ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ ДРЕБЕЗГА КОНТАКТОВ

Можейко Д. О., Иванюк А. А.
Кафедра электронных вычислительных машин, кафедра информатики,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: dimamozheiko13@gmail.com, ivaniuk@bsuir.by

В работе рассматривается вопрос генерации случайных чисел на основе дребезга контактов и их нормализации для достижения распределения близкого к равномерному. Предлагается схемотехническое решение для построения генератора случайных последовательностей на основе дребезга контактов. Прототипирование разработанного генератора проводилось на отладочных платах Digilent ZYBO Z7-10, цифровые схемы проектировались на языке VHDL для кристалла FPGA Xilinx Zynq-7000.

Введение

Дребезг контактов электромеханических коммутационных устройств неизбежное явление, наблюдаемое во время замыкания и размыкания контактов, что доказывалось в предыдущих исследованиях [1]. Причиной данного явления является кратковременное соударение и неконтролируемые отскоки контактов друг от друга, что приводит к нежелательным замыканиям и размыканиям электрических цепей.

Функционально движковые переключатели являются логическими переключателями, в то время как функционал нажатия кнопок более разнообразный: нажатие и удержание в течении заданного промежутка времени (инициализация/сброс), однократное нажатие и отпускание (настройка режима/навигация), многократное последовательное нажатие определенное число раз и различные другие комбинации.

Само явление дребезга носит случайный характер, обусловленный большим числом факторов: свойства материалов, из которых изготовлены коммутационные устройства и их контакты; геометрические размеры контактов и зазоров между ними; значения напряжения и силы тока в коммутируемых линиях; свойства окружающей среды (температура, влажность и т.п.), сила и скорость нажатия/переключения; время удержания и т.д. [2,3].

В работе рассматривается применение дребезга контактов кнопок, клавишных и движковых переключателей для генерации действительно случайных последовательностей.

I. Цифровая схема генератора случайных чисел

В ходе работы был спроектирован аппаратно-программный комплекс, при этом управление генератором и передачей данных от него осуществляется встроенным процессором ARM Cortex-A9, для которого была написана соответствующая программа. Весь аппаратно-программный комплекс был спроектирован при помощи САПР Xilinx Vivado/Vitis с применением языков VHDL и C.

Общая структура разработанного анализатора приведена на рисунке 1. Анализируемый сигнал от коммутатора подключается ко входу BTN и далее сэмплируется на триггере DFF на частоте FCLK=125 МГц [4]. Устройство управления CTRL_FSM определив первый значимый фронт сигнала от коммутатора запускает счетчик временного окна измерения TMW_CNT. Значение самого окна задается 32-разрядным значением на входной шине TMW. В этом окне измерений, в зависимости от логического состояния сигнала на линии BTN, работают линейные сдвиговые регистры с обратной связью LFSR. На LFSR_N, тактирующийся FCLK, поступает состояние сигнала BTN, учитывающееся при обратной связи, а на LFSR_B поступает логическое состояние BTN уже в качестве тактирующего сигнала. По окончании измерения блок CTRL_FSM прекращает управление счетом и вырабатывает сигнал готовности READY. После этого значения с двух LFSR складываются и передаются для дальнейшего анализа.

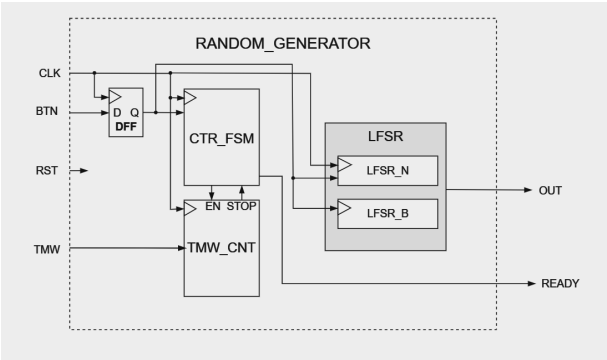

Рис. 1 – Структурная схема генератора

Использование представленной схемы, основанной на двух LFSR, вместо одного, обусловлено тем, что LFSR_B, тактирующийся сигналом BTN, будет срабатывать при каждом его фронте, тем самым реагировать на дребезг контактов коммутатора. LFSR_N, тактирующийся FCLK, будет сэмплировать сигнал BTN с частотой 125

Мгц и реагировать во время активного состояния коммутатора, такого как дребезг или его удержание в замкнутом состоянии. В итоге мы получаем схему с двумя LFSR, которая использует два фактора случайности, таких как количество фронтов сигнала и длительность активного состояния коммутатора.

II. Автоматизация и результат эксперимента

Для получения достаточной выборки было принято решение об автоматизации эксперимента. Была установлена система умного дома HAS(Home assistant service), налажена схема взаимодействия между HAS и устройством Fingerbot с помощью Zigbee радиомодуля. В ходе работы были рассмотрены различные типы коммутаторов и в качестве примеров выбраны: имеющаяся на плате кнопка ZYBO-Z7 (кнопка 1), а также внешний коммутатор DS-314 (кнопка 2), представленные на рисунке 2.

Рис. 2 – Рассмотренные в эксперименте коммутаторы и устройство Fingerbot

Было запрограммировано устройство Fingerbot с целью автоматизированного нажатия на кнопки в количестве 2500 раз. На рисунке 3 и 4 можно увидеть распределение величин в диапазоне от 0 до 255 для кнопки 1 и кнопки 2 соответственно.

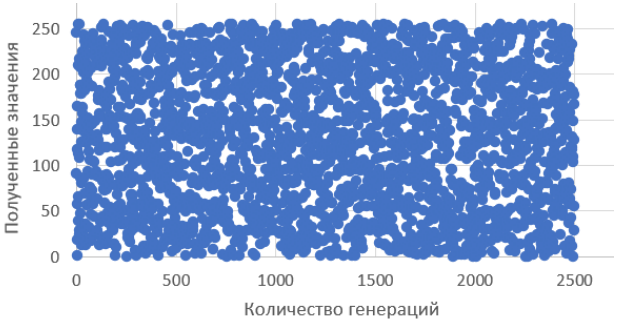

Рис. 3 – Распределение полученных значений для кнопки 1

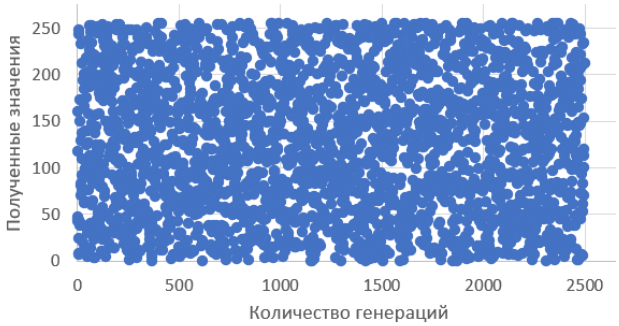

Рис. 4 – Распределение полученных значений для кнопки 2

III. Заключение

В работе рассмотрена генерация случайных чисел на основе дребезга контактов коммутаторов, используемых в цифровых устройствах различного назначения. В ходе работы была спроектирована цифровая система генератора случайных чисел на основе FPGA, позволяющая генерировать случайные последовательности по результатам нажатия/переключения коммутатора, учитывающая время дребезга, во время включения и выключения коммутатора, число импульсов дребезга, и время удержания коммутатора во включенном состоянии. В рамках проведенного эксперимента значение TMW_CNT было принято значению эквивалентному 1 секунде. Был автоматизирован процесс замыкания коммутаторов с помощью Home Assistant Service. А также собрана статистика по распределению значений диапазоне от 0 до 255.

Данная схема является универсальным методом получения случайных последовательностей, так она не требует больших аппаратурных затрат на реализацию и обладает хорошими статистическими свойствами вырабатываемых последовательностей. А также может быть использована как дополнительный источник энтропии в системах взаимодействующих с пользователем.

Список литературы

1. Можейко Д. О. Исследование дребезга контактов с целью генерирования случайных чисел / Д. О. Можейко, А. А. Иванюк // материалы 59-ой научной конференции аспирантов, магинстрантов и студентов БГУИР, 2023 года, Минск, Республика Беларусь / – Минск: БГУИР, 2023. – С. 41-43
2. Maxfield M. Switch Bounce and Debounce (Part 1): Switch Types [Electronic resource] / M. Maxfield. — Mode of access: `https://www.eeweb.com/switch-bounce-and-debounce-part-1-switch-types`. – Date of access: 03.05.2023.
3. Переключатели электромеханические для электрического и электронного оборудования. Общие технические условия: Межгосударственный стандарт ГОСТ IEC 61020-1-2016. Ч. 1. – Москва: Стандартинформ, 2017. – 50 с.
4. Zybo Z7: Zynq-7000 ARM/FPGA SoC Development Board [Electronic resource]. – Mode of access: `https://digilent.com/reference/programmable-logic/zybo-z7/start`. – Date of access: 15.05.2023.