Application Note

Synplicity

Designing Safe Verilog State Machines with Synplify

Introduction

One of the strengths of Synplify is the Finite State Machine compiler. This is a powerful feature that not only has the ability to automatically detect state machines in the source code, and implement them with either sequential, gray, or one-hot encoding. But also perform a reachability analysis to determine all the states that could possibly be reached, and optimize away all states and transition logic that can not be reached. Thus, producing a highly optimal final implementation of the state machine.

In the vast majority of situations this behavior is desirable. There are occasions, however, when the removal of unreachable states is not acceptable. One clear example is when the final circuit will be subjected to a harsh operating environment, such as space applications where there may be high levels of radiation. In the presence of high levels of radiation, storage elements (flip-flops) have been known to change state due to alpha particle hits. If a single bit of a state register where to suddenly change value, the resulting state may be invalid. If the invalid states and transition logic had been removed, the circuit may never get back to a valid state.

By default Synplify will create state machines that are optimized for speed and area. This application note will use an example state machine design to show the default small & fast implementation. It will also demonstrate how to trade-off some of that speed & area to produce highly reliable state machines using Synplify.

Example 1:
Assume that the transition diagram in figure 1 is to be implemented as a one-hot FSM:

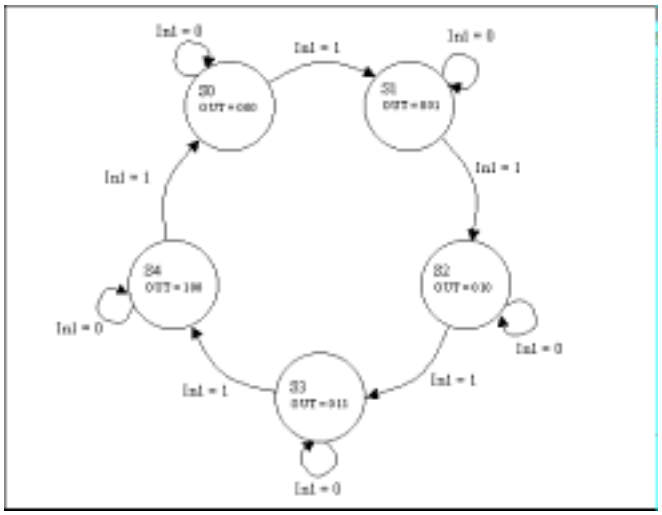

Fig. 1

One possible RTL implementation would be:

```
module FSM1 (clk, in1, rst, out1);
input        clk, rst, in1;
output [2:0] out1;

`define s0 3'b000
`define s1 3'b001
`define s2 3'b010
`define s3 3'b011
`define s4 3'b100

reg [2:0] out1;
reg [2:0] state /* synthesis syn_encoding = "onehot" */;
reg [2:0] next_state;

always @(posedge clk or posedge rst)
    if (rst) state <= `s0;
    else     state <= next_state;

always @(state or in1)
   case (state)
       `s0  : begin
          out1 <= 3'b000;
          if (in1) next_state <= `s1;
          else     next_state <= `s0;
       end
       `s1  : begin
          out1 <= 3'b001;
          if (in1) next_state <= `s2;
          else     next_state <= `s1;
       end
       `s2  : begin
          out1 <= 3'b010;
          if (in1) next_state <= `s3;
          else     next_state <= `s2;
       end
       `s3  : begin
          out1 <= 3'b011;
          if (in1) next_state <= `s4;
          else     next_state <= `s3;
       end
       `s4  : begin
          out1 <= 3'b100;
          if (in1) next_state <= `s0;
          else     next_state <= `s4;
       end
       default : begin
          out1 <= 3'b000;
          next_state <= `s3;
```



```
        end
    endcase

endmodule
```

Note:

1. The “syn_encoding” attribute is used to specify that this state machine should be encoded as one-hot.
2. There are 5 defined states (S0, S1, S2, S3, and S4), all of which are reachable.
3. Since the encoding style is one-hot, there are 27 undefined (and unreachable) states that are covered by the “default” branch of the case statement.
4. The state register resets to state S0.
5. The “default” case specifies a transition to state S3. Keep in mind that this circuit will never reach the “default” branch without some external influence such as an alpha particle hit or a physical defect in the target part.
6. Regarding coding style, parameter statements could have been used instead of define statements.

7. The state values defined in the source code describe a sequential encoding, however, the syn_encoding attribute directs the FSM compiler to implement this design as a one-hot state machine. The final circuit will have the state encodings: S0 = 00001, S1 = 00010, S2 = 00100, S3 = 01000, S4 = 10000.

The material covered in this application note applies to all supported encoding styles, one-hot, sequential, and gray

Default Implementation:

If Synplify is used to synthesize this design as is, the result is an optimized state machine with the transition logic for unreachable states removed. The final implementation is basically a shift register. Where the state register resets to the 00001 state (S0), and the output of state bit 4 is the input to state bit 3, the output of state bit 3 is the input to state bit 2, and so on. This is shown in figure 2 using the Technology View in HDL Analyst.

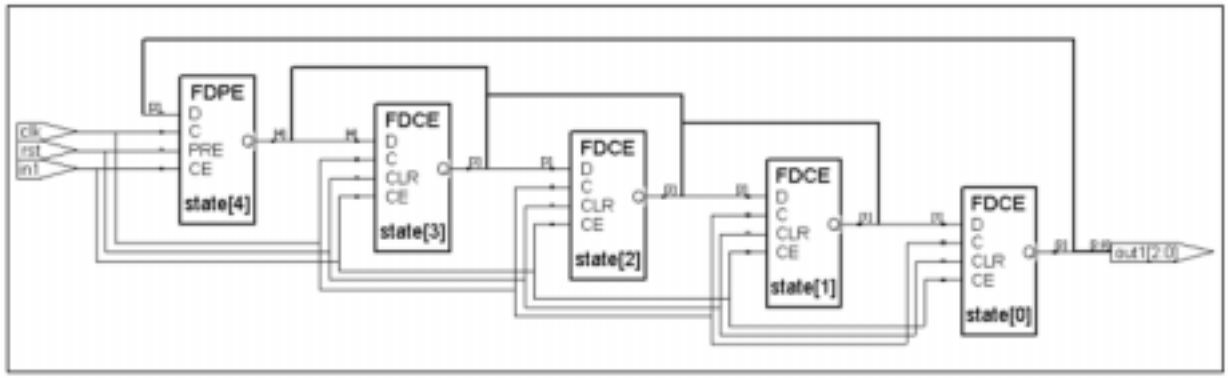

Fig 2

This is a very optimal result for both timing and area. In a normal operating environment this circuit will function perfectly. Suppose, however, that this circuit is to be placed in a hostile operating environment where a register could spontaneously change value due to an alpha particle hit, or some other reason. What would happen if this state machine ended up in the 00000 state? The next transition would shift all the state bits resulting in the state 00000. The result being that this FSM would effectively be stuck in the 00000 state.

"Safe" Implementation:

To handle this type of problem, the FSM compiler in Synplify has a special encoding directive, "safe", that will add logic such that if the state machine should ever reach an invalid state, it will be forced to the reset state. This behavior has the advantage of avoiding any possible "hang" conditions, where the state machine is unable to get back to a valid state, while having minimal impact on the timing of the circuit.

To enable this feature simply change the value of the syn_encoding attribute from:

```
reg [2:0] state /* synthesis syn_encoding = "onehot" */;
```

to:

```
reg [2:0] state /* synthesis syn_encoding = "safe,onehot" */;
```

Note:

The syn_encoding attribute can also be applied in the SCOPE graphical constraint editor or directly in the constraint (.sdc) file. Using the following syntax:

```
define_attribute {state[*]} syn_encoding {safe,onehot}
```

Synthesizing this design will result in a circuit that has the state transition logic implemented exactly as shown in figure 2 above, with the addition of the circuitry in figure 3 added to the reset logic.

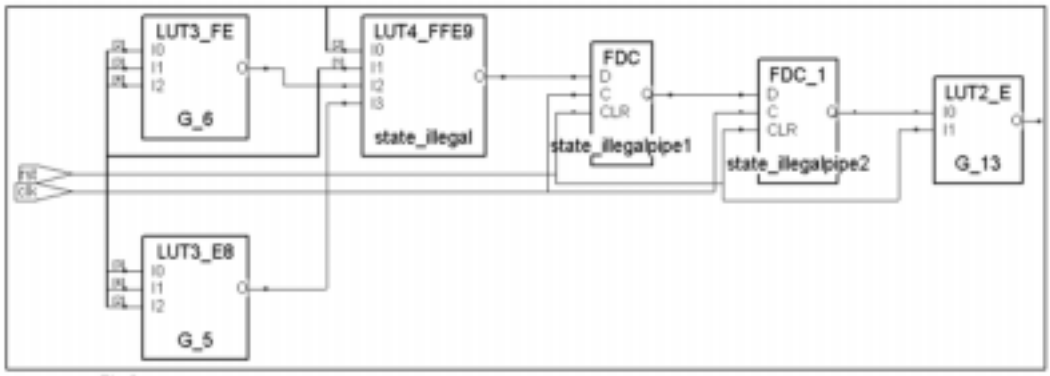

Fig 3

If an invalid state is detected, the state_illegalpipe1 register is set on the next rising clock edge. On the falling edge of the clock, the state_illegalpipe2 register is set. Instance G_13 ORs the original reset signal “rst” with the new recovery logic. The output of instance G_13 drives the clear/preset pins of the state bits, forcing the circuit to the (valid) reset state. Once this valid state is reached, the next rising edge of the clock will clear the state_illegalpipe1 register, the next falling edge of the clock will clear the state_illegalpipe2 register and normal operation will begin. Note that the result of this recovery logic, the output of state_illegalpipe2, is registered on the falling edge of the clock to prevent any harzardous conditions that could result from removing the reset signal too close to the active clock edge of the state registers.

The recovery logic discussed above is generated for the example circuit which happens to have an asynchronous reset. If the circuit had a synchronous reset instead, the logic implemented would be slightly different. Suppose the register definition was changed from:

```
       always @(posedge clk or posedge rst)
           if (rst) state <= `s0;
           else    state <= next_state;
to:
       always @(posedge clk)
              if (rst)      state <= `s0;
              else   state <= next_state;
```

For this synchronous reset implementation, the circuitry in figure 4 would be added to the reset logic:

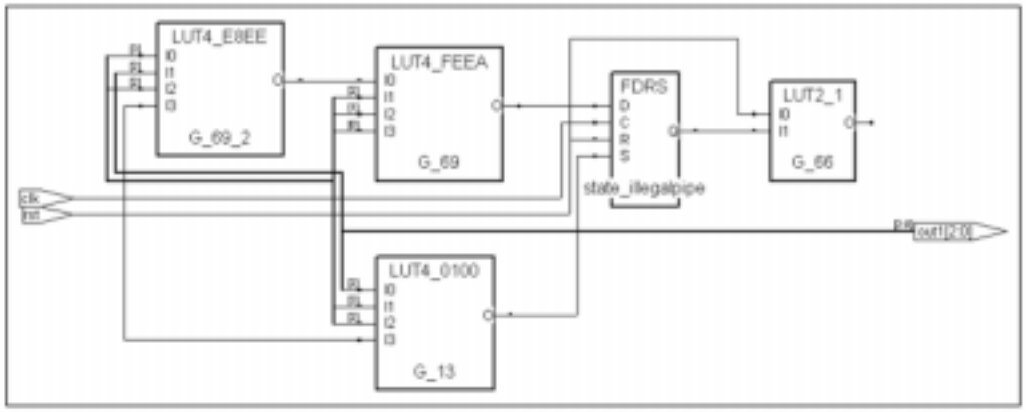

Fig 4

The recovery logic discussed above is generated for the example circuit which happens to have an asynchronous reset. If the circuit had a synchronous reset instead, the logic implemented would be slightly different. Suppose the register definition was changed from:

```
       always @(posedge clk or posedge rst)
           if (rst) state <= `s0;
           else    state <= next_state;
to:
       always @(posedge clk)
              if (rst)      state <= `s0;
              else   state <= next_state;
```

If an invalid state is detected, the state_illegalpipe register is set on the next rising clock edge. Instance G_66 ORs the original reset signal “rst” with the new recovery logic. On the next positive clock edge, the state register will switch to the (valid) reset state. Once this valid state is reached, the next rising edge of the clock will clear the state_illegalpipe register, and normal operation will begin.

In both the asynchronous and synchronous reset case, if the circuit should ever reach an invalid state (state 00000 for example), the recovery logic will be activated reseting the state register back to the 00001 state (S0). Once the FSM is back to the valid state of 00001 (S0), normal operation of the state machine can resume. Notice that upon entering an invalid state this circuit will recover to the 00001 state (S0) not the 01000 state (S3) as described in the “default” branch of the case statement.

This implementation eliminates the possibility of the state machine getting “stuck” in an invalid state and not returning to a valid state. This problem is handled with very minimal impact on the timing of the circuit. However, as pointed out above, the transition out of an invalid state is not implemented exactly as described in the “default” branch of the source code. This deviation from the defined “default” branch behavior only occurs for

invalid states. If the “default” case contained any valid state transitions they would be implemented as described in the source code.

“Exact” Implementation:

It is possible to get an implementation of the circuit that fully implements the “default” branch if it is necessary to do so. This requires disabling the reachability analysis of the state machine, which is done by turning off the FSM compiler, and explicitly defining the desired state encodings. This can have a significant affect on the area and timing of the circuit.

To get a full implementation of the “default” case change the state register description from:

```
    `define s0 3'b000
    `define s1 3'b001
    `define s2 3'b010
    `define s3 3'b011
    `define s4 3'b100

    reg [2:0] out1;
    reg [2:0] state /* synthesis syn_encoding = "onehot" */;
    reg [2:0] next_state;
to:
    `define s0 5'b00001
    `define s1 5'b00010
    `define s2 5'b00100
    `define s3 5'b01000
    `define s4 5'b10000

    reg [4:0] state /* synthesis syn_preserve=1 */;
    reg [4:0] next_state;
```

Note:

1. The state register is defined as 5 bits instead of 3 bits, and the state encodings have been explicitly defined as one-hot. This is done in order to make comparisons to the circuits in the previous sections which were implemented as one-hot. It is not a requirement for the encoding to be changed to one-hot in order to get a full implementation of the “default” case, any encoding will work fine.
2. A syn_preserve attribute is applied to the state register to disable the FSM compiler.
3. The syn_encoding attribute is no longer needed because the FSM compiler is disabled.
4. The rest of the code remains unchanged.

Figure 5 uses the RTL view of HDL Analyst to show that the “default” case is fully implemented.

The instances next_state14, next_state13, next_state12, next_state11, and next_state10 decode the current state (S4, S3, S2, S1, S0 respectively). The instances un13, un14, and un20 implement the next state logic for state S0 (bit 0 of the state register). The function is ((~In1 & S0) | (In1 & S4)). The function for state bits 1, 2, and 4 are very similar. Bit 3, however, has an extra term generated by instance un16. This term checks if the FSM is currently in a valid state. If so, the function ((~In1 & S3) | (In1 & S2)) is used. If not, bit 3 is forced high making the next state 01000 (S3) as described in the "default" branch of the original source code.

Summary:

To summarize, Synplify contains a powerful FSM compiler which by default will produce state machine implementations that are highly optimial in regards to area and timing. If recovery from an invalid state is important the "safe" feature can be used to force the state machine to the reset state if an invalid state is reached, with minimal impact on timing and area of the circuit. This implementation of transitioning out of an invalid state may differ from what is explicitly described in the source code. For most designs this is an acceptable deviation, since these transitions are by definition not valid. If these invalid state transitions must be handled exactly as described by the source code, the FSM compiler can be disabled. However, this may result in a substantial impact on timing and area.

To quantify the impact on timing and area, the three implementations of this state machine were synthesized targeting an Altera Flex10k part and a Xilinx Virtex part. The estimated timing and area results reported by Synplify are displayed in table 1 below.

Target	Altera Flex10k – EPF10K10A-1			Xilinx Virtex – XCV50-4		
	ns	LCs	Regs	ns	LUTs	Regs
Default	4.4	8	5	5.1	2	5
Safe	6.7	14	7	7.2	6	7
Full Default	11.4	18	5	12.7	17	5

Tab 1