state graph G'' that we build again has all of the states and trasitions as the original state graph G. There is a slight difference in the mapping function f where f(1)= 1 (assuming A is the first signal in V) and f(i)=i+1 for $1 < i \leq n$, then again it is inserting a constant signal to the original graph and thus G'' is similar to G.

Thus this construction of a restartable circuit provides the same sequences of states as in the original circuit during normal operation as well as fault mode operation. If we use the values of signals other than A, we cannot distinguish between the two circuits as it runs.