Detecting Malicious Behavior for the Sensors and Actuators Embedded in Medical Devices: A Hardware Approach

Razan Abdulhammed, Miad Faezipour and Khaled Elleithy
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT
rabdulha@my.bridgeport.edu, mfaezipo@bridgeport.edu, elleithy@bridgeport.edu

Abstract

The goal of this study is to investigate a behavior-rule based technique for detecting the malicious behavior of the sensors and actuators embedded in medical devices such as Vital Sign Monitor (VSM), Patient Analgesic Control (PCA), Cardiac Device (CD), and Continuous Glaucous Monitor (CGM). First, a set of behavior rules for both malicious and normal behaviors are proposed. Second, a transformation methodology has been used to transfer the proposed set of behavior rules into a state machine. Finally, a Finite State Machine (FSM) has been built using Altera ModelSim and Quartus II toolset. The simulation and synthesis results using a Field Programmable Gate Array (FPGA) demonstrate that our FSM hardware model can effectively identify malicious behavior from normal behavior.

***Keywords*: *FSM*; *Behavior rule*; *PCA*; *CD*; *VSM*; *CGM*; *FPGA*.**

Introduction

The proposed study uses sensors as well as actuator readings and settings to build a Behavior Monitoring Tool (BMT) that uses the notion of behavior rules to specify acceptable behaviors of sensors and actuators embedded in certain medical devices such as VSM, PCA, CD, and CGM. Tables 1 and 2 show a sample of both normal behavior status rules and malicious behavior status rules [1],[2], respectively.

TABLE 1. NORMAL BEHAVIOR STATUS RULES IN CONJUNCTION NORMAL FORM (CNF)

Description	Safe State	Trustee	Monitor
Pulse above threshold during analgesic request	(Analgesic Request = TRUE) ∧ (Pulse > Ts)	PCA	VSM
Pulse matches pacemaker frequency	Pulse = Pacemaker frequency	CD	VSM
Trustee blood pressure matches monitor	Trustee blood pressure = Monitor blood pressure	VSM	Peer VSM
Trustee Glucose matches monitor	Monitor Glucose = Trustee Glucose	CGM	Peer CGM

TABLE 2. MALICIOUS BEHAVIOR STATUS RULES IN CNF

Device	Malicious State	Device attributes
PCA	Analgesic Request Rate > T	Analgesic request
CD	(Mode =PACEMAKER) ∧ (| Pulse -Pacemaker Frequency |) > δ	CD mode ,pulse
VSM	| Monitor Oxygen Saturation - Trustee Oxygen Saturation | > δ	Oxygen Saturation
CGM	(Insulin Request = TRUE) ∧ (Pulse < T) ∧ (Glucose < T)	Insulin Request rate, pulse, Glucose

States in State Machine Terminology

Each device functions in different modes of operation, also known as states (see Figure 1). Table 3 shows different states of a system.

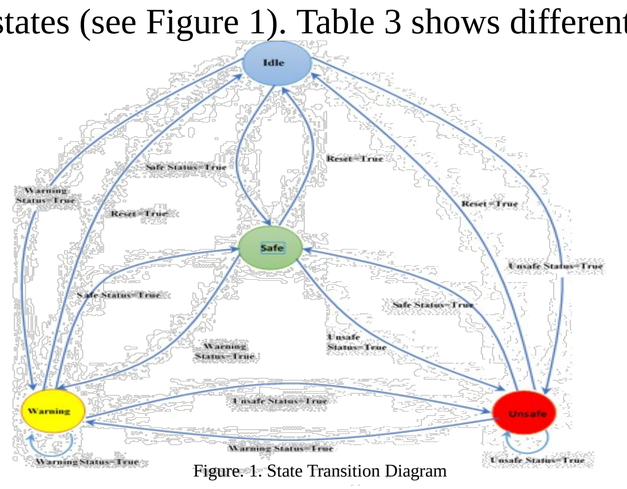

Figure. 1. State Transition Diagram

TABLE 3. DEVICE STATUS

Status	Cause	Output Alarm
Safe	The device is working correctly as specified by the behavior rules.	00
Unsafe	The device is seen to deviate from normal behavior specified by the behavior rules.	11
Warning	The values exceed the warning threshold for at least one behavior rule	10
Idle	Initial State of the system	01

Simulation and Synthesis

Using Altera ModelSim and Quartus II toolset, we implemented four Finite State Machines (FSM) for PCA, CD, VSM, and CGM, respectively. The resulting Register Transfer Level (RTL) views are shown in Figures 2, 3, 4 and 5, respectively. We ran a functional simulation within a range of different acceptable parameters of the state components. These ranges of values reflect the physiology and responses of patient treatment for each device. The waveform simulation results for PCA, CD, VSM, and CGM are shown in Figures 6, 7, 8, and 9, respectively. Furthermore, device utilization and power analysis summaries for the PCA and CD devices are shown in Tables 4, 5, 6 and 7, respectively.

1. PCA

An RTL circuit for the PCA device's FSM module is shown in Figure. 2.

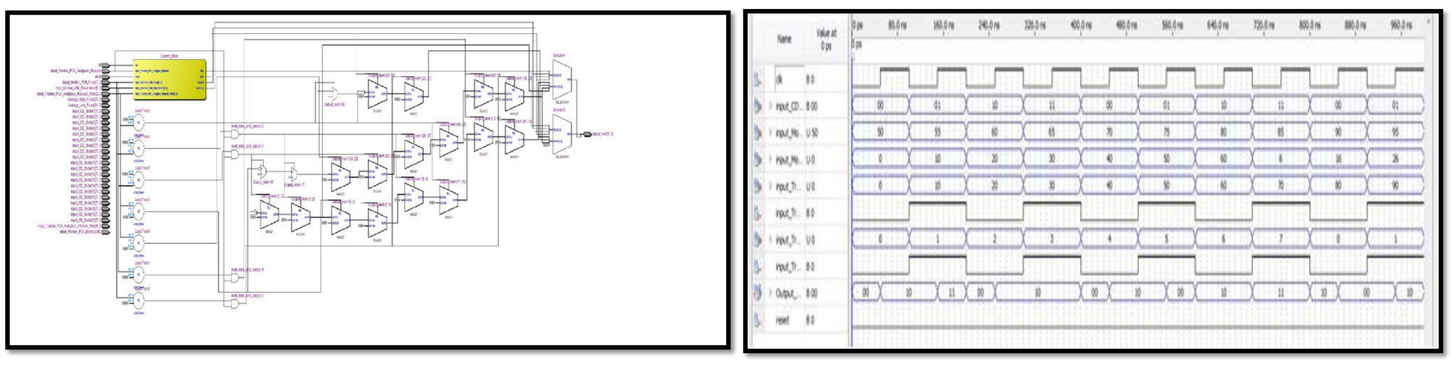

Figure 2. An RTL view of the PCA device's Behavior Specification Rules Tool (BSRT) along with the simulation waveforms

2. CD

An RTL circuit for the CD device's FSM module is shown in Figure 3.

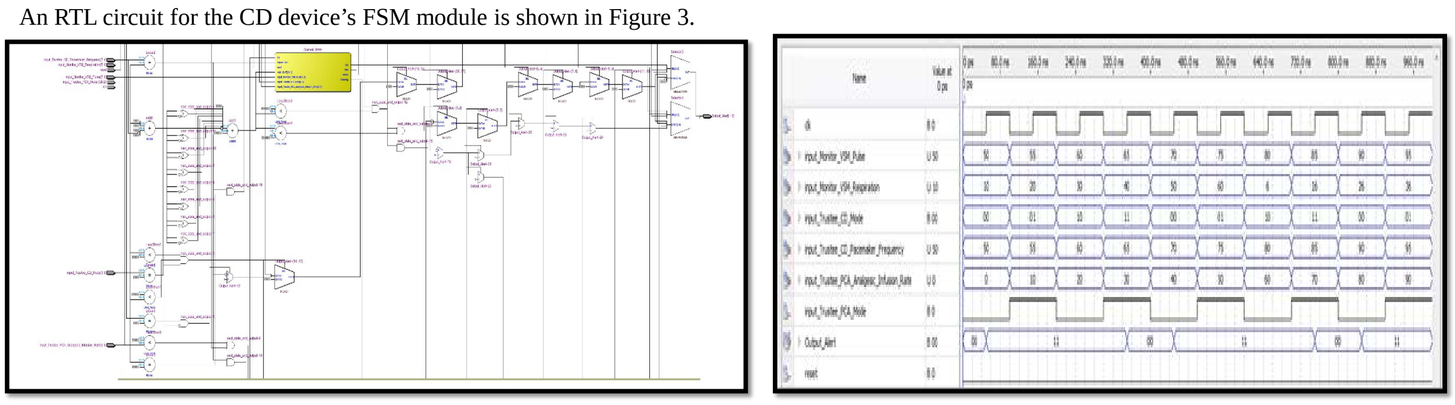

Figure 3. An RTL view for the CD device 's Behavior Specification Rules Tool along with the simulation waveforms

3. VSM

An RTL circuit for the VSM device's FSM module is shown in Figure 4.

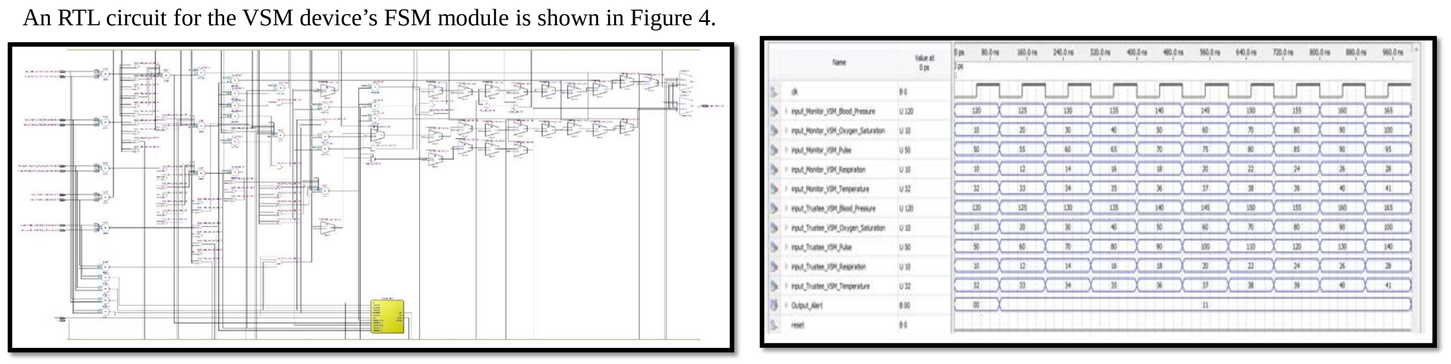

Figure 4. An RTL view for the VSM Behavior Specification Rules Tool along with the simulation waveforms

4. CGM

An RTL circuit for the CGM device's FSM module is shown in Figure 5.

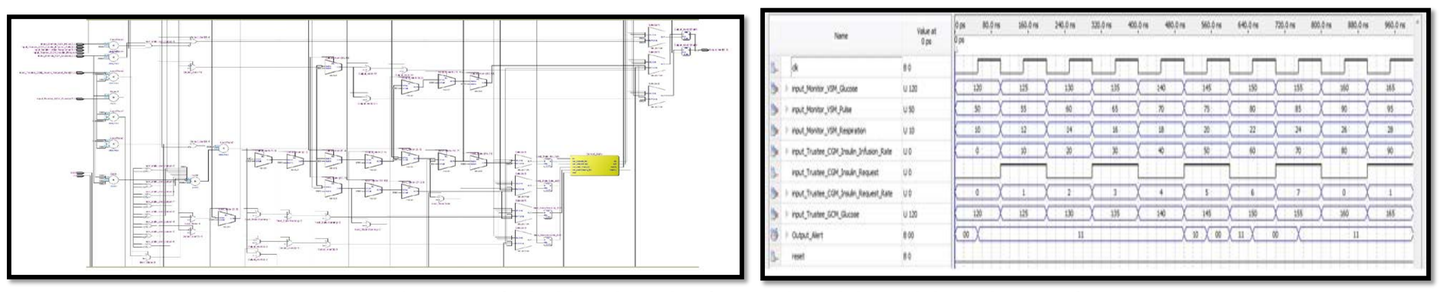

Figure 5. An RTL view for the CGM Behavior Specification Rules Tool along with the simulation waveforms

TABLE 4. UTILIZATION SUMMARY OF THE PCA BSRM TOOL

Attribute	Criteria
Family	Cyclone III
Device	EP3C120F780C7
Timing Models	Final
Total logic elements	57 / 119,088 (< 1 %)
Total combinational functions	57 / 119,088 (< 1 %)
Dedicated logic registers	4 / 119,088 (< 1 %)
Total registers	4
Total pins	32 / 532 (6 %)

TABLE 5. POWER ANALYSIS SUMMARY OF THE PCA BSRM TOOL

Attribute	Criteria
Family	Cyclone III
Device	EP3C120F780C7
Power Models	Final
Total Thermal Power Dissipation	120.48 mW
Core Dynamic Thermal Power Dissipation	1.64 mW
Core Static Thermal Power Dissipation	99.06 mW
I/O Thermal Power Dissipation	19.77 mW

TABLE 6. UTILIZATION SUMMARY OF THE CD BSRM TOOL

Attribute	Criteria
Family	Cyclone IV GX
Device	EP4CGX150DF31I7
Timing Models	Final
Total logic elements	54 / 149,760 (< 1 %)
Total combinational functions	54 / 149,760 (< 1 %)
Dedicated logic registers	4 / 149,760 (< 1 %)
Total registers	4
Total pins	36 / 508 (7 %)

TABLE 7. POWER ANALYSIS SUMMARY OF THE CD BSRM TOOL

Attribute	Criteria
Family	Cyclone IV GX
Device	EP4CGX150DF31I7
Power Models	Final
Total Thermal Power Dissipation	141.18 mW
Core Dynamic Thermal Power Dissipation	2.14 mW
Core Static Thermal Power Dissipation	118.71 mW
I/O Thermal Power Dissipation	20.33 mW

Conclusion

This study determined the effect of using a hardware approach to detect malicious behavior in sensors and actuators that are embedded in medical devices. The experimental results confirmed that the specification behavior rules can be utilized to build a hardware monitoring tool that can identify the expected normal behavior of a device and detect any deviation from its normal behavior. Furthermore, we showed through our analysis that our model is consistent with two dominant design requirements for next-generation high-end applications; lower power consumption and higher bandwidth. The reconfigurable nature of FPGA allows to modify and update the whole design according to the set of behavior rules, which outperform software based approaches that are difficult to update. In addition, hardware approaches are difficult to be hacked. One of the most significant findings to emerge from this study is that a hardware based specification rules approach can be used to identify malicious behavior.

References

[1] A. E. W. Johnson, T. J. Pollard, L. Shen, L.-w. H. Lehman, M. Feng, M. Ghassemi, et al., "MIMIC-III, a freely accessible critical care database," *Scientific Data*, *vol.* 3, p. 160035, 05/24/*online* 2016.
[2] D. Liu, M. Görges, and S. A. Jenkins, "University of Queensland vital signs dataset: Development of an accessible repository of anesthesia patient monitoring data for research," *Anesthesia & Analgesia*, *vol.* 114, *pp.* 584-589, 2012.

D-BEST Lab
Digital / Biomedical Embedded Systems & Technology Lab