УДК 621.391:519.21

АНАЛОГО-ЦИФРОВАЯ ИМИТАЦИОННАЯ МОДЕЛЬ ДЛЯ ИССЛЕДОВАНИЯ СЛУЧАЙНЫХ ПРОЦЕССОВ В СФЕРЕ БЕЗОПАСНОСТИ

Глухов О.А., Глухов Д.О., Смотрин К.А.

ФГБОУ ВПО «Поволжский государственный технологический университет», Йошкар-Ола,
e-mail: gluhovoa@volgatech.net, gluhovdo@volgatech.net, smotrinka@volgatech.net

Для анализа техносферной безопасности предлагается применить имитационное моделирование на основе аналого-цифровых электронных схем в программе Multisim-12. Предложенная модель объединяет в себе математическую модель марковских процессов и логические модели на основе деревьев событий. Структурная схема имитационной модели включает набор генераторов псевдослучайных последовательностей (ГСПП), счетчиков для оценки интенсивностей потоков событий и поле для логической схемы, моделирующей причинно-следственные связи сценариев развития угроз безопасности. Необходимое для моделирования количество некоррелированных друг с другом ГСПП реализуется совокупностью аналоговых линий задержки с нелинейными обратными связями. В качестве исходного источника потока случайных событий используется генератор теплового шума с пороговой обработкой. Отличительными преимуществами аналого-цифровой имитационной модели случайных процессов являются: асинхронный режим работы ГСПП, сжатие масштаба времени реальных случайных процессов в техносферной безопасности; простое и наглядное создание и изменение сложных логико-вероятностных структур, описывающих различные сценарии возникновения угроз безопасности; возможности экспорта экспериментальных данных в Labview, Mathcad, MathLab, Excel.

Ключевые слова: случайные процессы, безопасность, имитационное моделирование, аналого-цифровые схемы, псевдослучайные последовательности

ANALOG-DIGITAL IMITATION MODEL FOR RESEARCH STOCHASTIC PROCESSES IN VIEW OF SAFETY

Glukhov O.A., Glukhov D.O., Smotrin K.A.

Volga State University of Technology, Yoshkar-Ola,
e-mail: gluhovoa@volgatech.net, gluhovdo@volgatech.net, smotrinka@volgatech.net

This study invited to apply imitation modeling based on analog-digital circuitry in the program Multisim 12 for industrial safety analysis. The proposed model combines mathematical model of markovian processes and logical model based on fault tree analysis. Block diagram of the simulation model includes a set of pseudo-random sequence generators (PRSG), counters of the events flow density and a field for logic circuitry modeling causal relationships of security threats scenarios. The uncorrelated PRSGs, required for modeling, are implemented by a set of analog delay lines with non-linear feedbacks. As an initial pseudo-random sequence generator used the thermal noise source with threshold treatment. Distinctive advantages of analog-to-digital simulation models of stochastic processes are: asynchronous mode PRSG, real-time compression of stochastic processes in industrial safety; simple and intuitive creation and modification of complex logical structure describes various scenarios of safety threats; export possibilities of experimental data to Labview, Mathcad, MathLab, Excel.

Keywords: stochastic process, safety, imitation modeling, analog-digital circuitry, pseudo-random sequence

Исследование безопасности в техносфере тесно связано с изучением случайных процессов. Наиболее адекватным методом их описания является применение дискретных по значению и непрерывных во времени случайных процессов, моделирующих потоки событий, формирующих предпосылки и условия возникновения опасных проявлений техносферы. По аналогии с цифровой техникой при таком подходе момент перехода некоторой случайной функции времени от низкого уровня к высокому будет соответствовать моменту возникновения события, длительность этого состояния – длительности существования события, переход от высокого уровня к низкому – моменту его устранения.

В силу сложности вопросов безопасности в качестве инструмента исследования целесообразно применить имитационное моделирование. В общем случае имитационная модель – это логико-математическое описание объекта, которое может быть использовано для экспериментирования на компьютере в целях проектирования, анализа и оценки функционирования объекта. Такую модель можно «проиграть» во времени как для одного испытания, так и заданного их множества. При этом результаты будут определяться совокупностью процессов, имеющих случайный характер. По этим данным можно получить достаточно устойчивую статистику.

В анализе безопасности достаточно распространены методы, основанные

на применении графических структур типа деревьев событий (неисправностей и т.п.) [5]. Принципиально общим у этого направления является использование логических функций булевой алгебры (И, ИЛИ, И-НЕ, ИЛИ-НЕ исключающее ИЛИ), которые легко реализуются в программах схемотехнического моделирования.

Для имитационного моделирования авторы предлагают использовать аналого-цифровые электронные схемы, созданные в среде Multisim. Простота и наглядность процедуры изменения структуры дерева событий путем устранения или добавления логических элементов в программе «Multisim» обеспечивает эффективность предлагаемой структуры имитационной модели. Аналогично можно использовать и MicroCAP, Labview и другие программные продукты, предназначенные для схемотехнического моделирования.

В качестве модели источника случайных событий предлагается использовать генератор псевдослучайных чисел, отличительной особенностью которого является большая средняя частота появления сигналов – в зависимости от решаемой задачи её можно выбрать в диапазоне десятков-сотен мегагерц. В итоге реальные события, возникающие в интервалах тысяч – миллионов часов моделируются за доли секунды. На практике степень сжатия во времени определяется быстродействием компьютера и сложностью цифровой логической схемы, моделирующей структуры деревьев событий, описывающих различные сценарии возникновения угроз безопасности

Как отмечалось выше, в анализе безопасности широко применяются бинарные состояния типа «исправен-неисправен». Случайные процессы с «качественными» состояниями относятся к категории марковских процессов с непрерывным временем и дискретными состояниями. Понятие «состояние» является качественным и позволяет анализировать самые различные физические процессы. Неотъемлемой частью описания состояния дискретного случайного процесса является понятие «события», под которым будем понимать любой переход из одного состояния в другое. При анализе безопасности событиями являются не только факт возникновения угроз безопасности, но и факт их устранения, поэтому существенно важным является длительность нахождения в этом угрожающем состоянии. Таким образом, имеем два качественных состояния – «0» и «1», соответствующие соответственно состояниям «исправен» и «неисправен». Данный простейший случай двух состояний рассмотрен в [1], где приведены следующие формулы:

$$p_0(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\lambda+\mu} \cdot e^{-(\mu+\lambda)\cdot t};$$

$$p_1(t) = \frac{\lambda}{\lambda+\mu} \cdot \left(1 - e^{-(\mu+\lambda)\cdot t}\right),$$

где λ – интенсивность отказов (переход из состояния 0 в состояние 1); μ – интенсивность восстановления (переход из состояния 1 в состояние 0).

Рассматриваемый поток событий получаем после пороговой обработки случайного процесса, имитируемого генератором теплового шума, схема которого приведена на рис. 1.

Значение интенсивности потока событий задается уровнем порога их обнаружения и определяется количеством пересечений заданного порога за время наблюдения. Таким образом, в предлагаемой модели объединяются два подхода к исследованию случайных процессов в сфере безопасности: на основе теории марковских процессов и с применением логических моделей, описывающих причинно-следственные связи между событиями, формирующими угрозы безопасности.

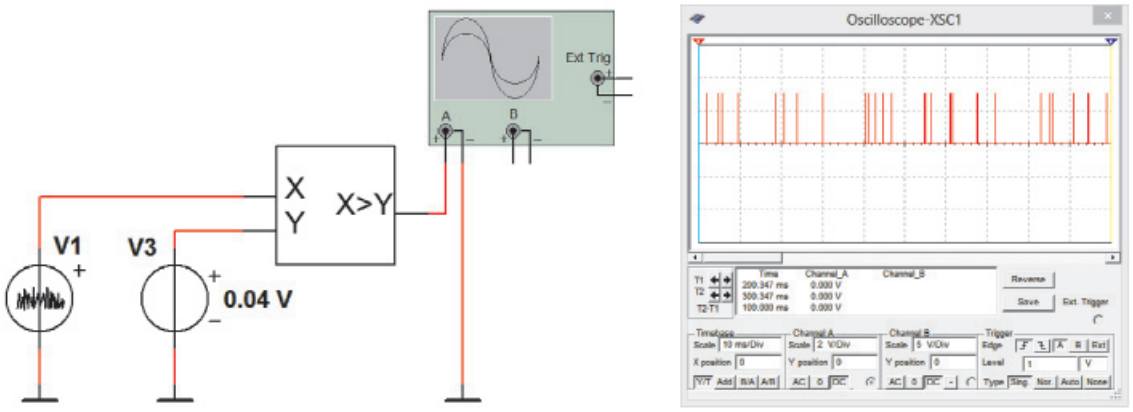

Рис. 1. Схема задающего генератора случайного потока импульсов и генерируемый им поток событий

Важнейшей задачей при реализации аналого-цифровой модели случайных процессов является получение нескольких – в общем случае *n* – статистически независимых источников потоков случайных событий, то есть случайных последовательностей. Как известно, для получения настоящих случайных последовательностей используют физические источники энтропии – например флуктуации тока в резисторе (тепловой шум), дробовой шум в электронно-вакуумных приборах, детекторы событий ионизирующей радиации или космического излучения и т.п. [2, 4]. В криптографии псевдослучайная цифровая последовательность чаще всего формируется последовательными регистрами сдвига с линейной обратной связью (РСЛОС). Для получения сигнала обратной связи используется элемент «исключающее ИЛИ», реализующий операцию XOR над некоторыми битами регистра, определяемыми последовательностью отводов обратной связи [3, 4]. Этот алгоритм имеет большую скорость работы и генерирует последовательности, статистически неотличимые от случайных. Однако любой генератор псевдослучайных чисел (ГПСЧ) с ограниченными ресурсами рано или поздно зацикливается – начинает повторять одну и ту же последовательность чисел. Если порождаемая последовательность ГПСЧ сходится к слишком коротким циклам, то такой ГПСЧ становится предсказуемым и непригодным для практических приложений.

Линейные кодовые последовательности имеют относительно низкую структурную скрытность. Под скрытностью в криптографии понимают способность противостоять мерам радиотехнической разведки: обнаружению сигнала и определению его структуры на основе оценки ряда его параметров [2]. В нашем случае надо понимать этот термин в широком смысле – как меру хаотичности и случайности. Более высокую структурную скрытность – то есть непредсказуемость – имеют нелинейные последовательности, которые формируются регистрами сдвига с нелинейными обратными связями, например схемой «И». Нелинейная обратная связь допускает нахождение всех разрядов регистра сдвига в нулевом состоянии и обеспечивает выход генератора из него. Это принципиально важно при моделировании редко повторяющихся событий, характерных для сферы безопасности, то есть когда основным состоянием процесса является отсутствие событий.

При предлагаемой имитационной модели в качестве исходного генератора событий предлагается использовать ГСПЧ, реализованный на встроенном в программе Multisim источнике теплового шума V1 и компараторе, реализующем пороговую обработку (рис. 1). При изменении напряжения опорного источника V3, определяющего порог срабатывания компаратора, изменяется интенсивность потока событий.

Получение необходимого количества некоррелированных друг с другом ГСПЧ реализуется схемами задержки с нелинейными обратными связями, имеющими ответвления между двумя линиями задержки (ЛЗ) со случайно выбранными длительностями.

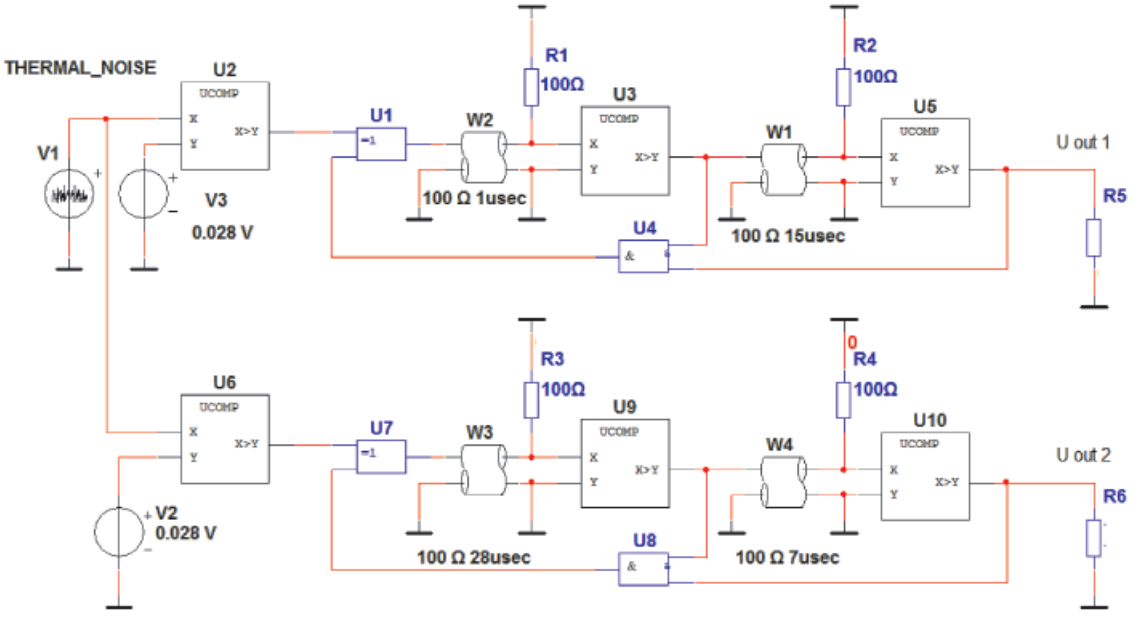

Рис. 2. Схема двух каналов ГСПЧ

Новизной в предлагаемой модели является применение вместо регистров сдвига совокупности ЛЗ. В общем случае количество отрезков линий задержки и соответственно количество ответвлений обратной связи может быть достаточно большим, причем обратные связи могут представлять собой как нелинейные на элементах «И», так и линейные на элементах «исключающее ИЛИ». Параметры ЛЗ задаются перед началом моделирования и их числовые значения являются случайными. Комбинации отношений длительности задержки обеспечивают различные параметры полученных ГСПЧ. Преимущества такого решения заключаются в возможности простого и наглядного изменения параметров ГСПЧ имитационной модели. В минимальной конфигурации достаточно иметь две ЛЗ, что показано на схеме двух каналов ГСПЧ на рис. 2.

Применение ЛЗ обеспечивает асинхронный режим работы источника случайного потока событий, что принципиально отличает предложенную схему от ГПСЧ, применяемых в криптографии, где передача данных происходит по сигналам тактирующего генератора.

Специфика и отличие от ГПСЧ, применяемых в криптографии, заключается также в том, что встроенный в программе Multisim источник теплового шума выполняет функцию как начальной кодовой последовательности, которая постоянно меняется, так и шифруемого сообщения. Начальная кодовая последовательность у всех ГСПЧ получается одинаковой, так как исходный источник теплового шума один, но после прохождения через линии задержки со случайными ответвлениями нелинейной обратной связи эти сигналы становятся некоррелированными. На рис. 3 показаны результаты моделирования при различных параметрах ЛЗ, демонстрирующие возможности разработанной схемы.

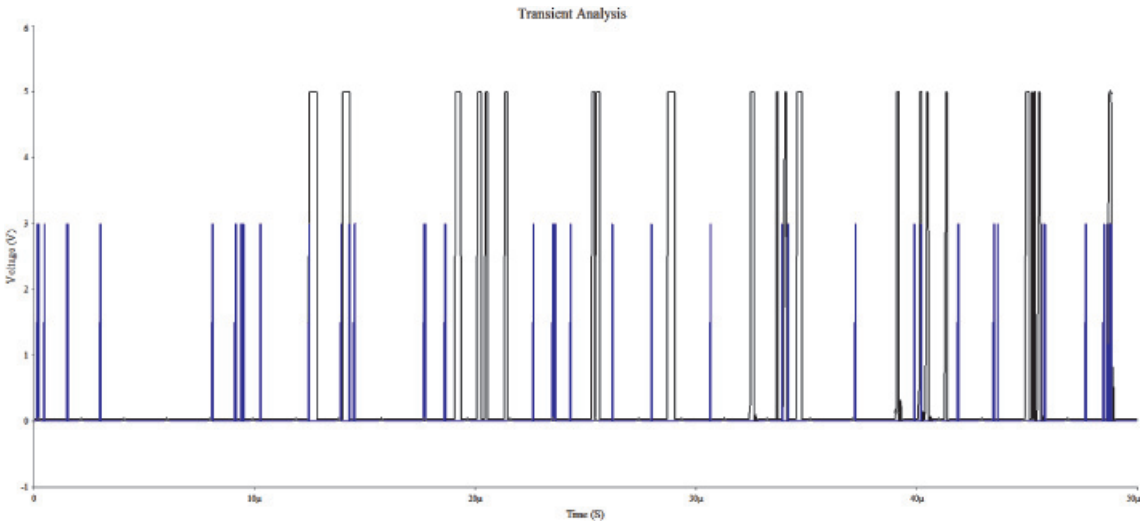

Рис. 3. Пример результатов моделирования в Multisim в режиме Transient analisys

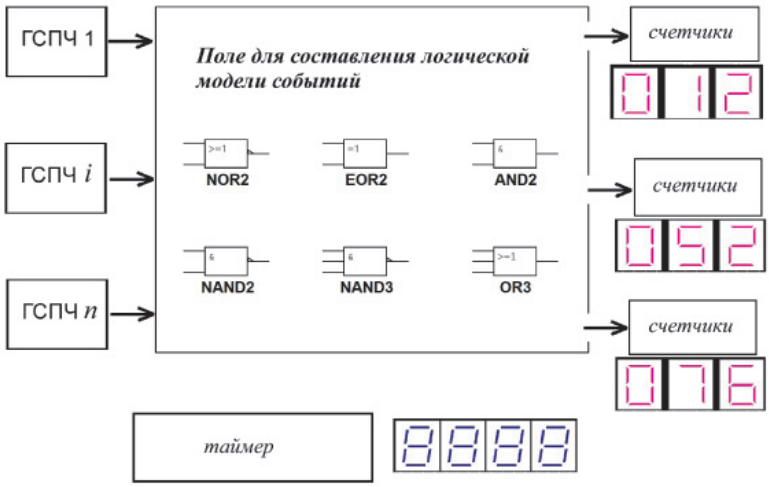

Рис. 4. Структурная схема имитационной модели

Исходный поток событий от задающего генератора случайного потока импульсов одинаков для всех каналов и на осциллограммах показан меньшей амплитудой. Выходной поток показан импульсами черного цвета с большей амплитудой.

Структурная схема имитационной модели приведена на рис. 4. Поле «логическая модель событий» предназначено для построения схемы из логических элементов и связей между ними на основе имеющейся в библиотеке Multisim элементной базы в соответствии с поставленной задачей моделирования. Очевидно, что основными элементами, необходимыми для построения деревьев событий, будут «И» и «ИЛИ», как это и рассмотрено в [5]. В то же время возможности схемотехники Multisim позволяют моделировать сценарии развития событий, включающие обратные связи, задержки, формирование заданных длительностей существования событий на основе одновибраторов, случайное или детерминированное перераспределение потоков случайных событий по различным вероятным сценариям на основе асинхронных мультиплексоров. Указанные возможности существенно расширяют диапазон применений разработанной модели при анализе безопасности.

Выходными параметрами модели являются счетчики количества событий, подключаемые в необходимые точки логической модели, а также таймер, определяющий интервалы времени от начала моделирования до его завершения. Управление таймером (сигнал «стоп») может осуществляться из любой точки логической схемы. Фактически таймер может измерять время не в секундах, а в количестве тактирующих импульсов, параметры которых задаются при начале моделирования с помощью опций источника «pulse voltage source». Параметры этих импульсов можно интерпретировать как события в реальной жизни: например при анализе пожарной безопасности типичным для объекта является интенсивность потока событий, приводящих к возникновению пожара, составляет порядка $10^{-5}…10^{-7}$ год$^{-1}$, а в предложенной имитационной модели этот поток будет моделироваться за единицы секунд. Счетчики реализуются на общеизвестных схемах и имеют выход на соответствующие семисегментные индикаторы. Таймер реализуется генератором импульсов и счетчиком.

Выводы

Предложенная модель объединяет в себе математическую модель марковских процессов с непрерывным временем и дискретными состояниями и логические модели, описывающие деревья событий и наиболее полно соответствующие реальным физическим процессам в сфере безопасности.

Отличительными преимуществами аналого-цифровой имитационной модели случайных процессов являются:

– сжатие масштаба времени реальных случайных процессов в техносферной безопасности (например, при анализе рисков пожара) в миллионы – миллиарды раз;

– простое и наглядное создание и изменение сложных логико-вероятностных структур (деревья событий, деревья отказов и т.п.), описывающих различные сценарии возникновения угроз безопасности;

– широкие возможности для обработки полученных экспериментальных статистических данных с возможностью их экспорта в специализированные программы для дальнейшей математической обработки (Labview, Mathcad, MathLab, Excel).

Список литературы

1. Вентцель Е.С., Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. – М.: Высш. шк., 2000. – 383 с.: ил.

2. Помехозащищенность радиосистем со сложными сигналами / Г.И. Тузов, В.А. Сивов, В.И. Прытков. – М.: Радио и связь, 1985. – 264 с.

3. Сизоненко А.Б. Многоканальный цифровой источник шума на основе рекуррентного регистра сдвига // Спецтехника и связь. – 2012. – № 3. – С. 51–54.

4. Horowitz, Paul, and Winfield Hill. The Art of Electronics. – 2nd ed. – Vol. 2. Cambridge: Cambridge UP, 1989. Print.

5. IEC 31010:2009 Risk management – Risk assessment techniques.

References

1. Vencel E.S., Ovcharov L.A. Teorija sluchajnikh processov i ejo inzhenernye prilozhenija (Theory of stochastic process and engineering applications). Moscow, High school Publ., 2000. 383 p.

2. Tuzov G.I., Sivov V.A., Prytkov V.I. Pomekhozashhishhjonnost radiosistem so slozhnymi signalami (Jamming protection of radio systems with complex signals). Moscow, Radio and Comm. Publ., 1985. 264 p.

3. Sizonenko A.B. Mnogokanalnyy tsifrovoy istochnik shuma na osnove rekurrentnogo registora sdviga // Spetstekhnika i svyaz no. 3, 2012, pp. 51–54.

4. Horowitz, Paul, and Winfield Hill. The Art of Electronics. 2nd ed. Vol. 2. Cambridge: Cambridge UP, 1989. Print.

5. IEC 31010:2009 Risk management – Risk assessment techniques.

Рецензенты:

Рябов И.В., д.т.н., профессор, Поволжский государственный технологический университет, г. Йошкар-Ола;

Скулкин Н.М., д.т.н., профессор, Поволжский государственный технологический университет, г. Йошкар-Ола.