АППАРАТНЫЕ ТРОЯНЫ. ЧАСТЬ 2: ПРИМЕРЫ РЕАЛИЗАЦИИ, СПОСОБЫ ВНЕДРЕНИЯ И АКТИВАЦИИ

HARDWARE TROJANS. PART2: EXAMPLES OF IMPLEMENTATION, METHODS OF INSERTION AND ACTIVATION

УДК 621.382, ВАК 05.27.01, DOI:10.22184/1993-8578.2016.70.8.12.20

Е.Кузнецов, А.Сауров**
E.Kuznetsov, A.Saurov**

Во второй части цикла статей, посвященных аппаратным закладкам в интегральных схемах – аппаратным троянам, приведены примеры их реализации и внедрения в интегральные схемы. Рассмотрены различные методы активации аппаратных троянов в электронной системе.
In the second part of a series of articles devoted to hardware Trojan examples of their implementation and insertion into integrated circuits are given. Various methods of hardware Trojan activating in electronic system are considered.

Аппаратные закладки лишь недавно попали в поле зрения исследователей, поэтому пока опубликовано сравнительно мало данных об их фактической реализации, и только в нескольких публикациях предпринято углубленное рассмотрение эффектов от атак с их использованием. Ниже рассматриваются наиболее интересные подходы к реализации аппаратных закладок.

В работе [1] представлены два наиболее общих подхода к созданию вредоносного процессора. Авторы показывают, как электрические схемы аппаратных троянов могут быть встроены в процессор для реализации таких атак, как кража паролей, расширение привилегий доступа и автоматические логины в систему. Представлена общая платформа для поддержки широкого спектра атак с возможностью их динамического обновления. В центральный процессор вносятся две модификации, которые реализуют механизм, обеспечивающий злоумышленнику доступ в защищенные области памяти, и теневой режим, позволяющий взломщику выполнить скрытую "встроенную программу". В работе описывается атака на логин, которая дает злоумышленнику полный высокий уровень доступа к процессору. Атака выполнена с помощью злонамеренной модификации, реализованной на схеме с использованием только 1341 вентилей. Авторами впервые приведена реализация аппаратной закладки, которая может использоваться в качестве общей программируемой платформы для атак. Показано внесение такой модификации на уровне VHDL (языка описания аппаратуры интегральных схем), проведено моделирование и синтез ИС для платформы на базе процессора Leon 3 SPARC 40 МГц. Рассмотрено обнаружение такого аппаратного трояна путем анализа внесенных им возмущений в аналоговые и цифровые сигналы. В частности, отмечается, что операционной системе виден программный компонент механизма доступа к памяти, и могут быть обнаружены задержки сигнала, связанные с внесением модификации. Также в работе [1] показаны общие подходы для обеспечения защиты от подобных вредоносных процессоров.

С целью изучения способов внедрения аппаратных закладок в политехническом институте Нью-Йоркского университета проводятся ежегодные конференции CSAW (Cyber Security Awareness Week – Неделя знаний об информа-

* НПК "Технологический центр"/ SMC "Technological Centre"

ционной безопасности). В рамках этой конференции организуются состязания между командами по внедрению и поиску встроенных аппаратных систем (Embedded System Challenge). В 2008 году было дано задание получить доступ к криптографическому устройству "АЛЬФА" на основе ПЛИС путем внесения набора аппаратных закладок, при этом устройство должно проходить тест на достоверность. Участникам соревнования выдали исходный HDL-код и предоставили один месяц на разработку. Победили две команды, одна из которых разработала механизм утечки информации секретных ключей через канал входа-выхода, другая – организовала DoS-атаку. Если обобщить все участвовавшие в состязании разработки, то аппаратные закладки были в 90% случаев внесены на этапе фазы разработки ИС, 50% из них активировались пользователем и 75% аппаратных троянов были размещены в схемах входа-выхода [2].

В работе [3] анализируется пространство проектных параметров аппаратных закладок и предлагается схема размером менее 50 вентилей, вырабатывающая мощность, которая может служить побочным каналом для скрытой утечки секретной информации. Технология, получившая название MOLES (Malicious Off-chip Leakage Enabled by Side-channels), была реализована в криптографической ИС на основе алгоритма AES, спроектированной по проектным нормам 45 нм. Использование метода расширенного спектра при разработке аппаратного трояна MOLES позволило осуществлять считывание многоразрядной информации на основе анализа потребляемой мощности с чувствительностью ниже уровня собственных шумов ИС, что обеспечивает скрытность. Авторы [3] заявляют, что данная технология обладает максимальной скрытностью и невосприимчивостью к большинству методов обнаружения аппаратных троянов, таких как визуальный контроль, проведение функциональных тестов и обнаружение на основе характерных "дактилоскопических" признаков ИС. Хотя схема задействует малое количество логических вентилей, вычислительные затраты для восстановления считанных данных, имеющих малое отношение сигнал / шум, с учетом вариабельности характеристик технологии, могут иметь критическое значение. Авторы [3] предложили обобщенную методологию проектирования и реализации MOLES-схем, опираясь на математический аппарат теории обнаружения для анализа дифференциальной мощности, которая необходима для экстракции многоразрядных ключей. Полученные результаты основаны на модели-

Hardware Trojans have only recently come in view of researchers, therefore, there is relatively little published data on their actual implementation, and only a few publications have undertaken an in-depth examination of the effects of their attacks. The following are considering the most interesting approaches to the implementation of hardware Trojans.

Paper [1] gives two of the most common approaches to creating malicious processors. The authors show how the electric circuits of hardware Trojans can be embedded in the processor to carry out such attacks as the theft of passwords, access privileges extension and automatic logins to the system. It presents a common platform to support a wide range of attacks with the possibility of their dynamic update. Two modifications are installed into the central processor to implement a mechanism that provides an attacker access to the protected memory area, and the shadow mode allowing an attacker to perform a silent embedded software. The Paper describes the attack on the login which allows the attacker a complete high level access to the processor. The attack is fulfilled with the help of a malicious modification based on the circuit by using only 1341 gates. For the first time the authors show the way of the implementation of hardware Trojan that can be used as a common programmed platform for the attacks. They show embedding of such a modification on the VHDL level (Hardware Description Language) and IC modelling and synthesis for the platform based on the 3 Leon SPARC 40 MHz processor have been conducted. Detection of this hardware Trojan by analysing the perturbations introduced by it into analogue and digital signals has been considered. In particular, it is noted that the operating system determines the software component of the memory access mechanism and it can detect a signal delay associated with the introduction of a modification. Also paper [1] shows common approaches to ensure the protection against these malicious processors.

In order to study how to embed hardware Trojans annual CSAW (Cyber Security Awareness Week)

ровании экстракции только коротких ключей (8-бит), весьма далеких от реальной разрядности используемых ключей. При этом авторы указывают, какие вопросы необходимо решить для практического надежного восстановления многоразрядных ключей на основе анализа потребляемой мощности крипто-процессора.

В работе [4] проведены эксперименты с двумя упрощенными аппаратными закладками, встроенными в схемы шифрования на основе RSA – алгоритма для анализа эффектов, связанных с побочными каналами. В аппаратных закладках использовался простой счетчик, отключавший ИС после определенной пороговой величины, и компаратор, который сравнивал данные на системной шине или регистре с фиксированной величиной и вносил изменения в вычислительный процесс при превышении соответствия. Указывается, что такие аппаратные закладки достаточно трудно обнаружить, и они могут использоваться для отключения электрических схем, кражи информации, сбоев в системе, нарушения целостности и безопасности всей системы, в которую включена "зараженная" ИС.

В работе [5] рассматривается пример аппаратного трояна, действие которого приводит к утечке информации из ядра DES-шифрования. За такт схема извлекает один бит 56-разрядного ключа. Вскрывая один бит в каждом 64-разрядном блоке предаваемых данных, троян обеспечивает утечку информации. После накопления всех 56-ти блоков зашифрованного текста, полный ключ передается по радиоканалу, компрометируя шифрование. Извлеченный ключ спрятан в допустимом диапазоне амплитуды или частоты, обусловленном вариацией параметров технологического процесса, что обеспечивает соблюдение разработанных функциональных спецификаций ИС.

В работе [6] описан новый тип аппаратных закладок, основанных на надежностных характеристиках ИС. Этот тип троянов –достаточно простые модификации технологического процесса, которые приводят к ускорению деградации КМОП ИС. Изменения в технологии могут не затрагивать внутренние характеристики схемы, однако влияют на увеличение вариабельности технологических параметров, поэтому выявляются в ходе технологических тестов. Такие аппаратные трояны могут основываться на следующих деградационных физических явлениях: эффекте горячих электронов (эффект HCI), электрическом пробое затворного диэлектрика, эффекте температурной нестабильности при обратном смещении в p-МОП транзисторе (NBTI эффект), эффекте электромиграции. По классификации их можно отнести к постоянно действующим аппаратным троянам типа DoS (отказ в обслуживании), которые приводят к постепенной деградации рабочих характеристик, либо к ранним отказам отдельных частей ИС.

conferences are held at the Polytechnic Institute of New York University. As part of this conference, competitions between the teams for embedding and searching embedded hardware systems (Embedded System Challenge) are organized. In 2008 the task was given to gain access to the FPGA-based ALPHA cryptographic unit by introducing a set of hardware Trojans, while the device must be tested for validity. The participants of the competition received the source HDL-code and were given one month for development. Two teams won, one of which developed a mechanism for leaks of secret keys via the input-output channel but the other team organized of DoS attack. To synthesize all the projects considered in the competition, the hardware Trojans were embedded at the stage of IC development phase in 90% of cases, 50% of them were activated by the user, and 75% of hardware Trojans were embedded in the input-output circuits [2].

Paper [3] analyses the space of design objectives of hardware Trojans and a scheme of fewer than 50 gates is offered generating power output which can serve as a side channel for clandestine leakage of confidential information. The technology called MOLES (Malicious Off-chip Leakage Enabled by Side-channels) has been implemented in the cryptographic 45 nm IC based on the AES algorithm. The use of the spread-spectrum technique in the development of the MOLES hardware Trojan allowed to carry out reading out a multi-bit data on the basis of power consumption analysis with the sensitivity of below the level of IC own noises that ensure clandestine activity. The authors of paper [3] claim that this technology has the highest secrecy and immunity to most methods of detection of hardware Trojans, such as visual

МЕХАНИЗМЫ АКТИВАЦИИ ЗАКЛАДОК

Как правило, после внедрения в систему аппаратная закладка находится в состоянии покоя, пока не будет активирована (запущена) для выполнения своей вредоносной функции. Механизмы активации могут иметь разнообразный характер, явный или скрытый, случайный, непосредственный, или заранее определенный, в результате которых аппаратный троян может изменять свое состояние и поведение. Знания об этих механизмах важны, поскольку процесс активации может нести информацию, позволяющую выявить и противодействовать аппаратной закладке. Следует пытаться активировать аппаратные трояны на этапах верификации ИС. Обычно это выполняется при аттестационном и функциональном тестировании ИС или при исследовании пространства состояний проекта, включая состояния входов-выходов и внутренней логики. Активация аппаратной закладки во время тестирования может помочь идентифицировать ее наличие в ИС. Различные механизмы активации и их классификация коротко рассмотрены ниже.

АППАРАТНЫЕ ТРОЯНЫ С ВНУТРЕННЕЙ АКТИВАЦИЕЙ

Внутренняя активация основывается на некоторых специфических состояниях, при достижении которых в целевом устройстве происходит активация аппаратной закладки. В большинстве случаев она строится на схемах секвенциальной (последовательностной) или комбинационной логики.

АКТИВАЦИЯ НА ОСНОВЕ КОМБИНАЦИОННОЙ ЛОГИКИ

Аппаратный троян с активацией на основе комбинационной логики запускается при достижении так называемого триггерного состояния, когда определенные значения (векторы) обнаруживаются на определенных узлах внутренней схемы ИС. Этот тип активационного механизма может быть реализован только с использованием комбинационной логики (комбинационный триггер). В работе [7] авторы приводят пример так называемого "однотактного чит-кода" – специфического адреса на шине, который активизирует аппаратный троян. На практике комбинационная активация может потребовать большего набора определенных одновременных состояний на некоторых узлах, например на внутренних регистрах, совмещенных со специфическим словом на шине данных и определенным словом на адресной шине. В работе [8] приводится пример, в котором для активации аппаратной закладки используются определенные комбинированные наборы на входах ИС. В частности, это может быть определенный входной набор, объединяющий данные, управляющие команды, адреса и команды самотестирования.

inspection, conducting functional tests and the detection based on the characteristic "dactylographic" IC features. Although the scheme uses a small amount of logic gates, the computational cost for restoring the read data having a low S/N ratio may be critical taking the technology characteristics variability into account. The authors of paper [3] proposed a generalized design methodology and implementation of MOLES-schemes basing on the mathematical apparatus of the theory of detection for the analysis of differential power which is necessary for the extraction of multi-bit keys. The received results are based on modelling the extraction of only short keys (8-bit), which are very far from the real bit keys used. At the same time the authors point out what issues are needed to be solved for practical reliable restoring multi-bit keys basing on an analysis of crypto-processor power consumption.

Paper [4] displays experiments with two simplified hardware Trojans embedded in encryption schemes based on RSA, an algorithm for the analysis of the effects associated with the side channels. The hardware Trojans used a simple counter disabling the IC after a certain threshold value and a comparator comparing the data on the system bus or a register with a fixed value and made changes in the computational process in case of threshold crossing. It is stated that it is rather difficult to detect such hardware Trojans and they can be used for turning off the electrical circuits, information theft, introducing errors, destroying the integrity and security of the entire system into which the "contaminated" IC has been embedded.

Paper [5] describes an example of a hardware Trojan the effect of which leads to the leakage of information from the kernel DES-encryption. The circuit

АКТИВАЦИЯ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТНОЙ ЛОГИКИ

Аппаратный троян с активацией на основе последовательностной логики запускается определенной последовательностью событий. Если сравнивать с комбинационной активацией, то активация на последовательностной логике имеет намного большее пространство состояний, так как триггерный механизм здесь может реализовываться с использованием конечного автомата. В работе [9] отмечается, что поскольку конечный автомат обеспечивает логическую глубину, последовательность событий обычно описывается маловероятными логическими величинами, и обнаружить их во время тестирования и верификации ИС намного труднее.

Простейшим последовательностным триггером является схема синхронного счетчика, которая активируется после определенного количества циклов синхронизации. В работе [7] такие трояны названы "бомбами замедленного действия". В работе [9] обсуждаются счетчики асинхронных последовательностей, в которых при определенных событиях осуществляется приращение, например, увеличение фронта импульса на выходе вентиля. Эти же авторы предлагают использование гибридного механизма активации, комбинируя синхронные и асинхронные триггеры.

Также в работе [9] рассматриваются так называемые последовательные чит-коды. Например, к активации аппаратного трояна приводит последовательность байт 0xd, 0xe, 0xc, 0xa, 0xf, 0xb, 0xa, 0xd в течение различных восьми циклов синхронизации. При этом нет необходимости, чтобы данные байты приходили последовательно, они могут быть разнесены по времени. Таким образом, активация аппаратного трояна достигается гораздо более сложной последовательностью событий.

Задать сложность последовательностного триггера не представляет труда для разработчика аппаратной закладки. Единственная проблема, связанная с увеличением сложности – потребляемая трояном мощность и количество логических вентилей, необходимых для его реализации. В связи с этим были предложены внутренние последовательностные механизмы активации, которые используют физические и аналоговые эффекты в ИС. Например, мониторинг температуры чипа или потребляемой мощности могут быть включены в механизм пусковой схемы. Более того, в работе [9] приводится конкретный пример схемы, состоящей из электрической емкости, заряжающейся через резистор. Заряд и напряжение на емкости определяются активностью окружающей логики, которая в свою очередь может отражать активность ИС. Аппаратная закладка запускается при достижении на емкости определенного значения порогового напряжения.

Активационный триггер может быть как цифровым, так и аналоговым. Аналоговая активация используется с целью увеличения

extracts one bit of a 56-bit key in one phase. Exposing one bit in each 64-bit transmission data block, the Trojan provides the information leakage. After accumulating all 56 blocks of an encrypted text the full key is transmitted over the air compromising the encryption. The extracted key is hidden within the allowable range of the amplitude or frequency specified by a variation of the technological process parameters, which ensures compliance with the designed functional IP specifications.

Paper [6] describes a new type of hardware Trojans based on the IC reliability characteristics. This type of Trojan is easily embedded into the technological process and leads to the faster degradation of CMOS IC. It is possible that modifications will not affect the characteristics of the internal circuits but they affect the increase in variability of process parameters, therefore they are identified in the course of technological tests. Such hardware Trojans may be based on the following degradation physical phenomena: the hot electron effect (HCI effect), electrical breakdown of the gate dielectric, the temperature instability effect at a reverse bias in the p-channel MOS transistor (NBTI effect), and the electromigration effect. According to the classification they can be attributed to a permanent type of DoS (Denial of Service) hardware Trojans which lead to a gradual degradation of performance or to the early failures of separate parts of IC.

MECHANISMS OF ACTIVATION OF TROJANS

As a rule, a hardware Trojan is dormant after embedding into the system until it is activated (started) to perform its malicious function. Activation mechanisms can be diverse in nature, explicit or hidden, incidental, direct, or

скрытности и сложности его обнаружения. Злоумышленник может использовать несколько индивидуальных триггеров последовательностного типа для активации различных троянов в ИС.

Активация на основе последовательностной логики может предусматривать как контентные, так и временные события. В работе [10] исследовались такие триггеры, когда активация трояна происходит при определенных контентных данных в определенное время. Для простого активационного триггера было показано, что время тестирования, за которое можно с большой вероятностью активировать такой троян, составляет $3 \cdot 10^{35}$ лет: рассматривалась вероятность определения комбинации определенных числовых кодов, вводимых с клавиатуры за определенный интервал времени.

Авторы [10] предложили также "температурный триггер". Принцип его действия заключается в следующем. Активность определенных участков ИС на кристалле модулирует частоту кольцевого генератора, выполненного на инверторах. Частота кольцевого генератора определяет тепловыделение, которое влияет на задержку в другом подобном кольцевом генераторе. При достижении определенной величины задержки происходит активация аппаратной закладки. Похожие механизмы могут быть построены на использовании в качестве сигнала для активации электромагнитных или радиочастотных помех, частоты или потребляемой мощности логической схемы, а также временной характеристики потребляемой мощности определенных участков ИС.

АППАРАТНЫЕ ТРОЯНЫ С ВНЕШНЕЙ АКТИВАЦИЕЙ

Внешняя активация подразумевает некое взаимодействие аппаратного трояна с внешней средой, отличной от системы, в которую внедрен троян. Преимущества использования внешних триггеров для атакующего заключается в том, что активация инициируется источником, расположенным вне системы и поэтому не зависящим от нее [11]. В этой же работе приводятся примеры приемников или антенн внешнего сигнала, внедренных в "зараженный" прибор.

В работе [8] рассматриваются встроенные в чип сенсоры, которые могут осуществлять мониторинг физических параметров: температуры, электрического напряжения, электромагнитных помех, влажности и высоты над уровнем моря. Активационные механизмы с подобными сенсорами на чипе часто называют триггерами побочного канала по аналогии с технологиями получения информации в электронных приборах без непосредственного влияния на них [12]. Другие внешние механизмы активации аппаратных троянов основаны на непосредственном взаимодействии с целевым прибором. Также активация может быть инициализирована прикрепленным компонентом системы, например дополнительной памятью.

predetermined, as a result of which a hardware Trojan can change its state and behaviour. Knowledge of these mechanisms is important because the activation process may carry the information that enables to identify and counteract the hardware Trojan. It is necessary to try to activate the hardware Trojans at the stages of IC verification. This is usually carried out during the conformance and functional testing of ICs or space research of project conditions including the status of inputs, outputs and internal logic. Activation of a hardware Trojan during testing can help to identify its presence in the IC. Various mechanisms of activation and their classification are briefly discussed below.

HARDWARE TROJANS WITH INTERNAL ACTIVATION

Internal activation is based on some specific conditions at which activation of hardware Trojans in the target device takes place. In most cases it is based on the circuits of the sequential or combinational logic.

ACTIVATION BASED ON THE COMBINATIONAL LOGIC

The hardware Trojan with activation based on the combinational logic is embedded when the so-called flip-flop state is achieved and when certain values (vectors) are found on certain sites of the internal IC schemes. This type of an activation mechanism can be implemented only by using the combinational logic (combinational flip-flop). In their paper [7] the authors give the example of the so-called "single-cycle cheat code", a specific address on the bus, which activates a hardware Trojan. In practice the combinational activation may require a larger set of definite simultaneous states at certain nodes, such as internal registers combined with a

ПОСТОЯННО АКТИВНЫЕ АППАРАТНЫЕ ЗАКЛАДКИ

Существуют аппаратные закладки, которые всегда активны и не могут быть активированы или дезактивированы специальным триггерным механизмом. Возможны также аппаратные трояны, которые вносят незаметные изменения в спецификацию, функциональность или синхронизацию системы и не нуждаются в триггерном механизме. В качестве примера таких постоянно действующих троянов можно привести аппаратную закладку, производящую утечку данных через побочный канал, который отражает активность специфической ИС.

Постоянно активные аппаратные закладки могут иметь и более тонкие триггерные механизмы. В работе [11] обсуждается такая модификация топологии, при которой отдельные узлы или части ИС имеют большую вероятность отказа, то есть можно говорить, что триггерный механизм постоянно действует и приводит к непрерывной деградации рабочих характеристик ИС. В работе [6] рассматриваются модификации в ИС, в результате которых она выходит из строя после определенного периода эксплуатации длительностью от нескольких месяцев до года. Примеры таких аппаратных троянов – преднамеренные изменения в технологическом процессе, приводящие к ухудшению надежности ИС. Трудность их обнаружения связана с тем, что вносимые изменения не влияют на параметры ИС, которые находятся в допустимых пределах, характерных для технологического процесса. Поскольку такие трояны постоянно активны, они не имеют побочных активационных эффектов, таких как изменения шумовых характеристик ИС, изменения характера потребляемой мощности или температуры.

ОСОБЕННОСТИ РАЗРАБОТКИ ТРИГГЕРНЫХ МЕХАНИЗМОВ АКТИВАЦИИ

Разработчику аппаратного трояна достаточно просто создать триггерный механизм активации, который будет трудно обнаружить, поскольку он может использовать огромное пространство состояний системы, в которую внедряется троян. Это пространство состояний включает все внутренние узлы логических схем, входов и выходов ИС, модификацию топологии ИС, вариации технологических процессов, аналоговые эффекты электроники в ИС. Гибридные механизмы, совмещающие некоторые или все известные триггерные принципы, делают работу по обнаружению аппаратных закладок все более трудной. Общее мнение исследователей сводится к тому, что постоянно действующие аппаратные закладки намного более трудны для обнаружения по сравнению со сложными конструкциями триггерных механизмов для предотвращения случайной активации или активации во время тестирования.

ЗАКЛЮЧЕНИЕ

Внести и активировать аппаратные трояны становится проще с увеличением пространства состояний, повышением параллельности вычислений,

specific word on the data bus and a certain word on the address bus. In Paper [8] there is an example in which certain combination sets at IC inputs are used to activate the hardware Trojan. In particular, it may be a certain input set combining the data, control commands, addresses and self-testing commands.

ACTIVATION BASED ON THE SEQUENTIAL LOGIC

Hardware Trojan with activation on the basis of the sequential logic is embedded with the help of a specific sequence of events. In comparison with the combinational activation, the activation based on the sequential logic has a much larger state space as a flip-flop mechanism in this case can be implemented using finite state automation. It is stated in paper [9] that since finite state automation provides a logical depth, the sequence of events is usually described with the help of unlikely logical values; as a result, it is much more difficult to detect it during testing and verifying IC.

The simplest sequential flip-flop is a synchronous counter circuit which is activated after a certain number of timing loops. In paper [7], these Trojans are called "delayed-action bombs". In paper [9] asynchronous sequence counters are considered in which at certain events increments, for example, an increase in pulse edge at the exit gate, are carried out. These authors offer the use of a hybrid activation mechanism combining synchronous and asynchronous flip-flops.

Paper [9] also considers the so-called sequential cheat codes. For example, the sequence of bytes 0xd, 0xe, 0xc, 0xa, 0xf, 0xb, 0xa, 0xd during eight different timing loops leads to activation of a hardware Trojan. Besides, it is not necessary for the data bytes to come

усложнением внутренней разводки и возрастанием числа входов-выходов современных ИС. В таких условиях аппаратная закладка может быть глубоко скрыта внутри конструкции ИС и очень трудно поддаваться обнаружению. Необходимо отметить, что разработки, направленные на предотвращение внесения аппаратных троянов на этапе проекта или изготовления ИС, все еще находятся в зачаточном состоянии.

Статья подготовлена при финансовой поддержке Минобрнауки России в рамках выполнения государственного задания 8.527.2016/БЧ.

ЛИТЕРАТУРА

1. **Baumgarten A. et al.** A case study in hardware Trojan design and implementation // International Journal of Information Security. 2011. Т. 10. №. 1. С. 1–14.
2. **Rajendran J. et al.** Towards a comprehensive and systematic classification of hardware trojans // Circuits and Systems (ISCAS), Proceedings of 2010 IEEE International Symposium on. IEEE, 2010. С. 1871–1874.
3. **Lin L., Burleson W., Paar C.** MOLES: malicious off-chip leakage enabled by side-channels // Proceedings of the 2009 International Conference on Computer-Aided Design. ACM, 2009. С. 117–122.
4. Agrawal D. et al. Trojan detection using IC fingerprinting // Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007. С. 296–310.
5. **Jin Y., Makris Y.** Hardware Trojans in Wireless Cryptographic ICs // IEEE Design & Test of Computers. 2010. Т. 27. №1.С. 26–35.
6. **Shiyanovskii Y. et al.** Exploiting semiconductor properties for hardware trojans // arXiv preprint arXiv:0906.3834. 2009.
7. **Waksman A., Sethumadhavan S.** Silencing hardware backdoors // Security and Privacy (SP), 2011. IEEE Symposium on. IEEE, 2011. С. 49–63.
8. **Tehranipoor M., Koushanfar F.** A survey of hardware trojan taxonomy and detection // IEEE Design and Test of Computers. 2010. №1. Т. 27. С. 10–25.
9. **Chakraborty R.S., Narasimhan S., Bhunia S.** Hardware Trojan: Threats and emerging solutions // High Level Design Validation and Test Workshop, 2009. HLDVT 2009. IEEE International. IEEE, 2009. С. 166–171.
10. **Chen Z. et al.** Hardware trojan designs on basys fpga board // Embedded System Challenge Contest in Cyber Security Awareness Week-CSAW. 2008. Т. 2008.
11. **Wang X., Tehranipoor M., Plusquellic J.** Detecting malicious inclusions in secure hardware: Challenges and solutions // Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on. IEEE, 2008. С. 15–19.
12. **Potkonjak M.** Synthesis of trustable ICs using untrusted CAD tools // Proceedings of the 47th Design Automation Conference. ACM. 2010. С. 633–634.

sequentially; they can be separated in time. Thus, the activation of a hardware Trojan is achieved by much more complex sequence of events.

To develop the complexity of a sequential flip-flop is not difficult for a developer of hardware Trojans. The only problem associated with increasing complexity is the power consumed by the Trojan and the number of logic gates required for its embedding. In this regard internal sequential activation mechanisms that use physical and analogue effects in ICs have been offered. For example, chip temperature or power consumption monitoring may be included in the flip-flop mechanism of the circuit. Furthermore, Paper [9] gives a specific example of a circuit consisting of capacitance charged through a resistor. The charge and voltage on the capacitance are determined by the surrounding logic activity, which in turn may reflect IC activity. A hardware Trojan starts when the capacitance achieves a certain value of the threshold voltage.

The activating flip-flop can be either digital or analogue. The analogue activation is used to increase the secrecy and complexity of its detection. An intruder can use several types of sequential individual flip-flops to activate various IC Trojans.

Activation based on the sequential logic can include both content- and time-related events. Paper [10] studies such flip-flops when activation of a Trojan comes with certain content data at a specific time. For activating a simple flip-flop, it is shown that the testing time, for which you are likely to activate such a Trojan, is $3 \cdot 10^{35}$ years, the likelihood of determining the combination of specific numerical codes entered from the keyboard for a certain period of time is considered.

The authors [10] also proposed a "temperature flip-flop". Its operating principle is as follows. The activity of specific IC sections on a crystal modulates the frequency of the ring oscillator performed on the inverters. The ring oscillator frequency determines the heat release which affects the delay in the other similar ring oscillator. When you reach a certain amount of delay, the activation of the hardware Trojan takes place. Similar mechanisms may be constructed for use as a signal to activate the electromagnetic or radio frequency interference, frequency or power consumption of a logic circuit as well as the time characteristics of the power consumption of certain sections of the IC.

HARDWARE TROJANS WITH EXTERNAL ACTIVATION

External activation involves an interaction of a hardware Trojan with an external environment that is different from the system in which the Trojan is embedded. The advantages of using external flip-flops for the intruder is that activation is initiated by a source located outside the system and therefore not depending on it. [11] The same paper gives the examples of receivers or external signal antenna embedded in the 'infected' device.

The paper [8] discusses the sensors built in chip, they can monitor physical parameters, e.g. temperature, voltage, electromagnetic interference, humidity and altitude. The activation mechanisms with similar sensors on the chip are often referred to as side-channel flip-flops similar to the technology of obtaining the information in electronic devices without producing any direct effect on them [12]. Other external mechanisms of activation of hardware Trojans are based on the direct interaction with the targeted device. Activation may also be initialised by the system's attached component, such as additional memory.

CONSTANTLY ACTIVE HARDWARE TROJANS

There are hardware Trojans that are always active, and they cannot be activated or deactivated by a special flip-flop mechanism. There are also hardware Trojans that make subtle changes to the system specification, functionality or synchronization without the need of any flip-flop mechanism. Such permanent Trojans can be illustrated by the example of the hardware Trojan generating data leakage through a side channel that reflects the activity of a specific IC.

Constantly active hardware Trojans can have flip-flop mechanisms that are more subtle. Paper [11] discusses a modification topology in which the individual components or parts of ICs have a greater probability of failure, in other words, you can say that the flip-flop mechanism operates continuously and leads to continuous degradation of operating characteristics of the IC. Paper [6] considers modifications in IP as a result of which it breaks down after a certain period of operation lasting from several months to a year.

Examples of such hardware Trojans include intentional changes in the process leading to a deterioration in the reliability of ICs. The difficulty of detecting them is due to the fact that the modifications made do not affect the change in IC parameters that are within acceptable limits typical for a process. Because these Trojans are always active, they have no side activation effects, such as changes in the noise characteristics of IC, a change in the nature of power consumption and temperature.

FLIP-FLOP ACTIVATION MECHANISM DEVELOPMENT FEATURES

It is quite easy for the developer of a hardware Trojan to create a flip-flop activation mechanism which will be difficult to detect because it can use the huge space of system states in which a Trojan is introduced. This space of states includes all the internal components of logic circuits, the IC inputs and outputs, the IC topology modification, variation of manufacturing processes and the effects of analogue electronics in IC. Hybrid mechanisms combining some or all of the known flip-flop principles make the detection of hardware Trojans increasingly difficult. The general opinion of researchers is that the permanent hardware Trojans are much more difficult to detect than the complex designs of flip-flop mechanisms to prevent accidental activation or activation during testing.

CONCLUSION

It becomes easier to introduce and activate hardware Trojans with the increase in the state of states, an increase in parallel computing, complexity of internal wiring and increasing the number of modern IC outputs/inputs. In such circumstances, hardware Trojans can be hidden deep inside the IC design and are very difficult to be detectable. It should be noted that developments designed to prevent the introduction of hardware Trojans at the stage of designing or manufacturing ICs, are still in their infancy. ■

This paper was created with the financial support of the Ministry of Education and Science of the Russian Federation within the framework of the state order 8.527.2016/БЧ.

ПЕРСПЕКТИВНАЯ ЭЛЕМЕНТНАЯ БАЗА ДЛЯ АППАРАТУРЫ С ЖЕСТКИМИ УСЛОВИЯМИ ЭКСПЛУАТАЦИИ

PROMISING ELEMENT BASE FOR EQUIPMENT OPERATING IN HARSH ENVIRONMENTS

УДК 621.382, ВАК 05.27.01, DOI:10.22184/1993-8578.2016.70.8.22.31

А.Денисов[*], *В.Коняхин*[*] / *A.Denisov@tcen.ru, V.Koniakhin@tcen.ru*
A.Denisov[*], *V.Koniakhin*[*]

Проанализированы варианты реализации специализированных микросхем. Рассмотрены особенности базовых матричных и базовых кристаллов как основы для реализации специализированных микросхем. Представлены современные серии базовых кристаллов 5521 и 5529, изготовленные по технологическим нормам 180 нм и 250 нм, а также БМК малой степени интеграции серий 5503 и 5507. Указанные БК и БМК составляют семейство серий, имеющих единую библиотеку функциональных ячеек, общие средства проектирования и аналогичные корпусные исполнения. Отличительной чертой семейства является повышенная стойкость к внешним воздействующим факторам космического пространства.

Possibilities of implementation of application-specific integrated circuit (ASIC) are analysed. The features of uncommitted logic array (ULA) and gate array (GA) as basis for the implementation of ASIC are considered. The up-to-date 180 nm and 250 nm 5521 and 5529 GA families and 5503 and 5507 small scale integration ULA families are presented. These GA and ULA form a group of families with a common library of functional cells, similar design tools and types of packages. Their distinctive feature is high resistance to space conditions.

Микроэлектроника является одной из отраслей промышленности, определяющих научно-технический прогресс общества. Большинство процессов, связанных с развитием микроэлектроники, носит выраженный экспоненциальный характер. В отличие от обычных отраслей промышленности, где создание более быстрого и лучшего устройства с удвоенными функциональными возможностями обычно удваивает стоимость разработки и производства изделия, в микроэлектронике справедливо обратное: переход на новые (меньшие) технологические нормы приводит к удешевлению с одновременным увеличением функциональных возможностей интегральных микросхем.

В этих условиях актуальна задача ускорения темпов разработки электронной компонентной базы (ЭКБ) для современной радиоэлектронной аппаратуры (РЭА), в особенности – больших интегральных схем (БИС), которые можно разделить на два основных класса: универсальные и специализированные. К первому классу относятся микропроцессоры, микроконтроллеры, периферийные устройства, устройства памяти (ПЗУ, ОЗУ и т.д.), серии стандартных микросхем и др., то есть микросхемы, функциональные возможности которых носят универсальный характер и могут быть использованы в различных устройствах и системах. Объем производства микросхем данного класса составляет сотни тысяч и миллионы штук в год, что минимизирует затраты на их проектирование и освоение в производстве.

[1] НПК "Технологический центр" / SMC "Technological Centre".

Специализированные микросхемы выполняют в аппаратуре конкретные специфические функции, присущие только ей, и в большинстве случаев не могут быть использованы где-либо еще. С завершением производства аппаратуры исчезает потребность и в выпуске предназначенных для нее специализированных микросхем. Как правило, серийность специализированных микросхем напрямую связана с объемом выпуска аппаратуры, в которой они применяются. Существует большая номенклатура специализированных микросхем с огромными объемами выпуска, например БИС, применяемые в автомобильной электронике, бытовой и компьютерной технике и др. При производстве таких микросхем затраты на их проектирование и организацию массового выпуска легко окупаются. Это наиболее рентабельный сектор рынка микроэлектроники.

Однако в современном обществе существует потребность в тысячах типов специализированных микросхем, которые выпускаются для удовлетворения нужд отдельных отраслей промышленности и конкретных типов РЭА. Объем производства таких микросхем может составлять от нескольких десятков до нескольких тысяч штук в год. Способность разрабатывать и производить их во многом определяет научно-технический и оборонный потенциал страны. Не случайно в санкционный список США против России попали крупнейшие предприятия отечественной микроэлектроники АО "Ангстрем" и ПАО "Микрон", являющиеся флагманами в производстве специализированных БИС.

Особую, наиболее сложную группу среди специализированных микросхем составляют БИС, применяемые в аппаратуре космического назначения и эксплуатируемые в условиях действия жестких внешних воздействующих факторов (ВВФ). Как правило, номенклатура таких микросхем велика, сроки разработки аппаратуры ограничены, а серийность, в силу специфики аппаратуры, часто не превышает нескольких сотен изделий в год. Производство, как правило, имеет прерывистый характер, а основной вклад в стоимость микросхем вносят затраты на освоение производства и проведение квалификационных и периодических испытаний для подтверждения уровня качества.

Современные специализированные микросхемы можно разделить на три группы: заказные микросхемы, программируемые логические интегральные схемы (ПЛИС) и полузаказные БИС на основе базовых (БК) или базовых матричных кристаллов (БМК). Принято считать, что полностью заказные микросхемы обеспечивают максимальную функциональность, надежность и стойкость к ВВФ, минимальную стоимость при

Microelectronics is one of the industries that determine scientific and technical progress of society. Most of the processes associated with the development of microelectronics have pronounced exponential character. Unlike conventional industries, where the creation of faster and better devices with enhanced functionality usually doubles the cost of development and production, in microelectronics the opposite is true: the transition to a new (smaller) technological standards leads to reduction in price with simultaneous increasing functionality of integrated circuits.

In these circumstances, it is urgent to accelerate the development of electronic component base (ECB) for modern electronic equipment (EE), especially of very large scale integrated circuits (VLSIC), which can be divided into two basic classes: generic and application-specific. The first class includes microprocessors, microcontrollers, peripheral devices, storage devices (ROM, RAM, etc.), a series of standard chips, etc., that is, versatile chips, which can be used in various devices and systems. The production volume of chips of this class reaches hundreds of thousands and millions of pieces per year

that minimizes the contribution to their cost of design and development.

Application-specific integrated circuit (ASIC) performs specific functions inherent only to a certain type of equipment, and in most cases can't be used anywhere else. After the end of production of such equipment, there is no need in ASIC intended for it. As a rule, the volume of production of ASICs is directly tied to volume of production of equipment in which they are applied. There is a large range of ASICs with huge production volumes, for example, VLSICs for automotive electronics, household and computer equipment

массовом производстве, но экономически не эффективны при малых объемах выпуска, так как требуют максимальных затрат при разработке и освоении производства. ПЛИС обладают преимуществами при разработке и отладке проекта микросхемы в составе аппаратуры. В то же время наличие дополнительных элементов для программирования снижает их надежность и увеличивает энергопотребление. По сравнению с заказными БИС стоимость ПЛИС существенно выше. Полузаказные БИС занимают промежуточное положение между полностью заказными микросхемами и ПЛИС. По показателям надежности, энергопотребления и стойкости к ВВФ они сравнимы с заказными БИС, а по длительности цикла "разработка – изготовление – поставка" сопоставимы с ПЛИС. Производство БМК и БК, как правило, поддерживается в течение длительного времени (более 15 лет). Дополнительно необходимо учитывать, что ПЛИС военного и космического назначения (уровней качества Military и Space) из-за введенного эмбарго в Россию не поставляются.

Выбор способа реализации специализированных БИС определяется множеством факторов, но, как правило, именно полузаказные БИС обеспечивают наилучшее соотношение эксплуатационных и экономических показателей. Рассмотрим особенности БМК и БК, как основы для реализации специализированных микросхем.

КОНСТРУКЦИЯ БМК

Базовый матричный кристалл (БМК) (англоязычные термин ULA, Uncommited Logic Array) – это универсальная заготовка в виде кремниевой пластины, на которой сформированы кристаллы с матрицей транзисторных структур. Такие кристаллы называют базовыми, поскольку все фотошаблоны для их изготовления, за исключением слоев металлизации, являются постоянными и не зависят от реализуемой схемы. Простейшие элементы (КМОП-транзисторы) располагаются в виде регулярной матрицы, поэтому кристалл называют матричным. В отличие от ПЛИС, логика работы которых задается посредством программно-управляемых элементов, специализация БМК формируется технологически в процессе микроэлектронного производства. Изготовление конкретной БИС заключается в выполнении завершающих технологических операций над кремниевыми пластинами с кристаллами-заготовками БМК. При этом в одном или нескольких слоях металлизации осуществляется коммутация КМОП-транзисторов на поле матрицы для формирования цепей схемы. В сравнении с ПЛИС в структуре БМК отсутствуют избыточные элементы, что в несколько раз снижает общую сложность микросхемы и повышает ее надежность.

В конструкции БМК можно выделить регулярное поле, окруженное областью периферийных контактов. Для определения размера поля БМК

etc. The costs of design and organization of mass production of such chips are easy to pay off. It is the most profitable sector of the market of microelectronics.

However, in modern society there is a need for thousands of types of ASICs, which are produced to meet the needs of specific industries and specific types of electronics. The production volume of such circuits can range from a few dozen to several thousand pieces per year. Ability to develop and produce them largely determines the scientific, technical and defence potential of the country. It is not coincidentally that the sanctions list of the USA against Russia includes the largest enterprises of the domestic microelectronics – Angstrem and Mikron, which are the flagships in the production of specialized VLSICs.

VLSICs, which are used in space equipment and operated under the influence of hard external factors, constitute a special, most complex group among ASICs. Usually, the range of such chips is large, the development time of equipment is limited, and seriality, due to the nature of the equipment, often does not exceed several hundred units per year. Production, as a rule, is intermittent, and the main parts of the cost of the chips are costs of the development of production and expenses of certification and periodic tests for confirmation of the quality level.

Modern ASICs can be divided into three groups: custom IC, field-programmable gate array (FPGA) (FPGA) and semicustom IC based on gate array (GA) or uncommitted logic array (ULA). It is considered that the fully custom chips provide maximum functionality, reliability and

используется понятие "эквивалентный вентиль". Один эквивалентный вентиль соответствует четырем КМОП-транзисторам, на которых можно реализовать логическую функцию "2И-НЕ" или "2ИЛИ-НЕ". При этом необходимо различать фактический размер поля и количество эквивалентных вентилей, которые могут быть использованы при реализации конкретной микросхемы. Отношение использованных эквивалентных вентилей к размеру поля БМК называется коэффициентом заполнения.

Сложность реализуемых на БМК микросхем определяется многими факторами: размером поля БМК, количеством доступных для использования внешних контактов, эффективностью средств проектирования, развитостью библиотеки функциональных ячеек, их быстродействием, возможностями охлаждения микросхем в аппаратуре и многими другими. На практике не удается использовать все 100% поля БМК. При заполнении поля кристалла менее чем на 70%, как правило, удается спроектировать топологию автоматически средствами САПР без вмешательства разработчика. При большем коэффициенте заполнения топология разрабатывается в интерактивном режиме с участием разработчика. Это усложняет процесс проектирования, но позволяет использовать кристалл меньшего размера, производство которого будет дешевле. Поэтому обычно БМК разрабатываются сериями. Серию составляют несколько конструктивно подобных БМК, имеющих общую библиотеку функциональных ячеек и различающихся размером поля кристалла и количеством внешних выводов. Для каждого большего по размеру типа БМК в серии размер поля обычно увеличивается примерно вдвое. Серии БМК также могут состоять из одного типоразмера кристалла, изготавливаемого в различных типах корпусов.

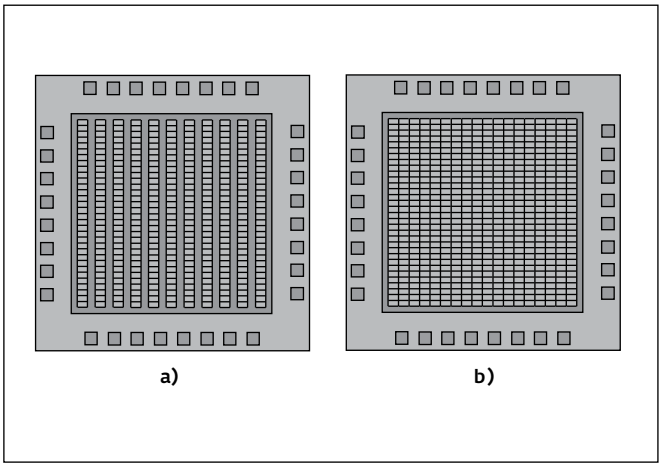

Рис.1. Варианты конструкций БМК: a – канальная; b – "море вентилей"

Fig.1. Variants of ULA design: a – row structure; b – sea of gates

Конструкция БМК, как правило, строится на 4-транзисторных базовых ячейках. Подобные ячейки позволяют эффективно использовать ресурсы БМК и реализовывать любые схемотехнические решения. Однако встречаются БМК

resistance to external factors, the minimum cost for mass production, but are not cost effective at low production volumes, as they require the maximum cost in the design and development of production. FPGAs have advantages in the development and debugging of the circuits project in the equipment. At the same time, the additional elements for programming reduce their reliability and increase power consumption. Compared to the custom VLSICs, the cost of FPGAs is significantly higher. Semicustom VLSICs occupy an intermediate position between a fully custom chips and FPGAs. In terms of reliability, power consumption, and resistance to external factors, they are comparable to custom VLSICs, and in terms of the duration of "development – production – supply" cycle they are comparable to FPGA. The production of GA and ULA, as a rule, is maintained for a long time (over 15 years). Additionally, it is necessary to consider that the FPGAs for military and space purposes (of Military and Space quality levels) are not supplied to Russia due to an embargo.

The choice of the method of implementation of specialized VLSICs depends on many factors, but, as a rule, the semicustom chips provide the best balance of operational and economic performance. Let's consider the features of GA and ULA as the basis for the implementation of ASICs.

DESIGN OF ULA

Uncommited logic array (ULA) is a versatile workpiece in the form of a silicon wafer with the chips with a matrix of transistor structures. All photomasks for the manufacture of such chips, except for metallization layers,

с разногабаритными ячейками или с регулярно повторяющимися транзисторными структурами.

По конструкции поля наибольшее распространение получили БМК, имеющие "канальную" организацию и БМК типа "море вентилей". При канальной организации поле БМК представляет собой последовательность столбцов или строк ячеек и каналов для трассировки (рис.1a). При использовании организации "море вентилей" поле БМК представляет собой сплошную регулярную структуру однотипных ячеек (рис.1b).

КОНСТРУКЦИЯ БК

БМК свойственны существенные ограничения, которые обусловлены применением однотипных транзисторов, предназначенных для построения схем цифровой обработки, но не позволяющих реализовывать сложные аналоговые и другие схемы, имеющие какие-либо особенности.

Указанный недостаток устраняется при применении базовых кристаллов. Современный БК имеет фиксированную периферийную область, как правило, совпадающую с периферийной областью БМК, но в поле БК фиксируются только цепи организации системы питания микросхемы. Это позволяет создавать на поле БК как матрицы различных цифровых транзисторов, аналогичные БМК, так и другие схемы (рис.2). Следует отметить, что БМК является фактически частным случаем БК, когда все поле последнего занято ячейками цифровых транзисторов.

Возможность реализации на поле БК матриц транзисторов различной мощности позволяет повысить частоту срабатывания триггеров более чем в два раза, что обеспечивает повышение системной частоты обработки информации, а также минимизирует площадь схемы.

Обычно с привязкой к конструкции БМК и БК создаются сложно-функциональные блоки (СФ-блоки), которые реализуют различные функции, такие как микропроцессорные ядра, микроконтроллеры, блоки памяти, интерфейсные блоки, блоки аналого-цифровой обработки и многие другие. Очень важно, что библиотека СФ-блоков может создаваться постепенно в процессе эксплуатации серии БМК и БК, как дополнительный результат проектирования конкретных БИС, а применение отработанных, прошедших экспериментальное апробирование СФ-блоков позволяет повысить качество разработки и сократить затраты на стадии проектирования микросхемы.

Следует отметить, что современные конструктивно-технологические базисы как на объемном кремнии, так и на структурах "кремний на изоляторе" позволяют создавать БК с повышенной устойчивостью к ВВФ, в том числе для аппаратуры космического назначения.

Таким образом, БК и БМК наиболее перспективны для создания специализированных

are constant and do not depend on the implemented scheme. The simplest elements (CMOS transistors) are arranged in a regular array. Unlike FPGAs, the logic of which is set by software-controlled items, the specialization of ULA is technologically formed in the process of microelectronic production. Production of specific VLSIC consists in accomplishment of the final manufacturing operations on silicon wafers with ULAs. The CMOS transistors on the array are switched in one or more layers of metallization for the formation of the circuit. Compared to FPGAs, the structure of ULA does not contain redundant elements, which greatly reduces the overall complexity of the circuit and increases its reliability.

ULA includes floor surrounded by the region of the peripheral contacts. To define the size of the ULA the concept of "equivalent gate" is used. One equivalent gate corresponds to the four CMOS transistors which can realize 2AND-NOT or 2OR-NOT logical functions. It is necessary to distinguish between the actual ULA size and the number of equivalent gates that can be used to implement ASIC. The ratio of used equivalent gates to the size of ULA is the fill factor.

The complexity of chips that are implemented on the ULA is determined by many factors: the size of ULA, the amount of external contacts, efficiency of design tools, level of the library of functional cells and their performance, cooling capabilities in hardware, and many others. In practice we cannot use 100% of the ULA area. When fill factor is less than 70%, as a rule, it is possible to design the topology automatically by CAD tools without the participation of the developer. In case of a larger fill

микросхем, особенно с повышенными требованиями к надежности в жестких условиях эксплуатации. Рассмотрим современные серии БК 5521 и 5529 [1–4], изготовленные по технологическим нормам 180 нм и 250 нм, а также БМК малой степени интеграции серий 5503 и 5507. Указанные БК и БМК составляют семейство серий, имеющих единую библиотеку функциональных ячеек, общие средства проектирования и аналогичные корпусные исполнения. Отличительной чертой семейства является повышенная стойкость к ВВФ космического пространства.

СЕМЕЙСТВО СЕРИЙ БМК / БК 5521 И 5529

Серии БМК и БК 5529 изготавливаются по КМОП-технологии с нормами 0,25 мкм на структурах "кремний на изоляторе" (КНИ), а серия БК 5521 – с технологическими нормами 0,18 мкм на объемном кремнии. Напряжение питания составляет 3 В ±10% или 3,3 В ±10%, расчетное время задержки на вентиль – 100 пс, тактовая частота D-триггера в счетном режиме – 500 МГц.

БМК серии 5529 соответствуют требованиям ОСТ В 11 0998, освоены в производстве НПК "Технологический центр" с изготовлением кристаллов микросхем на заводе "Микрон", входят в перечень изделий, разрешенных к применению МОП 44 001.02. В 2017 году будут завершены ОКР по освоению в производстве десяти типов БК серий 5529 и 5521. Повышенная устойчивость микросхем к воздействию одиночных заряженных частиц обеспечивается для серии 5529 конструктивно-технологическим базисом КНИ, а для серии 5521 – применением троированных триггеров.

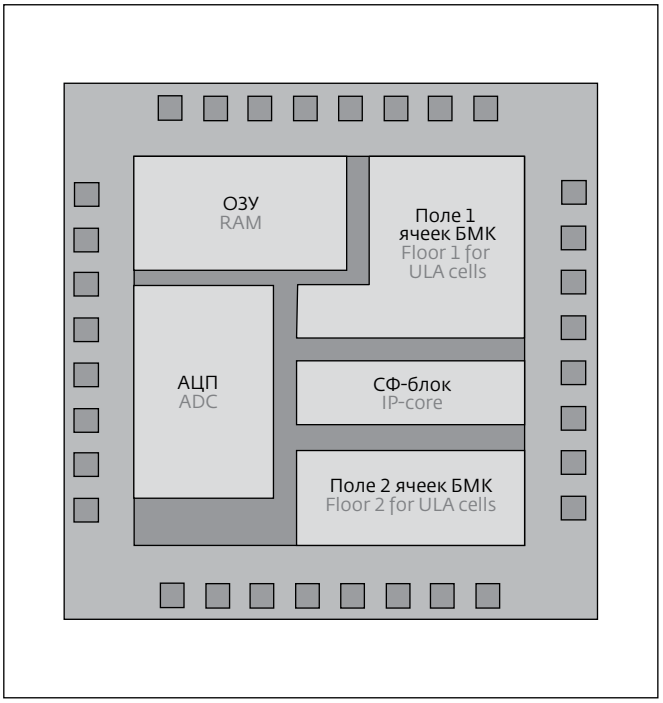

Рис.2. Конструкция БК
Fig.2. Design of GA

Состав и основные технические характеристики БМК и БК серий 5529 и 5521 приведены в табл.1.

factor the topology is designed in an interactive mode with the participation of the developer. This complicates the design process, but allows the use of smaller chip size, the production of which will be cheaper. So typically the families of ULAs are developed. The family includes several structurally similar ULAs with a common library of functional cells and different size of the floor and number of external contacts. For each larger type of ULA in family the floor size usually increases approximately twice. The ULA family can also consist of one size of the chip manufactured in different types of packages.

The ULA design is usually based on a 4-transistor cells. These cells allow to efficient use the resources of ULA and to implement any circuit solution. However, the ULA may include cells of different sizes or regularly repeated transistor structures.

The most widely used ULAs have row or sea-of-gates structure. ULA with row structure consists of a sequence of columns or rows of cells and channels for the wiring (Fig.1a). ULA of sea-of-gates type has a regular structure of identical cells (Fig.1b).

DESIGN OF GA

ULAs are characterized by significant limitations, which are caused by the use of similar transistors that are intended to build circuits of digital processing, but does not allow to implement complex analog and other circuits with special features.

This drawback is eliminated by the use of the GA. Modern GA has a fixed peripheral area, usually coinciding with the peripheral area of ULA, but in GA only chains of power supply of the

Таблица 1. Состав и основные характеристики БК серий 5529 и 5521
Table 1. Specifications of 5529 and 5521 GA families

Условное обозначение БК Abbreviation of GA		Тип корпуса Type of package	Количество внешних / информационных контактов Number of external / information contacts	Размер поля, тыс. эквивалентных вентилей Floor size, thousands of equivalent gates
Серия 5521 5521 family	Серия 5529 5529 family			
5521ТР01	5529ТР01	МК 5123.28-1.01	28 / 26	39
5521ТР02	5529ТР02	МК 4217.44-1	44 / 40	73
5521ТР03	5529ТР03	МК 4217.44-1	44 / 40	200
		МК 4239.68-2	68 / 64	
5521ТР04	5529ТР04	МК 4239.68-2	68 / 64	400
		МК 4247.100-2	100 / 88	
5521ТР05	5529ТР05	МК 4247.100-2	100 / 88	800
		МК 4248.144-3	144 / 120	
5521ТР06	5529ТР06	МК 4248.144-3	144 / 120	985
		МК 4249.176-1	176 / 152	
5521ТР07	5529ТР07	МК 4249.176-1	176 / 152	1 315
		МК 4250.208-1	208 / 184	
5521ТР08	5529ТР08	МК 4250.208-1	208 / 184	1 810
		МК 4245.240-7	240 / 208	
5521ТР09	5529ТР09	МК 4245.240-7	240 / 208	2 765
		МК 4244.256-4	256 / 224	
		МК 4251.304-1	304 / 272	
5521ТР10	5529ТР10	МК 4251.304-1	304 / 272	4 240
		МК 4254.352-1	352 / 288	

chip are fixed. This allows to create on the base of GA not only arrays of different digital transistors similar to ULA, but also other circuits (Fig.2).

It should be noted that ULA is actually a special kind of GA, when all the area is occupied by cells of the digital transistors.

The possibility of implementation in GA of the arrays of transistors of different power allows to increase the frequency of the triggers more than twice, which enhances the system frequency of information processing, and also minimizes the area of the circuit.

Usually ULA and GA create a basis for IP cores that implement various functions, such as microprocessor cores, microcontrollers, memory blocks, interface blocks, analog-to-digital processing and many others. It is very important that the library of IP Cores may be created gradually in the process of operation of the ULA and GA families, as an additional result of the designing of specific VLSICs, and the use of proven IP Cores allows to improve the quality of development and to reduce the costs of design of the chip.

It should be noted that the up-to-date technological basis both on bulk silicon and silicon on insulator structures allow to create the GA with increased resistance to external factors, including for equipment for space applications.

Thus, ULA and GA are the most promising solutions for the creation of ASICs, especially with high requirements for reliability in harsh environments. Let's consider the modern 180 nm and 250 nm 5521 and 5529 GA families [1–4], and small scale integration 5503 and 5507 ULA families. These GA and ULA

Таблица 2. Состав и основные характеристики БМК серий 5503 и 5507
Table 2. Specifications of 5503 and 5507 ULA families

Условное обозначение БМК Abbreviation of ULA		Тип корпуса Type of package	Количество внешних / информационных контактов Number of external / information contacts	Размер поля, эквивалентных вентилей Floor size, equivalent gates
Серия 5503 5503 family	Серия 5507 5507 family			
Н5503ХМ1	5507БЦ1У	Н09.28-1В	28 / 26	576
5503ХМ1У	5507БЦ1У1	МК 5123.28-1.01		
Н5503ХМ2	5507БЦ2У	Н14.42-1В	42 / 40	1 296
Н5503ХМ5	5507БЦ5У	Н18.64-1В	64 / 62	3 072
5503ХМ5Т	5507БЦ5Т	МК 4239.68-2		
5503БЦ7У	5507БЦ7У	Н18.64-1В	64 / 60	5 478
5503БЦ7Т	5507БЦ7Т	МК 4239.68-2	68 / 64	

СЕРИИ БМК 5503 И 5507

БМК 5503 и 5507 являются сериями малой степени интеграции и уже более 15 лет широко применяются в аппаратуре космического назначения. На основе БМК данных серий разработано более 500 типов БИС, в том числе для таких космических аппаратов и кораблей как "Прогресс-М", "Союз-ТМА", "Меридиан", "Лабиринт", "Пион", "Аркон-2", "Электра", "Луч", "ГЛОНАСС-М", "ГЛОНАСС-К", "Кондор", "Экспресс", для системы управления разгонным блоком "Бриз-М" и др.

Серии 5503 и 5507 являются полными конструктивными аналогами, изготавливаются по КМОП-технологии с нормами 1,6 мкм и состоят из четырех типоразмеров БМК каждая, выпускаемых в различных типах корпусов. Напряжение питания серий 5503 и 5507 составляет 5 В ±10% и 3 В ±10%, среднее время задержки на вентиль – не более 2 нс и не более 3 нс соответственно.

Состав и основные технические характеристики БМК этих серий приведены в табл.2.

Серии БМК 5503 и 5507 имеют единую библиотеку ячеек [5] с универсальной системой обозначений, которая состоит из трех частей:

- библиотека базовых ячеек (5503), которая включает все основные группы логических элементов, а также периферийные элементы, обеспечивающие функции входа, выхода и входа-выхода цифровых и аналоговых

form a group of families with a common library of functional cells, similar design tools and types of packages. Their distinctive feature is high resistance to space conditions.

5521 AND 5529 ULA/GA FAMILIES

ULA and GA of 5529 family are manufactured using 0.25 µm CMOS technology on the silicon on insulator (SOI) structures, and 5521 GA family – using 0.18 µm technology on bulk silicon. The supply voltage is 3 V ±10% or 3.3 V ±10%, the estimated delay time per gate is 100 ps, clock frequency of the D-type flip-flop in the counting mode is 500 MHz.

5529 ULA family meet the requirements of the ОСТ В 11 0998, are produced by SMC "Technological Centre" with the manufacture of chips at Mikron plant, and are included in the list of products permitted for use by МОП 44 001.02. In 2017, the production of ten types of GA of 5529 and 5521 families will be launched. Increased resistance to the single charged particles is provided for 5529 family by the use of SOI technology, and for 5521 family – by the use of triplicated triggers.

Specifications of 5529 and 5521 ULA/GA families are shown in table.1.

5503 AND 5507 ULA FAMILIES

Small scale integration 5503 and 5507 ULA families are more than 15 years widely used in equipment for space applications. ULAs of this families are a base for more than 500 types of VLSICs including such spacecraft and ships as Progress-M, Soyuz-TMA, Meridian, Labyrinth, etc.

5503 and 5507 families have the same design and are manufactured by 1.6 µm CMOS technology. Each family consist

сигналов, пассивное или активное доопределение внешнего контакта;
- библиотека цифро-аналоговых ячеек (5503+), позволяющих реализовать аналого-цифровую обработку сигналов;
- библиотека специальных ячеек (5503++), разработанных по специфическим требованиям различных заказчиков (сторонним заказчикам не предоставляется).

Разработка БИС выполняется на отечественной системе автоматизированного проектирования "Ковчег 3.0" [6]. В состав САПР входят все основные подсистемы, необходимые для разработки и подготовки к производству полузаказной БИС. Полная промышленная версия САПР "Ковчег 3.0" [6] доступна для свободного копирования (www.asic.ru), что позволяет создать на любом предприятии или в вузе полноценные рабочие места для проектирования БИС на БМК серий 5503 и 5507. Разработанные БИС могут быть изготовлены на микроэлектронном производстве НПК "Технологический центр" (www.tcen.ru).

Статья подготовлена при финансовой поддержке Минобрнауки России. Уникальный идентификатор ПНИ RFMEFI57814X0061.

ЛИТЕРАТУРА

1. **Басаев А.С., Денисов А.Н., Коняхин В.В., Мальцев П.П.** Специализированные интегральные микросхемы космического применения на основе базовых матричных кристаллов // Петербургский журнал электроники. 2008. №1. С. 34–39.
2. **Денисов А.Н., Коняхин В.В.** Разработки НПК "Технологический центр" для применения в аппаратуре космического назначения // Международная конференция "Микроэлектроника 2015". Интегральные схемы и микроэлектронные модули: проектирование, производство и применение : Сб. тезисов. – М.: ТЕХНОСФЕРА, 2015. С. 74–77.
3. **Денисов А.Н. Коняхин В.В.** Семейство серий БМК НПК "Технологический центр" // Международная конференция "Микроэлектроника 2015". Интегральные схемы и микроэлектронные модули: проектирование, производство и применение : Сб. тезисов. – М.: ТЕХНОСФЕРА, 2015. С. 104–112.
4. **Коняхин В.В., Денисов А.Н., Федоров Р.А.** и др. Микросхемы для аппаратуры космического назначения : Практ. пособие / Под общ. ред. А.Н.Саурова. – М.: ТЕХНОСФЕРА, 2016. 388 с.
5. **Денисов А.Н., Фомин Ю.П., Коняхин В.В., Федоров Р.А.** Библиотека функциональных ячеек для проектирования полузаказных микросхем серий 5503 и 5507 / Под ред. А.Н. Саурова. – М.: ТЕХНОСФЕРА, 2012. 304 с.
6. **Гаврилов С.В., Денисов А.Н., Коняхин В.В.** Система автоматизированного проектирования "Ковчег 2.1" / Под ред. Ю.А.Чаплыгина. – М.: Микрон-Принт, 2001. 194 с.

of four standard sizes of ULA, which are manufactured in different types of packages. The supply voltage is 5 V ±10% or 3 V ±10%, the average delay time per gate is no more than 2 ns and no more than 3 ns, respectively.

Specifications of these ULA families are shown in table.2.

5503 and 5507 ULA families have a common library of cells [5] with the universal system of notation, which consists of three parts:
- library of core cells (5503), which includes all major groups of logic elements and peripheral elements that provide the functions of input, output and input/output of digital and analog signals, passive or active assignment of external contact;
- library of digital-to-analog cells (5503+) allowing to implement the analog-to-digital processing of signals;
- library of special cells (5503++) developed for the specific requirements of different customers (not available for outside customers).

VLSICs are developed using domestic Covcheg 3.0 CAD [6]. CAD includes all main subsystems for development and pre-production of semicustom VLSIC. Full industrial version of CAD is available for free copying (http://www.asic.ru) that allows to create in any enterprise or institution full-featured workplaces for development of VLSIC on 5503 and 5507 ULA families. Developed VLSICs can be manufactured by SMC "Technological Centre" (http://www.tcen.ru).

This paper was created with the financial support of the Ministry of Education and Science of the Russian Federation. Unique identifier RFMEFI57814X0061.

СОВРЕМЕННЫЕ МИКРОСХЕМЫ МАЛОЙ СТЕПЕНИ ИНТЕГРАЦИИ ДЛЯ АППАРАТУРЫ КОСМИЧЕСКОГО НАЗНАЧЕНИЯ

UP-TO-DATE SMALL SCALE INTEGRATION CHIPS FOR SPACE APPLICATIONS

УДК 621.382, ВАК 05.27.01, DOI:10.22184/1993-8578.2016.70.8.32.38

В.Коновалов, В.Коняхин*, С.Бражников* / V.Konovalov@tcen.ru, V.Koniakhin@tcen.ru, S.Brazhnikov@tcen.ru*
V.Konovalov, V.Koniakhin*, S.Brazhnikov**

Представлены две серии микросхем малой степени интеграции, разработанные на основе базового кристалла 5529ТР015: серия многофункциональных микросхем стандартной логики и серия цифро-аналоговых микросхем для организации дифференциальной линии связи LVDS и LVDM. Приведены основные характеристики микросхем и состав реализованных в них функций.

This article describes two series of small-scale integration chips developed on the basis of 5529TP015 structured application specific integrated circuit: a series of standard logic multifunctional integrated circuits and a series of digital-analog integrated circuits for LVDS and LVDM differential communication line buildup. It presents the basic characteristics of the microcircuits and the list of functions implemented wherein.

Микросхемы малой степени интеграции более 30 лет широко использовались в качестве основных компонентов при проектировании цифровых устройств. Однако в настоящее время их применение в цифровых устройствах существенно сократилось. На смену микросхемам малой степени интеграции пришли ПЛИС, микроконтроллеры, сигнальные процессоры и другие специализированные микросхемы, позволяющие создавать гораздо более совершенные и технически более сложные изделия.

При проектировании аппаратуры довольно часто возникают проблемы согласования сигналов между микросхемами. В подобных случаях применение больших интегральных схем, таких как ПЛИС, может быть не целесообразным. Для этих задач в настоящее время широко используются микросхемы согласующей логики в микроминиатюрных корпусах. В большинстве своем это микросхемы инверторов или логических элементов с малым количеством входов. Серии таких микросхем малой степени интеграции занимают свою нишу на рынке микроэлектроники, имеют широкую номенклатуру и в больших количествах выпускаются для коммерческого и промышленного применений.

Для создания особо надежной аппаратуры специального и космического назначения с длительным сроком эксплуатации без возможности ремонта требуются микросхемы военного или космического уровня качества. При ее разработке и производстве вся применяемая электронная компонентная база подвергается дополнительным отбраковочным испытаниям (ДОИ). ДОИ – это длительные и дорогостоящие испытания, которые проводятся для каждой партии и каждого типа микросхем. Соответственно, чем шире номенклатура применяемых в аппаратуре микросхем, тем существеннее затраты на ДОИ. При этом, потребность в микросхемах малой степени интеграции, как правило, мала (единицы, десятки штук), однако их номенклатура может быть значительной.

* НПК "Технологический центр" / SMC "Technological Centre".

Перечисленные выше факторы говорят о необходимости создания функционально гибких, универсальных микросхем, способных выполнять функции схем малой степени интеграции и имеющих высокую надежность для применения в аппаратуре космического назначения.

МНОГОФУНКЦИОНАЛЬНЫЕ МИКРОСХЕМЫ МАЛОЙ СТЕПЕНИ ИНТЕГРАЦИИ

В НПК "Технологический центр" на основе младшего типа базового кристалла серии 5529 были разработаны две многофункциональные цифровые микросхемы 5529ТР015-674 и 5529ТР015-675 для аппаратуры космического назначения, позволяющие заменить большинство типов микросхем малой степени интеграции.

При проектировании многофункциональных микросхем необходимо было достигнуть компромисса между функциональной гибкостью

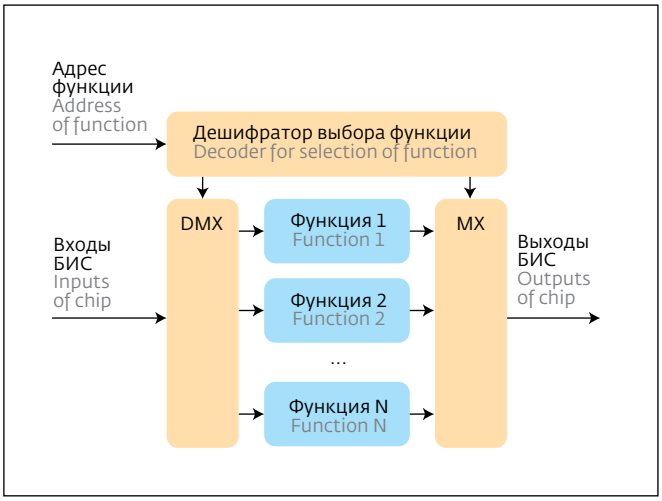

Рис.1. Структурная схема БИС 5529ТР015-674 и 5529ТР015-675

Fig.1. Block diagram of 5529TP015-674 and 5529TP015-675 chips

Small-scale integration chips for over 30 years has been widely used as key components in the design of digital devices. At present, however, their application in digital devices have declined significantly. FPGA, microcontrollers, signal processors and other specialized chips that allow to create much more sophisticated and technically more complex products, replaced the small-scale integration chips.

A problem often encountered in the design of the equipment is the coordination of signals between chips. In such cases, the use of large scale integrated circuits, such as FPGAs, may not be appropriate. For this purpose, matching chips in microminiature packages are widely used. The majority of these chips are inverters or logic elements with a small number of inputs. Wide range of such small-scale integration chips occupy a special niche in the market of microelectronics, and in large numbers are manufactured for commercial and industrial applications.

The development of highly reliable equipment for special and space applications with a long service life without repair requires chips of military or space level of quality. During its development and production all electronic components are subjected to additional screening tests. It is a long and costly tests, which are conducted for each batch and each type of chip. Accordingly, the wider range of chips is used in equipment, the greater are the cost of the screening tests. At the same time, the need for small-scale integration chips is usually small (units or tens of units), but their diversity may be significant.

These factors indicate the need to create functionally flexible, versatile chips, which would be capable to perform the functions of the small-scale integration chips and would have the high reliability for use in equipment for space applications.

MULTIFUNCTION SMALL-SCALE INTEGRATION CHIPS

SMC "Technological Centre" has developed on the basis of lower type of 5529 gate array two multifunctional digital circuits – 5529TP015-674 and 5529TP015-675, which are intended for equipment for space applications and can replace most types of small-scale integration chips.

When designing circuits, it was necessary to reach a compromise between functional flexibility and ease of implementation. The selection of the function is implemented by means of decoding of its address, which is set by the connection of specific external pins of the chip to "power" or "ground". Block diagram of multifunction chip is shown in Fig.1. Address of the configured function is transferred to the decoder of function selection. The outputs of the decoder multiplex the inputs and outputs of the chip to the unit that implements the corresponding function. This method is quite simple and secure as it doesn't use memory cells for configuring ship. The number of possible functions realizable with this method of configuration is equal to 2^N,

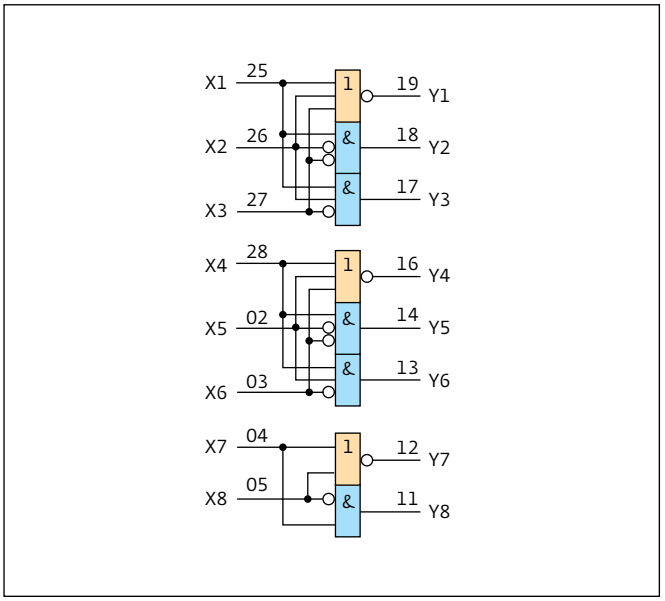

Рис.2. Схема и логические функции выходов микросхемы 5529ТР015-675 при выполнении функции "054"

Fig.2. Diagram and logic functions of outputs of 5529TP015-675 chip when "054" function is executed

и простотой реализации. Был применен способ выбора функции с помощью дешифрации ее адреса, задаваемого подключением к "питанию" или "земле" специальных внешних выводов микросхемы. Структурная схема БИС серии многофункциональных микросхем представлена на рис.1. Адрес сконфигурированной функции поступает на дешифратор выбора функции. Выходы дешифратора мультиплексируют входы и выходы микросхемы к блоку, реализующему соответствующую адресу функцию. Такой способ является достаточно простым и надежным, так как не использует ячейки памяти для конфигурирования микросхемы. Количество возможных реализуемых функций при таком способе конфигурирования равно 2^N, где N – количество адресных выводов, что обеспечивает достаточную функциональную гибкость. Также важными характеристиками микросхем серии являются небольшие габариты, надежность работы и устойчивость к воздействию специальных факторов.

Для определения набора функций, планируемых для реализации в микросхеме 5529ТР015-674, был проведен анализ серий 54(74), 4000 и отечественных микросхем малой степени интеграции. На основании результатов анализа были выбраны наиболее востребованные функции. Многофункциональная цифровая микросхема последовательностной логики 5529ТР015-674 имеет восемь информационных выходов, десять информационных и семь адресных входов и реализует 124 функции следующих типов:

- логические элементы и разветвители;
- цифровые компараторы;
- шифраторы;
- дешифраторы;
- мультиплексоры;

where N is the number of address pins that provides enough functional flexibility. Small size, reliability and resistance to influence of special factors are important characteristics of the chips of this family.

To determine the set of features planned for implementation in 5529TP015-674 chip, the analysis of 54 (74), 4000 families and domestic small-scale integration chips was carried out. The most popular functions were selected based on the results of the analysis. 5529TP015-674 multifunction digital sequential logic chip has eight data outputs, ten information and seven address inputs and implements 124 functions of the following types:

- logic elements and splitters;
- digital comparators;
- encoders;
- decoders;
- multiplexers;
- adders;
- composers;
- RS, D and JK flip-flops;
- registers;
- shift registers;
- Johnson counters;
- binary and binary-decimal counters.

Some chips of 74 family that have functions implemented in 5529TP015-674 chip are presented in the table.

Multifunction digital chip 5529TP015-675 511 implements 511 different combinational logic functions, has eight information outputs and also eight information and nine address inputs. The chip contains all the possible logic functions with two and three input variables, and potentially the most common functions with more variables [1]. Eight different matching functions are defined in one function for greater flexibility of the chip. The example below shows the logical functions that correspond to the configuration address "054" (a graphical image shown in Fig.2):

Таблица. Некоторые микросхемы 74-й серии, функционально реализованные в 5529ТР015-674
Some chips of 74 family, which are functionally implemented in 5529TP015-674 chip

Обозначение Designation	Краткое описание Brief description
74LS54	3-2-2-3-входная AND-OR логическая схема 3-2-2-3-input AND/OR inverter gate
74F74	Два D триггера Dual D-type flip-flop
74LS75	4-битный регистр D триггеров-защелок 4-bit bistable latches
74LS83	4-битный сумматор 4-bit adder
74LS85	4-битный компаратор с выработкой сигналов LT, GT, EQ 4-bit magnitude camparator
74LS95	4-битный сдвиговый регистр 4-bit shift register
74F112	Два JK-триггера Dual J-K negative edge-triggered flip-flop
74F113	Два JK-триггера Dual J-K negative edge-triggered flip-flop
74LS137	Дешифратор 3 в 8 с защелками на входе адреса 3-to-8 decoder with address latches
74F139	Два дешифратора 2 в 4 Dual 2-to-4 decoder
74LS147	Приоритетный шифратор 10 в 4 10-to-4 priority encoder
74LS148	Приоритетный шифратор 8 в 3 8-to-3 priority encoder
74LS153	Два мультиплексора 4 в 1 Dual 4-to-1 multiplexer
74LS157	Четыре мультиплексора 2 в 1 Quad 2-to-1 multiplexer
74LS158	Четыре мультиплексора 2 в 1 с инверсией Quad 2-to-1 multiplexer inverter
74LS161	4-разрядный двоично-десятичный счетчик 4-bit binary-decimal counter
74LS163	4-разрядный двоично-десятичный счетчик 4-bit binary-decimal counter
74LS164	8-битный сдвиговый регистр 8-bit shift register
74LS168	4-разрядный двоичный счетчик 4-bit binary counter
74LS170	Регистровая матрица 4×4 4×4 register file
74LS173	4-битный регистр с высокоимпедансным состоянием выходов 4-bit D-type register with 3-state outputs
74LS190	4-разрядный двоично-десятичный счетчик 4-bit binary-decimal counter
74LS194	4-битный универсальный сдвиговый регистр 4-bit bidirectional universal shift register
74LS195	4-битный универсальный сдвиговый регистр (JK управление) 4-bit parallel-access shift register

Обозначение Designation	Краткое описание Brief description
74LS240	Восемь инверторов с высокоимпедансным состоянием выходов Octal buffer/line driver with 3-state outputs
74LS241	Восемь буферов с высокоимпедансным состоянием выходов Octal buffer/line driver with 3-state outputs
74LS247	Дешифратор 4 в 7 для семисегментного индикатора BCD to 7-segment decoder
74LS248	Дешифратор 4 в 7 для семисегментного индикатора BCD to 7-segment decoder
74F256	Две 4-битные адресных защелки Dual 4-bit addressable latch
74LS257	4-разрядный мультиплексор 2 в 1 Quad 2-input multiplexer
74LS258	4-разрядный мультиплексор 2 в 1 с инверсией Quad 2-to-1 line multiplexer inverter
74LS259	8-битная адресная защелка 8-bit addressable latch
74LS273	8-битный регистр со сбросом 8-bit register with clear
74LS279	Четыре RS защелки Quad SR latch
74LS280	9-битный XOR/XNOR 9-bit odd/even parity generator/checker
74LS348	Приоритетный шифратор 8 в 3 с высокоимпедансным состоянием 8-input priority encoder with 3-state outputs
74F350	4-битная логика сдвига 4-bit shifter with 3-state output
74LS352	2-разрядный мультиплексор 4 в 1 Dual 4-input multiplexer
74F373	8-битный регистр защелок с высокоимпедансным состоянием Octal transparent latch with 3-state outputs
74F374	8-битный регистр с высокоимпедансным состоянием Octal transparent latch with 3-state outputs
74LS395	4-битный сдвиговый регистр с высокоимпедансным состоянием 4-bit shift register with 3-state outputs
74LS399	4-битный регистр с мультиплексированием входов Quad 2-input multiplexer
74F538	Дешифратор 3 в 8 с высокоимпедансным состоянием 1-to-8 decoder with 3-state outputs
74F539	Два дешифратора 2 в 4 с высокоимпедансным состоянием Dual 1-to-4 decoder with 3-state outputs

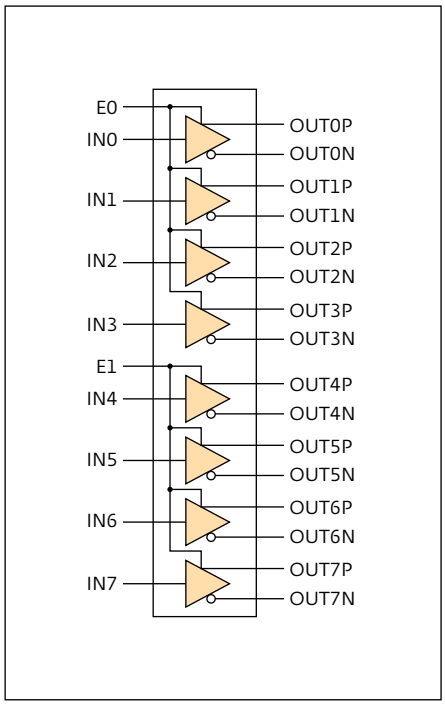

Рис.3. Функциональная схема микросхем 5529ТР015-688 и 5529ТР015-698
Fig.3. Functional diagram of 5529TP015-688 and 5529TP015-698 chips

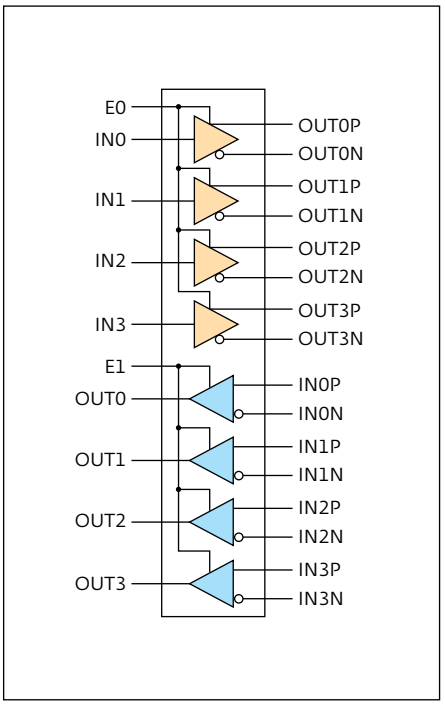

Рис.4. Функциональная схема микросхем 5529ТР015-689 и 5529ТР015-699
Fig.4. Functional diagram of 5529TP015-689 and 5529TP015-699 chips

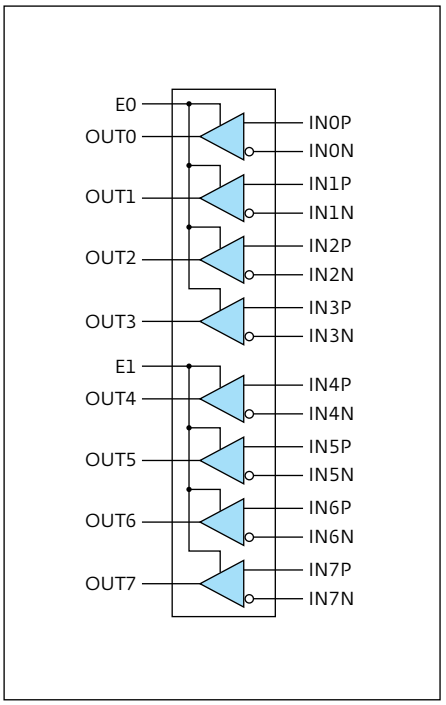

Рис.5. Функциональная схема микросхемы 5529ТР015-697
Fig.5. Functional diagram of 5529TP015-697 chip

- сумматоры;
- формирователи;
- RS, D и JK триггеры;
- регистры с записью по фронту и по уровню синхросигнала;
- сдвиговые регистры;
- счетчики Джонсона;
- двоичные и двоично-десятичные счетчики.

Некоторые микросхемы 74-й серии, функционально аналогичные реализованным в микро-

$Y1 = \overline{X1 + X2 + X3}$;
$Y2 = X1 \& \overline{X2} \& \overline{X3}$;
$Y3 = X1 \& X2 \& \overline{X3}$;
$Y4 = \overline{X4 + X5 + X6}$;
$Y5 = X4 \& \overline{X5} \& \overline{X6}$;
$Y6 = X4 \& X5 \& \overline{X6}$;
$Y7 = \overline{X7 + X8}$;
$Y8 = X7 \& \overline{X8}$.

CHIPS OF LVDS/LVDM TRANSMITTERS AND RECEIVERS

In addition to a multifunction chips, SMC "Technological Centre" has also developed a series of chips of receivers and transmitters for LVDS and LVDM standards of low-voltage differential signaling [2].

5529TP015-688 and 5529TP015-698 chips contains eight LVDS and eight LVDM transmitters, respectively. Their functional diagram is shown in Fig.3.

5529TP015-689 chip contains four LVDS transmitters and four LVDS/LVDM receivers; 5529TP015-699 chip – four LVDM transmitters and four LVDS/LVDM receivers. Functional diagram of 5529TP015-698 and 5529TP015-699 chips is shown in Fig.4.

5529TP015-697 chip contains eight LVDS/LVDM receivers. Its functional diagram is shown in Fig.5.

5529TP015-695 chip contains four M-LVDS half-duplex transceivers. Functional diagram of 5529TP015-695 chip is shown in Fig.6.

5529TP015-696 chip is a switch of two two-digit buses of LVDS/LVDM differential lines. This chip has a special input for control of the power of differential outputs, which allows to choose the mode that meets the standards LVDS or LVDM. Functional diagram of 5529TP015-696 chip is shown in Fig.7.

Full detailed description of 5529 gate array and chips presented in this article is given in the book [3]. ■

This paper was created with the financial support of the Ministry of Education and Science of the Russian Federation. Unique identifier RFMEFI57815X0104.

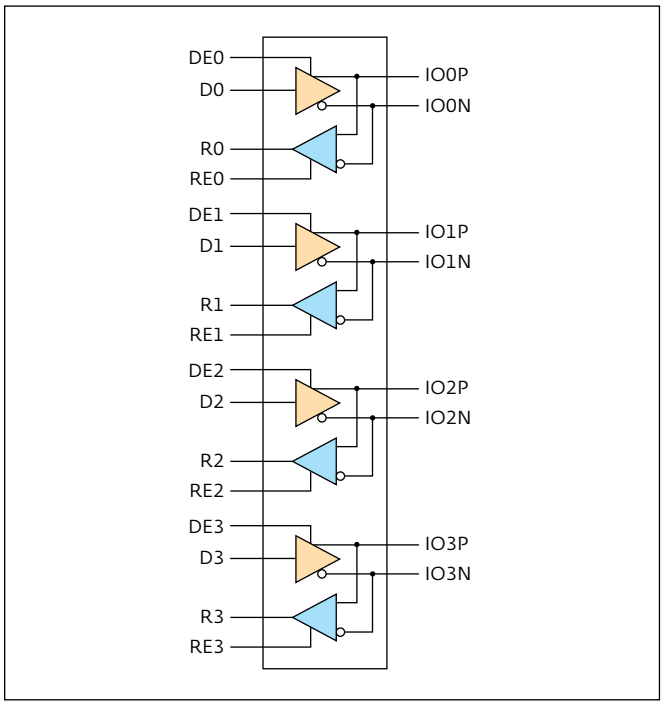

Рис.6. Функциональная схема микросхемы 5529ТР015-695
Fig.6. Functional diagram of 5529TP015-695 chip

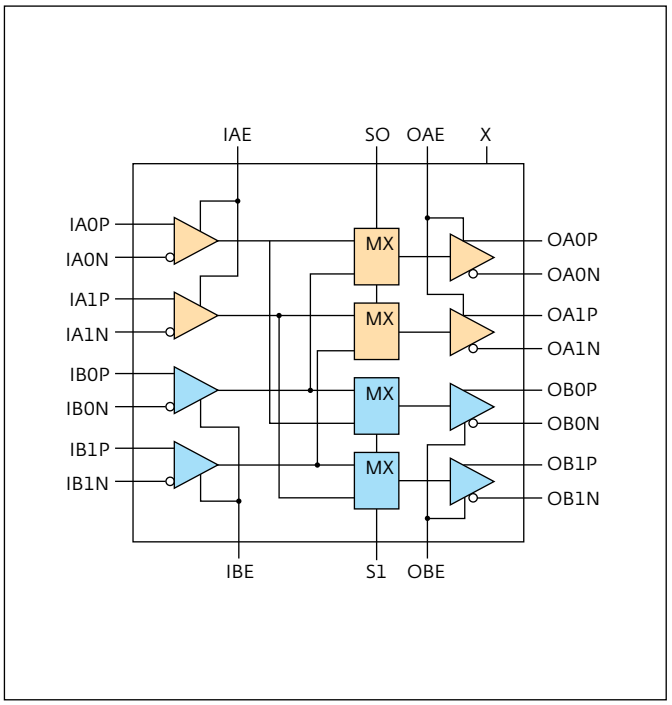

Рис.7. Функциональная схема микросхемы 5529ТР015-696
Fig.7. Functional diagram of 5529TP015-696 chip

схеме 5529ТР015-674 функциям, представлены в таблице.

Многофункциональная цифровая микросхема 5529ТР015-675 реализует 511 различных комбинационных логических функций, имеет восемь информационных выходов, а также восемь информационных и девять адресных входов. В микросхеме представлены все возможные логические функции при двух и трех входных переменных, а также потенциально наиболее используемые варианты функций с большим числом переменных [1]. Для большей гибкости применения микросхемы в одной функции определено сразу восемь различных комбинационных функций. В качестве примера ниже представлены логические функции, выполняемые микросхемой и соответствующие конфигурационному адресу "054" (их графическое изображение показано на рис.2):

$$Y1 = \overline{X1 + X2 + X3};$$
$$Y2 = X1 \,\&\, \overline{X2} \,\&\, \overline{X3};$$
$$Y3 = X1 \,\&\, X2 \,\&\, \overline{X3};$$
$$Y4 = \overline{X4 + X5 + X6};$$
$$Y5 = X4 \,\&\, \overline{X5} \,\&\, \overline{X6};$$
$$Y6 = X4 \,\&\, X5 \,\&\, \overline{X6};$$
$$Y7 = \overline{X7 + X8};$$
$$Y8 = X7 \,\&\, \overline{X8}.$$

МИКРОСХЕМЫ LVDS / LVDM-ПРИЕМНИКОВ И ПЕРЕДАТЧИКОВ

Помимо многофункциональных микросхем, в НПК "Технологический центр" также была разработана серия микросхем приемников и передатчиков стандартов низковольтной дифференциальной линии связи LVDS и LVDM [2].

Микросхемы 5529ТР015-688 и 5529ТР015-698 представляют собой восемь передатчиков дифференциальной линии LVDS и восемь передатчиков дифференциальной линии LVDM соответственно. Их функциональная схема представлена на рис.3.

Микросхема 5529ТР015-689 содержит по четыре передатчика дифференциальной линии LVDS и приемника дифференциальной линии LVDS / LVDM, а микросхема 5529ТР015-699 – по четыре передатчика дифференциальной линии LVDM и приемника дифференциальной линии LVDS / LVDM. Функциональная схема 5529ТР015-689 и 5529ТР015-699 приведена на рис.4.

Микросхема 5529ТР015-697 содержит восемь приемников дифференциальной линии LVDS / LVDM. Ее функциональная схема представлена на рис.5.

Микросхема 5529ТР015-695 включает четыре полудуплексных приемопередатчика много-

точечной дифференциальной линии M-LVDS. Функциональная схема 5529ТР015-695 приведена на рис.6.

Микросхема 5529ТР015-696 представляет собой коммутатор двух двухразрядных шин дифференциальных линий LVDS / LVDM. Данная микросхема имеет специальный вход управления мощностью дифференциальных выходов, который позволяет выбирать режим, соответствующий стандартам LVDS или LVDM. Функциональная схема 5529ТР015-696 показана на рис.7.

Полное подробное описание базовых кристаллов серии 5529 и микросхем, представленных в данной статье, приведено в книге [3].

Статья подготовлена при финансовой поддержке Минобрнауки России. Уникальный идентификатор ПНИ RFMEFI57815X0104.

ЛИТЕРАТУРА

1. **Денисов А.Н., Коняхин В.В.** Разработки НПК "Технологический центр" для применения в аппаратуре космического назначения // Международная конференция "Микроэлектроника 2015". Интегральные схемы и микроэлектронные модули: проектирование, производство и применение : Сб.тезисов. – М.: ТЕХНОСФЕРА, 2015. С. 74–77.
2. ANSI/TIA/EIA-644, Electrical Characteristics of Low Voltage Differential Signaling (LVDS) Interface Circuits, March 1996.
3. **Коняхин В.В., Денисов А.Н., Федоров Р.А.** и др. Микросхемы для аппаратуры космического назначения : Практ. пособ. / Под общ. ред. А.Н.Саурова. – М.: ТЕХНОСФЕРА, 2016. 388 с.

V КОНГРЕСС ПРЕДПРИЯТИЙ НАНОИНДУСТРИИ

1 декабря в пресс-центре МИА "Россия сегодня" состоялся V Конгресс предприятий наноиндустрии, в котором приняли участие более 600 гостей из России и зарубежных стран. В рамках конгресса были представлены разработки портфельных компаний "РОСНАНО" и нанотехнологических центров в медицине, электронике, строительстве и других областях. Участники форума обсудили пути поддержки инновационных компаний и проблемы развития высокотехнологичных разработок в стране.

Открывая конгресс, председатель правления УК "РОСНАНО", председатель правления Фонда инфраструктурных и образовательных программ (ФИОП) Анатолий Чубайс отметил, что за последние годы в России было создано несколько новых промышленных направлений, основанные на разработках в таких областях, как возобновляемая энергетика, производство современной упаковки, инновационных стройматериалов. По оценке "РОСНАНО" объем российской наноиндустрии приближается к 1300 млрд. руб. В развитии отрасли участвуют около 500 стартапов и тысячи состоявшихся промышленных компаний.

В рамках конгресса было проведено несколько мероприятий, посвященных развитию технологического предпринимательства. Так, в панельной дискуссии "Эволюция технологического предпринимательства: от героев-одиночек до конвейерного производства стартапов" приняли участие А.Чубайс, член правления Центра стратегических разработок "Северо-Запад", член экспертного совета Правительства РФ Петр Щедровицкий, директор направления "Молодые профессионалы" Агентства стратегических инициатив Дмитрий Песков, сооснователь и гендиректор наноцентра "ТехноСпарк" Денис Ковалевич, вице-президент китайского нанополиса Сучжоу Фэн Чжан, генеральный менеджер центра исследований и разработок бельгийского Католического университета Левен Пол ван Дун, а также сооснователь и гендиректор компании Drukka Startup Studio, автор книги "Анатомия стартап-студий" Аттила Сигети.

Зарубежные гости поделились с участниками конгресса опытом создания крупных инновационных центров. В частности, П. ван Дун рассказал, как небольшой университетский город Левен, где в 1970-е годы самым крупным производством был пивоваренный завод, превратился в один из крупнейших в Европе инновационных кластеров. А.Сигети сообщил о методе серийного производства стартапов, что позволяет значительно удешевить и ускорить процесс развития инновационных компаний. Д.Ковалевич, говоря о конвейере инноваций, подчеркнул, что нельзя рассматривать стартапы как просто маленькие компании, которые должны реализовывать все бизнес-процессы собственными силами – нужно под каждую задачу создавать или искать определенного исполнителя.

В рамках конгресса прошла серия дискуссий, посвященных развитию различных направлений наноиндустрии – сектора инновационных стройматериалов, фармацевтики, новой энергетики, электроники, подготовки кадров и др. Также на конгрессе состоялось вручение знака "Российская нанотехнологическая премия" и награждение лауреатов Российской молодежной премии в области наноиндустрии.

Организаторами V Конгресса предприятий наноиндустрии являются Фонд инфраструктурных и образовательных программ и Межотраслевое объединение наноиндустрии, партнерами выступили Российский экспортный центр, Фонд содействия инновациям, "Деловая Россия", "ОПОРА России", Агентство по технологическому развитию. Спонсор конгресса – банк "Открытие".

РОСНАНО

АЦП С КОНТУРОМ ФАЗОВОЙ АВТОПОДСТРОЙКИ ЧАСТОТЫ

ADC PHASE LOCKED LOOP

УДК 621.382, ВАК 05.27.01, DOI:10.22184/1993-8578.2016.70.8.40.47

М.Сизов[1, 2], Н.Малашевич[2], Р.Федоров[2] / vozis1@yandex.ru, N.Malashevich@tcen.ru, R.Fedorov@tcen.ru
M.Sizov[1, 2], N.Malashevich[2], R.Fedorov[2]

Описывается новый тип АЦП с контуром фазовой автоподстройки частоты (АЦП с ФАПЧ). Представлена функциональная структура разработанного устройства. Рассмотрены особенности АЦП с ФАПЧ. Показан переход от использования дискретных компонентов к реализации устройства на базовом матричном кристалле (БМК) серии 5503 на основе радиационно-стойкой КМОП-технологии.

This article describes a new type of ADC with the phase locked loop (ADC with PLL). It describes the functional structure of the developed device. It also outlines the features of ADC with PLL. It shows the transition from the device implementation using discrete components to the implementation on 5503 series gate array based on radiation-hardened CMOS technology.

В настоящее время разработка электронных устройств ведется с использованием микроконтроллеров (МК), содержащих в своем составе один или несколько аналогово-цифровых преобразователей (АЦП). АЦП, входящие в МК, иногда не удовлетворяют требованиям по точности и шумовым характеристикам. В связи с этим в научно-производственном подразделении "Дозор" был разработан новый тип АЦП с контуром фазовой автоподстройки частоты (ФАПЧ) [1].

Ближайшим прототипом АЦП с ФАПЧ является синтезатор стабильных частот. Подобные синтезаторы находят применение в качестве опорных генераторов в преобразователях частоты, электронных музыкальных инструментах и во многих других устройствах. На рис.1 показана функциональная схема синтезатора частоты.

Выходным сигналом синтезатора является переменное напряжение с частотой $F_{ГУН} = N \cdot F_1$. К точности и стабильности частоты предъявляются высокие требования.

В АЦП используется промежуточное преобразование аналогового сигнала (напряжения) в длительность импульса с помощью контура ФАПЧ [1]. Подробное описание принципа работы ФАПЧ приведено в [2, 3].

Функциональная схема АЦП на основе ФАПЧ представлена на рис.2. АЦП с ФАПЧ содержит элементы синтезатора и дополнительные элементы (на схеме обведены пунктиром). Основными являются следующие функциональные блоки:

- источник опорного напряжения – обязательный элемент АЦП. Амплитуда выходных импульсов фазового детектора равна опорному напряжению U_p, а длительность импульсов T_x равна фазовому сдвигу между сигналами F_1 и F_0;
- фильтр низкой частоты (ФНЧ), выполненный по схеме пропорционально-интегрирующего (ПИ) фильтра с дополнительным входом для подключения внешнего сигнала (U_x), который преобразуется сначала в длительность импульса, а потом в двоичный код;
- ПИ-фильтр, обеспечивающий астатизм системы ФАПЧ, то есть установившиеся средние значения напряжения выходного сигнала фазового детектора $U_{ФД}$ и входного сигнала U_x всегда равны. За счет интегратора и отрицательной обратной связи

[1] НПП "Дозор" / SMD "Dozor".
[2] НПК "Технологический центр" / SMC "Technological Centre".

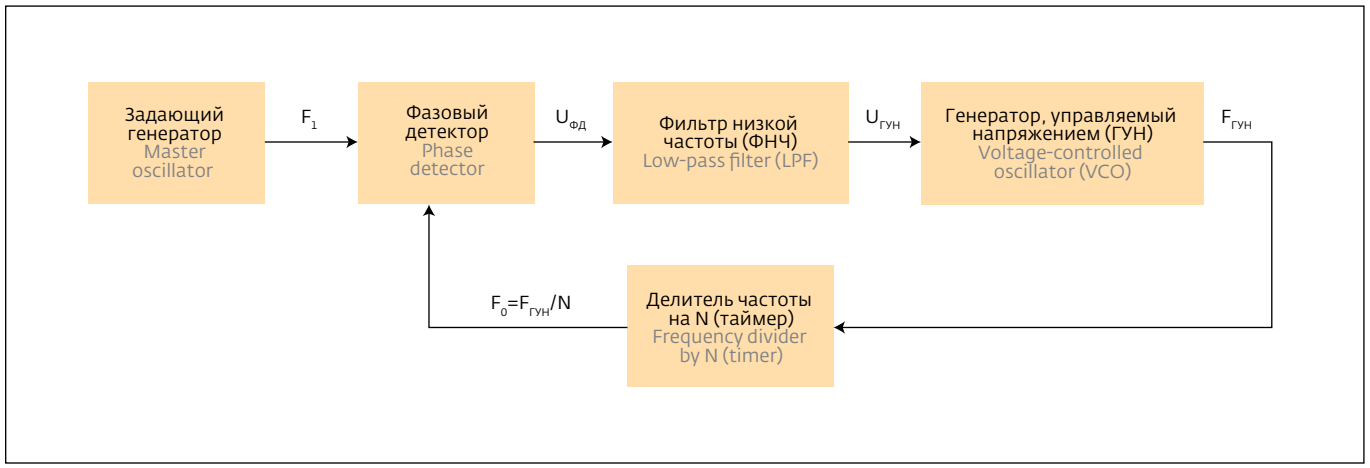

Рис.1. Функциональная схема синтезатора частоты
Fig.1. Functional diagram of frequency synthesizer

напряжение на входе ГУН поддерживается таким, чтобы частоты сигналов F_1 и F_0 были равными. Фазовый сдвиг T_x между сигналами F_1 и F_0 определяется выражением $T_x = T_1 \cdot U_x / U_p$, где T_1 – период частоты F_1, U_x – входное напряжение, U_p – опорное напряжение АЦП;

- ОЗУ для хранения текущего значения двоичного кода. Запись кода производится в момент переднего фронта импульса сигнала F_0;
- фазовый детектор (ФД) импульсного типа, выполненный на логических элементах и имеющий линейную выходную фазовую характеристику для обеспечения высокой точности преобразования.

В АЦП с ФАПЧ сигналы двух генераторов частот F_1 и F_0 являются внутренними, их форма напряжений должна быть прямоугольной, чтобы обеспечить работу ФД импульсного типа. Так как ФД определяет временной интервал между передними фронтами импульсов F_1 и F_0, то скважность этих импульсов не влияет на точность измерения фазового сдвига.

Currently, the development of electronic devices is carried out using a microcontrollers (MC), containing one or more analog-to-digital converters (ADC). Sometimes, ADC for MC do not meet the requirements of accuracy and noise. In this regard, the scientific and production division "Dozor" has developed a new type of ADC with the phase locked loop (PLL) [1].

The closest prototype of ADC with PLL is stable frequency synthesizer. Such synthesizers are used as reference oscillators in frequency converters, electronic musical instruments and many other devices. Fig.1 shows a functional diagram of the frequency synthesizer.

The output signal of the synthesizer is an alternating voltage with a frequency $F_{ГУН} = N \cdot F_1$. Accuracy and stability of frequency have to meet high requirements.

ADC uses intermediate conversion of the analog signal (voltage) into the pulse by means of PLL [1]. A detailed description of the working principle of PLL is given in [2, 3].

Functional diagram of the ADC with PLL is presented in Fig.2. ADC with PLL contains elements of the synthesizer and additional elements (in the diagram circled by dashed lines). The main ones are the following functional blocks:

- reference voltage source is a required element of ADC. Amplitude of the output pulses of the phase detector is equal to the reference voltage U_p, and the pulse duration T_X is equal to the phase shift between the signals F_1 and F_0;
- low-frequency filter (LFF) designed as a proportionally-integrating (PI) filter with additional input for external signal (U_x), which is converted into pulse width, and then into a binary code;
- PI filter provides the astaticism of the PLL system, that is, the steady-state average

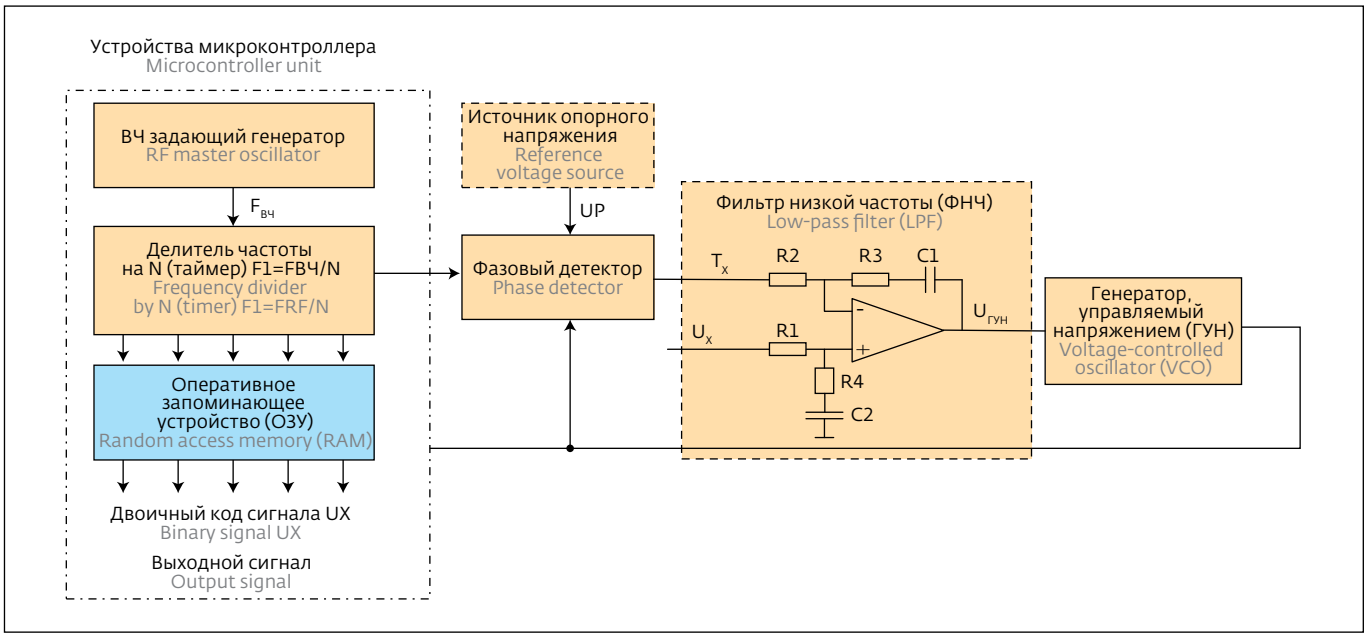

Рис.2. Функциональная схема АЦП с ФАПЧ
Fig.2. Functional diagram of the ADC with PLL

В научно-производственном подразделении "Дозор" в 2012 году была проведена разработка 15-канальной системы сбора информации для летающей лаборатории на базе 32-разрядного микроконтроллера 1986ВЕ1 и АЦП с ФАПЧ, параметры которой приведены в табл.1.

АЦП с ФАПЧ является следящей системой с астатизмом второго порядка. Установившееся значение ошибки в таких устройствах равно нулю, точнее – напряжению смещения на входе ОУ $+U_x / K_{осс}$, где $K_{осс}$ – коэффициент ослабления синфазной составляющей ОУ. Например, ОУ 140УД31АТ, имеющий входное напряжение смещения 25 мкВ и коэффициент ослабления синфазной составляющей более 110 дБ, гарантирует преобразование напряжения U_x = 5 В в длительность импульсов с погрешностью менее 0,002%. Номиналы резисторов R1 и R3 (рис.2) должны

values of the output signal of the phase detector $U_{ФД}$ and of the input signal U_x are always equal. Thanks to the integrator and a negative feedback, the input voltage of VCO is maintained so that the frequency of the signals F_1 and F_0 are equal. Phase shift T_x between signals F_1 and F_0 is equal to $T_x = T_1 \cdot U_x / U_p$, where T_1 is the period of frequency F_1, U_x is input voltage, U_p is reference voltage of the ADC;

- RAM for storing the current value of the binary code. Code is written in the time of the leading edge of the pulse signal F_0;
- pulse phase detector (PD) based on logic elements and having a linear output phase characteristic to ensure high precision conversion.

In ADC with PLL the signals of the two oscillators F_1 and F_0 are internal, their form of voltage needs to be rectangular, to ensure the operation of pulse PD. Since PD measures the time interval between leading edges of the pulses F_1 and F_0, the off-duty ratio of these pulses does not affect the measurement accuracy of the phase shift.

In 2012 the scientific and production division "Dozor" has developed a 15-channel information-gathering system for the flying laboratory on the basis of 32-bit microcontroller 1986BE1 and ADC with PLL, the parameters of which are given in table.1.

ADC with PLL is a tracking system with astaticism of the second order. The steady-state error in such devices is equal to zero, more precisely – to the bias voltage at the input of op-amp $+U_x / K_{occ}$, where K_{occ} is common-mode rejection ratio (CMRR) of op-amp. For example, ОУ 140УД31АТ, which has an input bias voltage of 25 μV and CMRR more than 110 dB, guarantees

Таблица 1. Параметры 15-канальной системы сбора информации на базе 32-разрядного микроконтроллера 1986ВЕ1Т и АЦП с ФАПЧ
Table 1. Parameters of 15-channel information-gathering system based on 32-bit microcontroller 1986BE1T and ADC with PLL

Число разрядов АЦП Number of ADC bits	18
Число отсчетов АЦП Number of ADC counts	200 000
Приведенная погрешность преобразования в диапазоне температур от –60 до 125 °С Reduced conversion error in temperature range from –60 to 125 °C	< 0,1%
Рабочий диапазон входного сигнала, В Working range of input signal, V	0,5–4,5
Вес младшего разряда выходного кода АЦП, мкВ Weight of LSB of ADC output code, μV	25
Уровень "шума" в выходном сигнале АЦП, мкВ (в размахе) Noise in ADC output signal, μmV (p-p)	125
Полоса пропускания АЦП, Гц Bandwidth of ADC, Hz	80
Рабочая частота преобразователя с ФАПЧ, Гц Operating frequency of ADC with PLL, Hz	400
АЧХ АЦП Frequency response of ADC	Фильтр низкой частоты второго порядка с подавлением помех с частотами, кратными 400 Гц Second order low pass filter with interference suppression for frequencies multiple of 400 Hz
Тип Type	АЦП с промежуточным преобразованием напряжения в длительность импульсов ADC with intermediate conversion of voltage to pulse duration
Способ преобразования Conversion method	Фазовая автоподстройка частоты (ФАПЧ) Phase-locked loop (PLL)

the voltage conversion U_x = 5 V into pulse duration with an accuracy of less than 0.002%. The values of resistors R1 and R3 (Fig.2) must be equal to each other (±5%) to compensate input currents of op amp. The elements R2, R4, C1 and C2 do not affect the accuracy.

The voltage at the output of op-amp controls the frequency and phase of VCO. Since the VCO is a second integrating element in the PLL loop, it only responds to the steady component of this complex signal.

The output signal of PD, a rectangular pulse, whose area (the average voltage value over the period of the conversion frequency F_1) is equal to the input voltage U_x, is a feedback signal in the ADC circuit. PD is manufactured on the base of 5503 gate array family. The duration of the output pulse of PD can be less than 1 ns.

The resolution of the ADC with PLL is determined by the performance (circuitry) of the circuit of PD and by a clock frequency of MC or counter, which forms a signal F_1. The maximum operating frequencies of MC and logic elements had reached the level of 1 GHz and above. It is important to note the great potential of ADC with PLL. Moreover, the device contains only one precision element – operational amplifier (op amp). Other elements (resistors and capacitors) may have uncertainty of ± (5–10)%.

Possibilities of ADC with PLL based on a 32-bit 1986BE1T microcontroller with a clock frequency of 140 MHz are tested and presented in table.2.

In 2015, to reduce the dimensions of the designed ADC with a PLL, SMC "Technological Centre" has developed and manufactured the 5503XM1У-651 chip of dual-channel PLL. The chip has

Таблица 2. Варианты АЦП с ФАПЧ
Table 2. Modifications of ADC with PLL

Полоса пропускания АЦП, Гц Bandwidth of ADC, Hz	Число разрядов АЦП Number of ADC bits	Частота преобразования, Гц Frequency of ADC with PLL, Hz	Максимальное значение кода АЦП Maximum ADC value
2	24	10	14 000 000
10	22	50	2 800 000
20	21	100	1 400 000
80	19	400	350 000
200	18	1 000	140 000
800	16	4 000	35 000

быть одинаковыми (±5%) для компенсации входных токов ОУ. Элементы R2, R4, C1 и C2 не влияют на точность.

Напряжение на выходе ОУ управляет частотой и фазой ГУН. Так как ГУН является вторым интегрирующим элементом в контуре ФАПЧ, то он реагирует только на постоянную составляющую этого сложного по форме сигнала.

Сигналом обратной связи в схеме АЦП является выходной сигнал ФД – прямоугольный импульс, площадь которого (среднее значение напряжения за период частоты преобразования F_1) равна входному напряжению U_x. ФД изготовлен на БМК серии 5503. Длительность выходного импульса ФД может быть менее 1 нс.

Разрешающая способность АЦП с ФАПЧ определяется быстродействием (элементной базой) схемы ФД и тактовой частотой МК или счетчика, который формирует сигнал F_1. Предельные рабочие частоты МК и логических элементов уже достигли уровня 1 ГГц и выше. Важно отметить большие потенциальные возможности АЦП с ФАПЧ. При этом устройство содержит только один прецизионный элемент – операционный усилитель (ОУ), остальные же элементы (резисторы и конденсаторы) могут иметь разбросы значений характеристик ± (5–10)%.

28 pins, supply voltage of 5 V and is made using 1.6 μm CMOS technology. Fig.3 shows the 5503XM1У-651 chip in MK 5123.28-1.01 package.

One 5503XM1У-651 chip replaces more than 30 standard logic chips on discrete components, which are used to build components of the PLL. The chip includes the phase detector and VCO.

SMC "Technological Centre" has developed a gate array family with standardized library of basic and standard functional cells, common design tool based on Kovcheg CAD and the means for prototyping [4]. The entry-level 5503 and 5507 gate array families have uniform nomenclature and are based on radiation-hardened 1.6 μm bulk silicon CMOS technology. Wiring is carried out in the first metal layer and in the polysilicon layer. Gate arrays of these series are allowed for use in special-purpose equipment [5]. More than 600 types of semicustom very large scale integrated circuits of various purpose are designed and manufactured on the basis of 5503 and 5507 gate arrays families, including for space-based equipment, for example, for Progress-M and Soyuz-TMA spacecrafts, Briz-M upper stages and many other [6,7,8].

The 5503XM1У-653 chip with two additional 4-bit counters has been created on the basis of 5503XM1У-651 chip. The counter divides the output frequency of the VCO by 16, thereby averaging the noise of the VCO and, consequently, reducing ADC noise.

5503XM1У-617 chip, containing a set of op amps, was used to implement the low-pass filter. Fig.4 shows a block diagram of one channel of the PLL using 5503XM1У-653 and 5503XM1У-617 chips.

Возможности АЦП с ФАПЧ на базе 32-разрядного микроконтроллера 1986ВЕ1Т с тактовой частотой 140 МГц проверены и представлены в табл.2.

С целью уменьшения габаритов разработанного макета АЦП с ФАПЧ, в 2015 году по заказу НПП "Дозор" в НПК "Технологический центр" была разработана и изготовлена микросхема БМК 5503ХМ1У-651 двухканального ФАПЧ. Микросхема имеет 28 выводов, питающее напряжение 5 В и выполнена по КМОП-технологии с нормами 1,6 мкм. На рис.3 показана микросхема 5503ХМ1У-651 в корпусе МК 5123.28-1.01.

Одна микросхема 5503ХМ1У-651 заменяет более 30 микросхем стандартной логики на дискретных элементах, которые входят в состав ФАПЧ и служат для построения его компонентов. В состав микросхемы входят фазовый детектор и генератор, управляемый напряжением.

НПК "Технологический центр" разработал семейство БМК, имеющих унифицированную библиотеку базовых и типовых функциональных ячеек, единые средства проектирования на базе САПР "Ковчег" и средства прототипирования микросхем [4]. Младшими в семействе БМК являются серии 5503 и 5507, которые унифицированы по составу и изготавливаются по радиационно-стойкой КМОП-технологии с нормами 1,6 мкм на объемном кремнии. Разводка осуществляется в первом слое металла и слое поликремния. БМК этих серий имеют

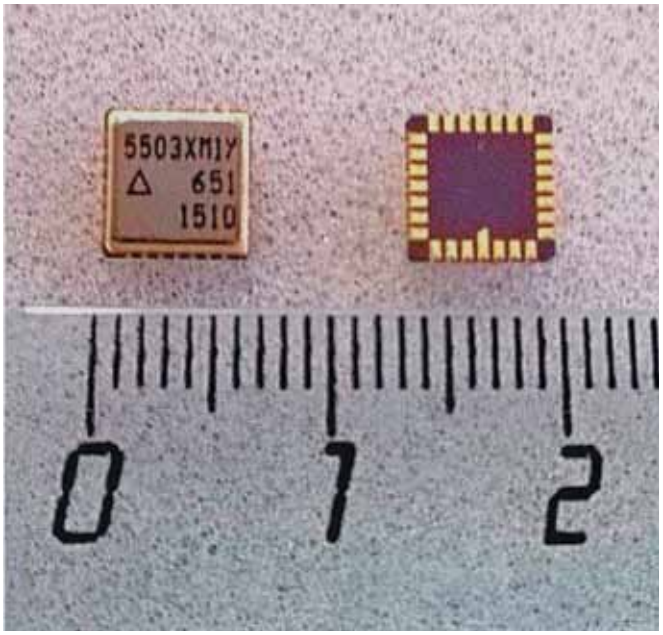

Рис.3. Микросхемы 5503ХМ1У-651 в корпусе МК 5123.28-1.01
Fig.3. 5503XM1У-651 chip in MK 5123.28-1.01 package

категорию качества "ВП" и разрешены к применению в аппаратуре специального назначения [5]. На базе БМК серий 5503 и 5507 разработано и выпускается более 600 типов полузаказных микросхем различного назначения, в том числе для аппаратуры космического базирования, например, для космических кораблей "Прогресс-М", "Союз-ТМА", разгонного блока "Бриз-М" и многих других аппаратов [6, 7, 8].

55503XM1У-617 chip includes the following functional blocks (Fig.5):

- six independent op-amps;
- two inverting amplifier;
- reference voltage source (1,12 V);
- current setting unit.

The current setting unit for setting of op-amp mode is connected to the R0 pin. Between this pin and "total 0V" it is necessary to connect a resistor from 100 kΩ to 1 MΩ to set the bias current of all op-amps, which determines their performance. The total consumption current of IC is proportional to the current through the R0 output.

The reference voltage source on width of forbidden band has a high resistance CREF output to connect a filter capacitor (about 10 nF) and the input for INRI mode. The change of voltage on the CREF output in the temperature range is depended by the value of external adjustment resistor on the INRI output. Between this output and the "total 0" it is necessary to connect a resistor – from 8.1 kΩ to 10 kΩ. The sensitivity of the reference voltage source to the change in voltage is 2 mV/V. Inside the chip the CREF output is connected to the noninverting inputs of the op-amp.

The characteristics of a single op-amp are presented in table.3.

The development of the circuitry for implementation of the ADC with PLL continues. SMC "Technological Centre" has developed on the basis of the 5503XM1У-653 chip the 5503XM1У-670 chip. The new chip includes additional operational amplifier for implementation of low-pass filter, and also modified VCO. ■

This paper was created with the financial support of the Ministry of Education and Science of the Russian Federation. Unique identifier RFMEFI58015X0005.

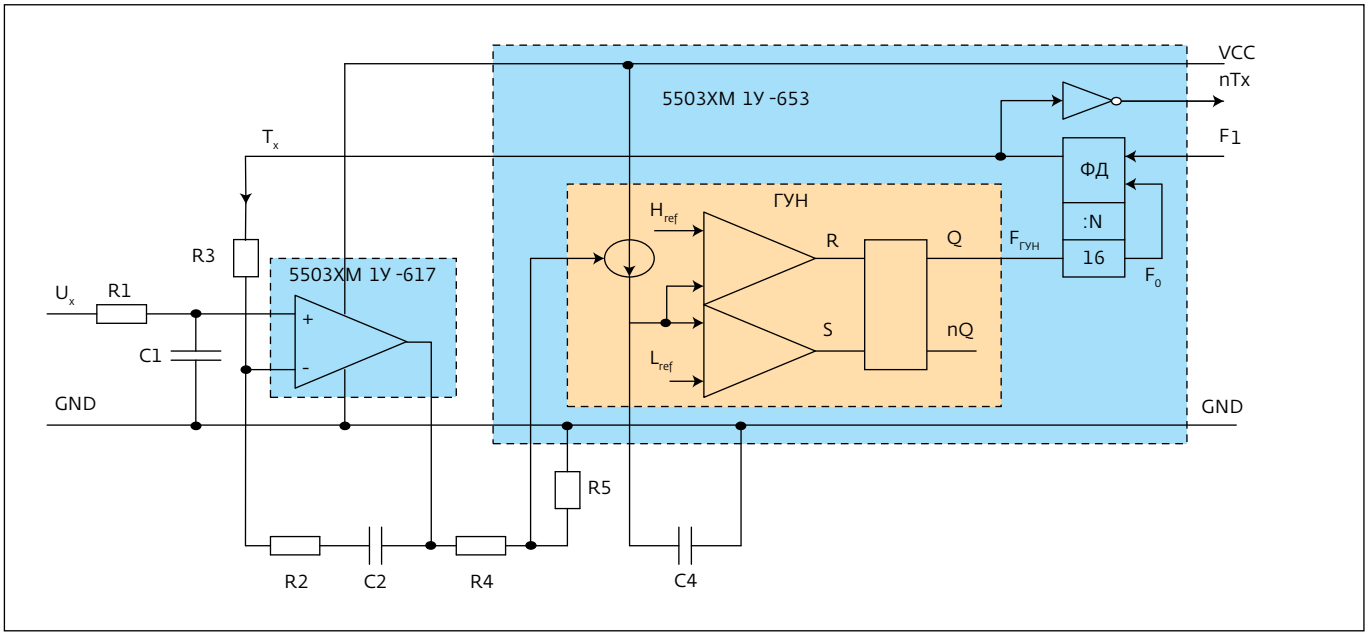

Рис.4. Блок-схема одного канала ФАПЧ на микросхемах 5503ХМ1У-653 и 5503ХМ1У-617
Fig.4. Block diagram of one channel of PLL on 5503ХМ1У-653 and 5503ХМ1У-617 chips

Развитием микросхемы 5503ХМ1У-651 стала микросхема 5503ХМ1У-653, где к имеющимся блокам добавлены два 4-разрядных счетчика. Счетчик делит выходную частоту ГУН на 16, тем самым усредняя шумы ГУНа и, как следствие, уменьшая шумы АЦП.

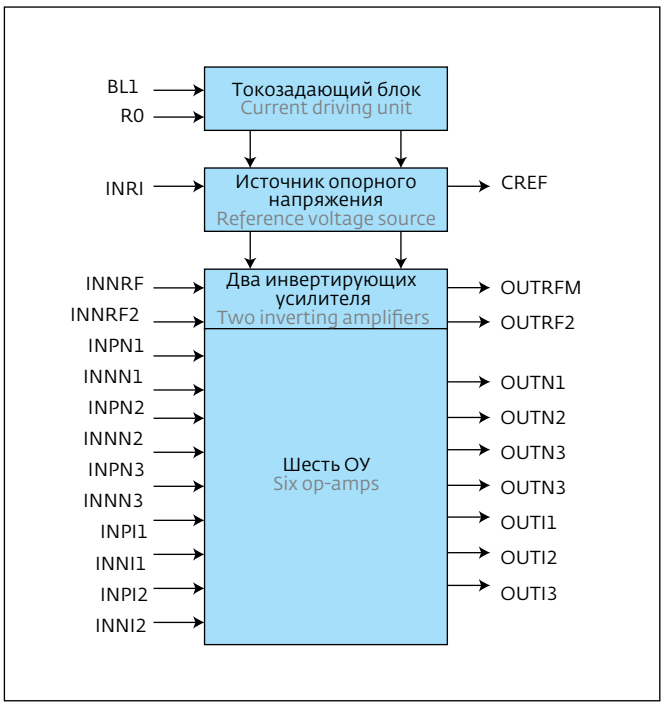

Рис.5. Функциональная блок-схема микросхемы 55503ХМ1У-617
Fig.5. Functional block diagram of 55503ХМ1У-617 chip

Для реализации ФНЧ была использована микросхема 5503ХМ1У-617, которая содержит в своем составе набор ОУ. На рис.4 показана блок-схема одного канала ФАПЧ с использованием микросхем 5503ХМ1У-653 и 5503ХМ1У-617.

Микросхема ОУ 55503ХМ1У-617 включает следующие функциональные блоки (рис.5):

- шесть независимых ОУ;
- два инвертирующих усилителя;
- источник опорного напряжения на 1,12 В;
- токозадающий блок.

Токозадающий блок для установки режима ОУ подключен к выводу R0. Между этим выводом и "общим 0В" необходимо подключить резистор от 100 кОм до 1 МОм для задания тока смещения всех ОУ, определяющего их быстродействие. Общий ток потребления микросхемы пропорционален току через вывод R0.

Источник опорного напряжения на ширине запрещенной зоны имеет высокоомный выход CREF для подключения фильтрующего конденсатора (порядка 10 нФ) и вход установки режима INRI. Изменение напряжения на выходе CREF в диапазоне температур определяется номиналом внешнего регулировочного резистора на выводе INRI. Между этим выводом и "общим 0 В" необходимо подключить резистор номиналом от 8,1 до 10 кОм. Чувствительность

Таблица 3. Основные характеристики ОУ
Table 3. Key features of op-amp

Входное напряжение, В Input voltage, V	0,2 – VCC-0,2
Выходное напряжение, В Output voltage, V	0,2 – VCC-0,2
Коэффициент усиления с разомкнутой обратной связью, дБ Gain with open feedback loop, dB	≥ 61
Запас по фазе, град Phase margin, deg	65
Частота единичного усиления, МГц Unity gain frequency, MHz	3
Напряжение смещения нуля, мВ Offset voltage, mV	≤ 15
Максимальный выходной ток, мА Maximum output current, mA	≤ 2
Максимальный входной ток, мкА Maximum input current, μA	≤ 3

источника опорного напряжения к изменению напряжения питания составляет 2 мВ/В. Внутри микросхемы выход CREF подключен к неинвертирующим входам ОУ.

Характеристики единичного ОУ представлены в табл.3.

Развитие элементной базы, предназначенной для реализации АЦП с контуром фазовой автоподстройки частоты, продолжается. В настоящее время в НПК "Технологический центр" разработана микросхема 5503ХМ1У-670, которая является развитием микросхемы 5503ХМ1У-653. В состав новой микросхемы добавлен ОУ, предназначенный для реализации ФНЧ, а также измененный генератор, управляемый напряжением.

Статья подготовлена при финансовой поддержке Минобрнауки России. Уникальный идентификатор ПНИЭР RFMEFI58015X0005.

ЛИТЕРАТУРА

1. **Сизов М.В.** Преобразователь напряжения в длительность импульса, стабилизированный ФАПЧ // Современная электроника. 2012. № 6.
2. Система ФАПЧ и ее применения. http://catalog.gaw.ru/index.php?page=document&id=1478.
3. Контур фазовой автоподстройки частоты и его основные свойства. http://www.dsplib.ru/content/pll/pll.html.
4. **Денисов А.Н., Фомин Ю.П., Коняхин В.В., Федоров Р.А.** Библиотека функциональных ячеек для проектирования полузаказных микросхем серий 5503 и 5507. – М.: ТЕХНОСФЕРА, 2012. С. 304.
5. **Гаврилов С.В., Денисов А.Н., Коняхин В.В., Малашевич Н.И., Федоров Р.А.** Семейство серии базовых матричных кристаллов // Известия высших учебных заведений. Электроника. 2015. Т. 20. № 5. С. 497–504.
6. **Денисов А.Н., Коняхин В.В.** Разработки НПК "Технологический центр" для применения в аппаратуре космического назначения. – М.: ТЕХНОСФЕРА, 2015. С. 74.
7. **Денисов А.Н., Коняхин В.В., Якунин А.Н., Бец В.П.** Разработка аппаратуры космического применения с использованием базовых матричных кристаллов // Вестник НПО им. С.А.Лавочкина. 2012. № 5. С. 67–73.
8. **Басаев А.С., Денисов А.Н., Коняхин В.В., Сауров А.Н.** Применение базовых матричных кристаллов при разработке аппаратуры специального назначения // Вестник Концерна ПВО Алмаз-Антей. 2011. № 2. С. 69–79.

РЕАЛИЗАЦИЯ ЭКСПЕРИМЕНТАЛЬНОГО ОБРАЗЦА ПРОГРАММНОГО КОМПЛЕКСА КОНТРОЛЯ СБОЕУСТОЙЧИВОСТИ ПРОЕКТА МИКРОСХЕМЫ

IMPLEMENTATION OF EXPERIMENTAL SOFTWARE PROTOTYPE FOR CONTROL OF FAULT TOLERANCE OF IC DESIGN

УДК 621.382, УДК 004.42, ВАК 05.27.01, DOI:10.22184/1993-8578.2016.70.8.48.58

О.Брехов, А.Клименко*, А.Жданов*, А.Якупов* / obrekhov@mail.ru, a.v.klimenko@mai.ru, a.a.shdanov@mai.ru, yau@mai.ru*
O.Brekhov, A.Klimenko*, A.Shdanov*, A.Yakupov**

Представлена совокупность разработанных модулей, образующих ядро программного обеспечения экспериментального образца программно-аппаратного комплекса (ПАК) контроля сбоеустойчивости проекта микросхемы. Контроль сбоеустойчивости основан на использовании расширенного метода внесения неисправностей, подразумевающего моделирование многоуровневого воздействия неисправностей. Программные модули ПАК обеспечивают обработку проекта микросхемы, генерацию списка сбоев, генерацию тестовых воздействий и обработку результатов моделирования. Технические решения, воплощенные в ПАК, позволяют выполнять гибкий выбор источников возникновения сбоев в микросхеме и получать детальную информацию о локализации критических сбоев, приводящих к отказу моделируемой системы. Использование ПЛИС-прототипирования вместо программных симуляторов при моделировании позволяет добиться ускорения процесса контроля сбоеустойчивости.

A set of developed modules that form the software core of the experimental prototype of a hardware-software system (HSS) for control of fault tolerance of IC design is presented. Control of fault tolerance is based on the use of the extended method of fault injection, which implies the modeling of the multi-level impact of faults. Software modules of HSS provides processing of the IC design, generation of the list of faults, generation of test inputs and processing of the simulation results. Technical solutions embodied in the HSS, allow a flexible choice of sources of faults in the chip and obtaining detailed information about the localization of the critical faults that caused a failure of the simulated system. The use of FPGA prototyping instead of software simulation allows to accelerate the control of fault tolerance.

Разработка устройств типа "система на кристалле" (СнК) включает в себя решение целого комплекса взаимосвязанных задач от проектирования структуры и выбора аппаратной базы до реализации экспериментальных образцов. При этом, проведение тестирования работоспособности на этапе разработки имеет первостепенное, а для устройств на основе заказных и полузаказных микросхем – критическое значение, так как качество тестирования существенно влияет на стоимость разработок. К устройствам специального назначения (в частности, компонентам космической техники) предъявляются дополнительные требования по обеспечению работоспособности в условиях воздействия агрессивных внешних сред. В связи с этим, актуально тестирование сбоеустойчивости устройств типа СнК на этапе их разработки.

* Московский авиационный институт (национальный исследовательский университет) / Moscow Aviation Institute (National Research University).

Широко известно, что одним из основных источников сбоев электроники как космического, так и наземного применения является космическая радиация [1]. Тестирование работоспособности микросхем в условиях воздействия радиации обычно производится методом внесения неисправностей и может выполняться либо на поздних стадиях разработки путем испытания экспериментальных образцов в ускорителях частиц, либо на ранних стадиях путем моделирования сбоев проектов микросхем с применением программно-аппаратных комплексов (ПАК). Второй способ позволяет избежать дорогостоящего изготовления экспериментальных образцов в циклах тестирования-перепроектирования и поэтому используется многими разработчиками. Известно множество реализаций аппаратно-программных решений (в частности, [2–5]) для контроля работоспособности СнК в условиях воздействия космической радиации. Имеются решения на основе ПЛИС-прототипирования, которые обеспечивают оптимальное соотношение цены и быстродействия ПАК [6]. Однако известные подходы не обеспечивают возможность детального исследования воздействия источников сбоев на микросхемы.

В данной статье рассмотрена совокупность программных модулей разработанного ПАК для контроля сбоеустойчивости проекта микросхемы, использующего расширенный метод внесения неисправностей [7]. Метод использует стек из трех моделей (внешних воздействий, появления угроз и локализации неисправностей), и позволяет исследовать многоуровневое воздействие неисправностей на микросхему.

Структурная схема предложенного ПАК представлена на рис.1. Комплекс содержит в своем составе рабочую станцию, на базе которой реализуется программная составляющая, а также четыре специализированные платы расширения Xilinx Virtex-6 FPGA ML605 Evaluation Kit.

ПАК позволяет оценить сбоеустойчивость устройств типа СнК для произвольной целевой аппаратной базы (ЦАБ), реализуя пошаговое моделирование [8]. Данная методика подразумевает проведение функционального тестирования исходного проекта микросхемы, описанного на подмножестве языка Verilog [9] на уровне цифровых функциональных элементов ЦАБ путем ПЛИС-прототипирования, с последующим внедрением средств внесения сбоев в исходный проект и проведением функционального тестирования модифицированного проекта с определением их эквивалентности. В случае эквивалентности исходного и модифицированного проектов методика предписывает моделирование функционирования последнего в условиях наличия сбоев, результаты которого позволяют определить сбоеустойчивость исходного проекта микросхемы.

Рассмотрим программную составляющую разработанного ПАК.

Development of devices of "system on chip" (SoC) type includes a whole set of interrelated tasks from design of structure and selection of hardware base to implementation of experimental samples. At the same time, the testing efficiency at the design stage is paramount, and for devices that are based on custom and semicustom chips it is critical, as the quality of testing significantly affects the cost of development. Devices for special purposes (in particular, components of space equipment) must meet additional requirements to ensure the operability in the conditions of aggressive external environments. In this regard, the testing of failure tolerance of devices like SoC at the stage of their development is urgent.

It is widely known that one of the main failure sources of electronics in both the satellite and terrestrial applications is cosmic radiation [1]. The testing of operability of chips in conditions of radiation exposure is usually provided by method of fault injection, and can be executed either on later stages of development by testing experimental models in particle accelerators or in the early stages, by simulation of failures of designs of the chips with use of hardware-software systems (HSS). The second method avoids the costly fabrication of experimental samples in the cycles of testing, redesign, and therefore is used by many developers. Many implementations of hardware and software solutions to control the operability of the SoC under conditions of exposure to cosmic radiation are well known (in particular, [2–5]). There are solutions based on FPGA prototyping, which provide the optimal ratio of price and performance of HSS [6]. However, the

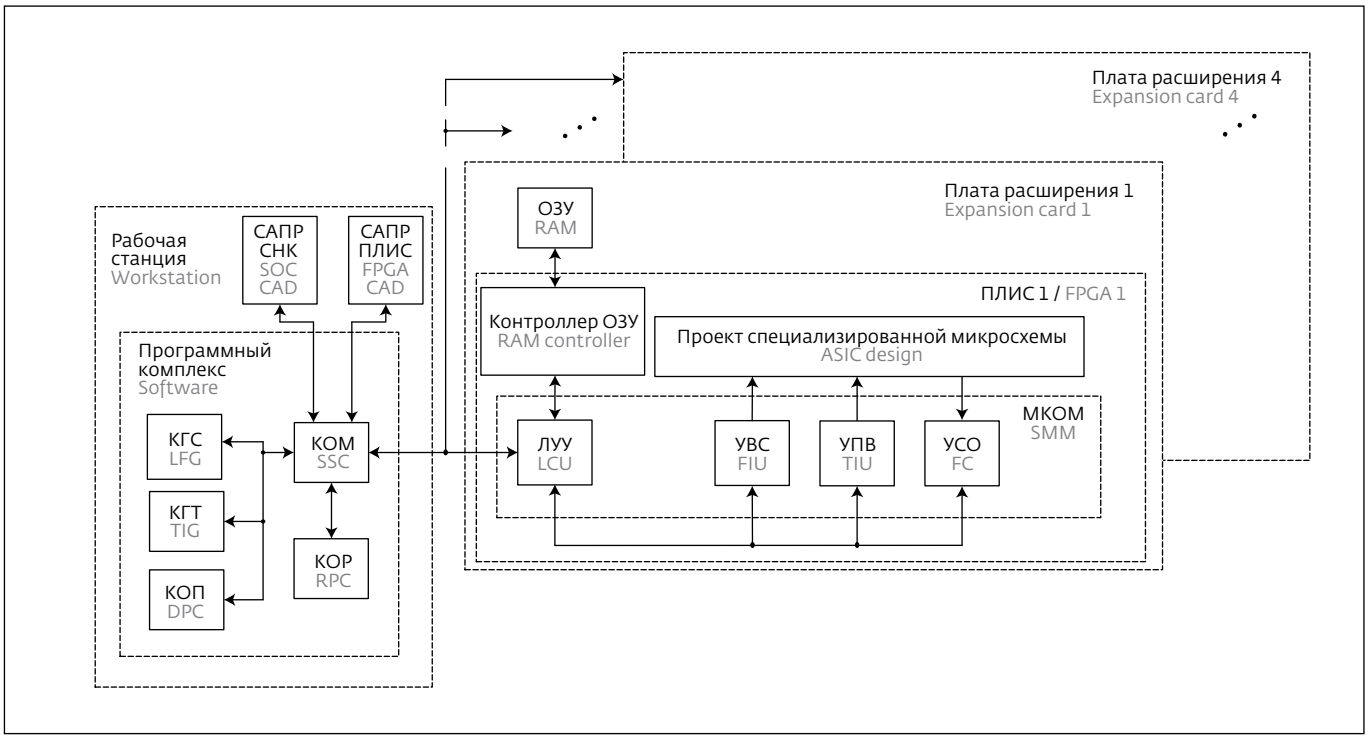

Рис.1. Функциональная схема ПАК: КГС – компонент генерации списка сбоев; КГТ – компонент генерации тестовых воздействий; КОП – компонент обработки проекта микросхемы; КОМ – компонент обеспечения моделирования; КОР – компонент обработки результатов моделирования; САПР – система автоматизированного проектирования; ОЗУ – оперативное запоминающее устройство; ЛУУ – локальный узел управления; УВС – узел внесения сбоев; УПВ – узел подачи тестовых воздействий; УСО – узел сбора откликов; ПЛИС – программируемая логическая интегральная схема; МКОМ – микроядро обеспечения моделирования

Fig.1. Functional diagram of HSS: LFG – generator of list of faults; TIG – generator of test inputs; DPC – component for processing of IC design; SSC – component for simulation support; RPC – component for processing of simulation results; CAD – computer-aided design system; RAM – random access memory; LCU – local control unit; FIU – fault injection unit; TIU – test inputs unit; FC – feedback collector; FPGA – field-programmable gate array; SMM – simulation management microcore

known approaches do not provide the possibility of detailed studies of the impact of sources of failures on the chip.

This paper describes a set of software modules of developed HSS for control of the failure-stability of IC design using an advanced method of fault injection [7]. The method uses a stack of three models (of external influences, of emergence of threats and of fault localization), and allows to study the multi-level impact of faults on the chip.

Structural diagram of the proposed HSS is presented in Fig.1. The complex contains a workstation with software component, as well as four specialized expansion boards – Xilinx Virtex-6 FPGA ML605 Evaluation Kit.

HSS allows to estimate the failure-stability of devices like the SoC for an arbitrary target hardware, implementing step-by-step simulation [8]. This technique involves carrying out functional testing of the initial IC design, described on a subset of the Verilog language [9] at the level of the digital functional elements of the target hardware, through FPGA prototyping, with the subsequent introduction of the means of fault injection in the original design and functional testing of the modified design with the determination of their equivalence. In the case of equivalence of the original and modified designs, the methodology requires modeling the functioning of the latter in the presence of failures, the results of which determine the failure-stability of the initial IC design.

Let's consider a software component of the developed HSS.

GENERAL DESCRIPTION OF SOFTWARE SYSTEM

The structure of the software system is shown in Fig.2. The

ОБЩЕЕ ОПИСАНИЕ ПРОГРАММНОГО КОМПЛЕКСА

Структура программного комплекса представлена на рис.2. Программный комплекс реализован на основе пяти основных компонентов, позволяющих осуществлять обработку проекта микросхемы, генерацию списка сбоев и тестовых воздействий, а также обработку результатов моделирования проекта микросхемы с имитацией сбоев. ПАК содержит САПР СнК ЦАБ и Xilinx ISE, обеспечивающие синтез списков соединений элементов устройства в соответствующих базисах.

Программный комплекс осуществляет решение следующих задач:

- выполнение функционального анализа проекта микросхемы, созданного средствами САПР СнК (представленного в виде списка соединений для ЦАБ);
- обнаружение в проекте микросхемы блоков, в которых наиболее вероятно возникновение сбоев;
- определение последствий сбоев в функционировании микросхемы;
- формирование внешних воздействий для контроля сбоеустойчивости микросхемы;
- формирование данных для программирования аппаратных средств, обеспечивающих имитацию сбоев в соответствии с методикой моделирования;
- моделирование функционирования проекта микросхемы с имитацией сбоев;

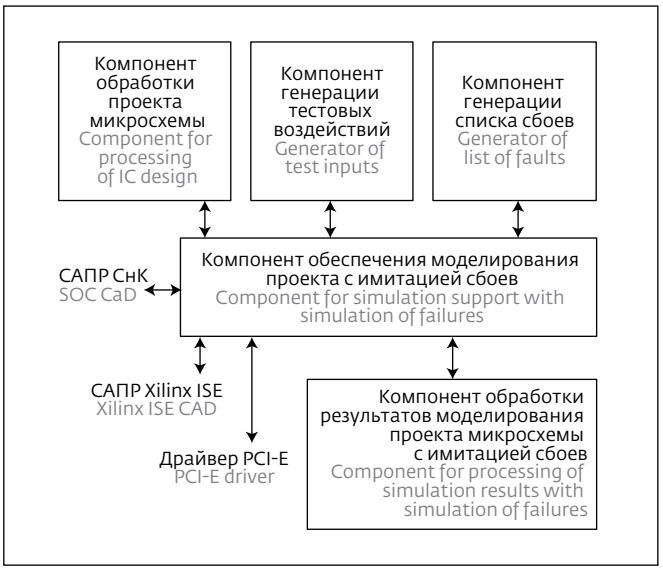

Рис.2. Структурная схема программного комплекса
Fig.2. Block diagram of software system

- формирование временных диаграмм внутренних сигналов проекта микросхемы при имитации сбоев;
- сбор, анализ, хранение и обработка данных моделирования.

Программный комплекс позволяет моделировать функционирование целевой микросхемы типа СнК на базовых матричных кристаллах (БМК) серий 5521 и 5529 в условиях воздействия космической радиации. В процессе моделирования на основе известных характеристик потоков

software complex is realized on the basis of five main components, allowing to carry out processing of IC design, the generation of a list of faults and test inputs, and also processing of results of modeling of IC design with simulated failures. HSS contains CADs for SoC, target hardware and Xilinx ISE, providing a synthesis of the lists of compounds of elements of the device in the respective bases.

The software system carries out the following tasks:

- functional analysis of the IC design created by SoC CAD tools (represented as a list of connections for target hardware);
- detection in the IC design of units, in which fault occurrence is the most likely;
- determine the consequences of faults in operation of IC;
- generation of external influences to control the failure-stability of the chip;
- data generation for programming hardware for the simulation of faults in accordance with the methodology of simulation;
- modeling the operation of the IC design with simulated failures;
- formation of a timing chart of internal signals of the IC design at simulation of failures;
- collection, analysis, storage and processing of simulation data.

The software system allows to simulate operation of the target SoC on 5521 and 5529 gate array families in conditions of exposure to cosmic radiation. In the process of modeling based on the known characteristics of streams of charged particles and of the target chips, the time moments of failures of different types and their localization are

заряженных частиц и целевой микросхемы определяются моменты времени возникновения сбоев разных типов и осуществляется их локализация. Процесс моделирования включает несколько этапов, в частности: тестирование исходного проекта микросхемы, внедрение в проект микросхемы функциональности по внесению сбоев, моделирование функционирования полученного проекта при отсутствии и наличии сбоев. На каждом этапе осуществляется мониторинг значений сигналов на выходах микросхемы и внутренних сигналов, задаваемых пользователем, а также проводится их сравнение с эталонными значениями. Анализ результатов моделирования позволяет оценить сбоеустойчивость целевой микросхемы типа СнК в условиях заданного воздействия космической радиации.

Далее опишем четыре компонента программного комплекса, реализующих его основной функционал и заявленных для регистрации в Федеральной службе по интеллектуальной собственности в качестве программ для ЭВМ.

КОМПОНЕНТ ОБРАБОТКИ ПРОЕКТА МИКРОСХЕМЫ

Основными функциями компонента обработки проекта микросхемы являются генерация модифицируемой части кода микроядра обеспечения моделирования проекта микросхемы с имитацией сбоев и его интеграция в проект микросхемы, а также обработка технологических библиотек элементов БМК серий 5521 и 5529 и ПЛИС Virtex 6 LX240T FPGA.

Исходные данные для компонента обработки проекта микросхемы:

- проект микросхемы на структурном языке Verilog;
- библиотека элементов ЦАБ на структурном языке Verilog;
- упорядоченный список элементов проекта микросхемы, в которые могут вноситься неисправности в процессе моделирования;
- библиотека элементов со средствами внесения неисправностей в базисе ЦАБ на структурном языке Verilog;
- упорядоченный список выводов проекта микросхемы, в которые будут передаваться входные воздействия;
- упорядоченный список выводов элементов в проекте микросхемы, с которых будет осуществляться чтение откликов;
- упорядоченный список выводов внутренних элементов проекта микросхемы, состояния которых подвергаются мониторингу;
- вывод сигнала тактовой частоты проекта микросхемы.

Результатами работы модуля являются:

- файл описания проекта микросхемы на структурном языке Verilog с внедренными средствами внесения неисправностей и выводами контроля значений внутренних сигналов;
- модифицированный проект микросхемы, реализованный в ПЛИС.

Компонент обработки проекта микросхемы состоит из следующих модулей:

determined. The modeling process involves several steps, in particular, testing of the source IC design, implementation in the IC design of functionality for fault injection, simulation of the operation of the obtained design in the absence and presence of failures. At each step, the monitoring signals at the outputs of the chip and internal signals specified by the user and they comparing with reference values are carried out. Analysis of simulation results allows to evaluate the tolerance of the target SoC in conditions of a given exposure to cosmic radiation.

We will describe the four components of the software system implementing its basic functionality, which are declared for registration in the Federal service for intellectual property as computer programs.

COMPONENT FOR PROCESSING OF IC DESIGN

The main functions of Component for processing of IC design are generating a modifiable part of the code of the microkernel of simulation support with simulation of failures, its integration in the project of the chip and processing of technology libraries of 5521 and 5529 gate array families and Virtex 6 LX240T FPGA.

The source data for Component for processing of IC design:

- IC design in structural Verilog language;
- library of elements of the target hardware in the structural Verilog language;
- ordered list of elements of IC design for simulation of failures;
- library of elements with means of fault injection in the basis of target hardware in the structural Verilog language;
- ordered list of terminals in IC design for input actions;

- модуль промежуточного представления структуры проекта микросхемы и генерации кода;
- модуль считывания библиотеки элементов;
- модуль модификации проекта микросхемы;
- лексический анализатор;
- синтаксический анализатор.

Лексический и синтаксический анализаторы используются в процессе анализа файла проекта микросхемы, представленного в виде кода на структурном языке Verilog.

Анализ файла проекта микросхемы производится с использованием восходящего синтаксического анализа, основанного на концепции LR-анализа [10].

КОМПОНЕНТ ГЕНЕРАЦИИ СПИСКА СБОЕВ

Основной задачей компонента генерации списка сбоев (КГСС) является генерация исходных данных о вносимых неисправностях для моделирования проекта микросхем с имитацией сбоев. Решение основной задачи КГСС подразумевает определение промежутков модельного времени между соседними фактами внесения неисправностей, определение множества элементов микросхемы для каждого факта внесения неисправностей и установление типа неисправности для каждого элемента при факте внесения неисправностей.

Компонент может работать в двух режимах: детализированном и базовом. Детализированный режим подразумевает использование стека из трех моделей [8]: внешних воздействий (МВВ), появления угроз (МПУ) и локализации неисправностей (МЛН). В этом режиме в качестве источника сбоев рассматривается космическая радиация. Базовый режим подразумевает задание параметров источников возникновения сбоев пользователем. Как следствие, в этом режиме может быть рассмотрен любой источник неисправностей, влияние которого на микросхему приводит к возникновению логических сбоев (например, инверсия бита).

Для работы КГСС в детализированном режиме задаются следующие данные:

- дата запуска космического аппарата (КА) базирования микросхемы, которая требуется для расчета солнечной активности (СА) за период эксплуатации КА (срока активного существования, САС);
- САС КА (для определения периода расчета);
- параметры орбиты КА;
- данные о плотностях энергетических спектров частиц космического пространства (КП) для различных точек околоземного пространства в различных фазах солнечной активности;
- наименования элементов микросхемы, выбранных для моделирования;
- технологические данные микросхемы, включая значение рабочей тактовой частоты и используемый уровень напряжения;
- данные устройства, реализуемого на базе целевой микросхемы, включая период его работы, а также список соединений элементов устройства.

- ordered list of terminals in IC design for reading responses;
- ordered list of terminals of the internal elements of IC design, the status of which is monitored;
- output of clock frequency of the IC design.

The results of the operation of the module are:

- IC design description file in the structural Verilog language with embedded means of fault injection and the terminals for the control of internal signals;
- modified IC design implemented in the FPGA.

Component for processing of IC design consists of the following modules:

- module of the intermediate representation of IC design structure and code generation;
- reader of library elements;
- module for modification of IC design;
- lexical analyzer;
- syntax analyzer.

Lexical and syntactic analyzers are used in the process of analysis of IC design file, presented as structured Verilog language code.

The analysis of IC design file is carried out using a bottom-up parser based LR-analysis [10].

GENERATOR OF LIST OF FAULTS

The main objective of the generator of list of faults (LFG) is the generation of source data on injected faults for simulation of IC design with simulated failures. The solution of the main task of LFG involves determining periods of model time between adjacent facts of fault injection, determining a plurality of chip elements for each case of fault injection and identification of type of fault for each element at each fault injection.

The component can operate in two modes: basic and detailed. Detailed mode involves the use

Для работы КГСС в базовом режиме задаются следующие данные:

- типы частиц, воздействующих на микросхему (требуется выбрать из базы данных внешних воздействий или создать новый тип);
- наименования элементов микросхемы, выбранных для моделирования;
- рабочая тактовая частота микросхемы;
- период работы устройства;
- список соединений элементов устройства.

Тип частиц характеризуется законом распределения времени до следующего попадания частицы данного типа в микросхему, вероятностью возникновения каждого типа сбоев при попадании частицы данного типа в микросхему, а также площадью поражения, определяющей радиус окружности в плоскости микросхемы, с центром в точке падения частицы (все элементы, находящиеся в пределах этой окружности, подвержены влиянию данной частицы).

Результатом работы КГСС является список сбоев, состоящий из заголовка "параметры моделирования" и последовательно расположенных данных нескольких экспериментов. Заголовок "Параметры моделирования" содержит поля "Параметры орбиты КА" и "Дата старта КА". Данные каждого эксперимента содержат заголовок "заголовок эксперимента" и массив из k пакетов моделирования. "Заголовок эксперимента" содержит следующие поля:

- массив имен элементов микросхемы, моделируемых в данном эксперименте;
- координаты моделируемого участка орбиты;
- данные о моделируемых потоках заряженных частиц КП на данном участке орбиты;
- комментарий, описывающий особенности эксперимента.

Каждый пакет моделирования состоит из полей "Смещение" и "Массив сбоев". Значение поля "Смещение" характеризует временной интервал между предыдущим актом внедрения неисправностей в проект целевой микросхемы и актом внедрения неисправностей, описанных в данном пакете. Смещение измеряется в тактах рабочей тактовой частоты моделируемого устройства.

Размерность массива сбоев равна количеству элементов, выбранных для моделирования в данном эксперименте. Каждый элемент массива содержит код неисправности, которая соответствует моменту модельного времени, определяемому значением поля "Смещение".

КОМПОНЕНТ ГЕНЕРАЦИИ ТЕСТОВЫХ ВОЗДЕЙСТВИЙ

Компонент генерации тестовых воздействий (КГТ) предназначен для формирования векторов входных сигналов, подаваемых в процессе контроля сбоеустойчивости микросхемы. Тестовые воздействия формируются на этапе функционального тестирования на основе информации о входных воздействиях и эталонных откликах, полученных при разработке проекта целевой микросхемы. КГТВ выполняет следующие функции:

of a stack of three models [8]: of external influences (MEI), of emergence of threats (MET) and of fault localization (MFL). In this mode, the cosmic radiation is considered as the source of the failure. The basic mode assumes that the user specifies the parameters of the sources of failures. As a consequence, any source of faults, the impact of which on the chip leads to logical failures (e.g., bit flip), can be considered in this mode.

To operate in detailed mode the following data are given:

- date of launch of the spacecraft (SC) with chip, which is required for the calculation of solar activity (SA) during the period of operation of the SC (active lifetime, AL);
- AL of SC (to define the calculation period);
- parameters of SC orbit;
- data on the densities of the energy spectra of space particles for different locations in near-Earth space in different phases of solar activity;
- names of elements of the chip selected for modeling;
- process data of the chips, including the value of operating clock frequency and the voltage level;
- data of the device, implemented on the basis of the target IC, including the period of his work, as well as a list of connections of elements of the device.

To operate in basic mode the following data are given:

- types of particles that act on the chip (it is required to select from the database of external influences or to create new type);
- names of elements of the chip selected for modeling;
- operating clock frequency of the chip;
- period of operation of the device;

- анализ исходного файла данных о входных воздействиях и эталонных откликах, полученного на предыдущих этапах разработки;
- на основе полученной информации формируются массивы векторов входных воздействий и эталонных откликов;
- передача векторов входных воздействий компоненту обеспечения моделирования проекта микросхемы с имитацией сбоев, выполняющему функции управления остальными компонентами программного комплекса.

Исходными данными для компонента генерации тестовых воздействий являются:

- исходный файл данных о входных воздействиях и эталонных откликах;
- список имен выводов проекта микросхемы, в которые будут передаваться входные воздействия;
- список имен выводов проекта микросхемы, с которых будет осуществляться чтение откликов;
- наименование входного вывода моделируемого проекта микросхемы, используемого в качестве сигнала тактовой частоты;
- активный фронт сигнала тактовой частоты.

Выходными данными компонента генерации тестовых воздействий являются массивы векторов входных воздействий и векторов эталонных откликов.

КОМПОНЕНТ ОБРАБОТКИ РЕЗУЛЬТАТОВ МОДЕЛИРОВАНИЯ

Компонент обработки результатов моделирования проекта микросхемы предназначен для контроля моделирования проекта микросхемы с имитацией сбоев путем сравнения массивов векторов откликов, полученных в результате моделирования в условиях наличия и отсутствия сбоев, с массивом векторов эталонных откликов. Массив векторов эталонных откликов может быть получен как результат работы КГТВ после функционального тестирования маршрута моделирования проекта микросхемы с имитацией сбоев.

Компонент обработки результатов моделирования проекта микросхемы предназначен для решения следующих задач:

- обнаружение в проекте микросхемы блоков, в которых наиболее вероятно возникновение сбоев;
- проверка функциональной эквивалентности исходного проекта микросхемы в ЦАБ и проекта микросхемы в базисе ПЛИС на этапе функционального тестирования, а также эквивалентности последнего модифицированному проекту микросхемы с внедренными средствами внесения неисправностей на этапе моделирования с имитацией сбоев;
- контроль сбоеустойчивости исходного проекта микросхемы по результатам моделирования работоспособности модифицированного проекта микросхемы в условиях наличия сбоев;
- определение последствий возникновения сбоев в функционировании микросхемы;
- формирование отчета о результатах моделирования проекта микросхемы с имитацией сбоев;

- list of connections of the elements of the device.

Type of particles is characterized by the distribution law of time between influences of particles of same type, by the probability of occurrence of each type of failure when hit by particles of a given type, and by the area of the lesion, which determines the radius of the circle in the plane of the chip, centered at the point of incidence of the particles (all elements within this circle, will be affected by this particle).

The result of operation of LFG is the list of faults consisting of a header "simulation parameters" and consecutive data of several experiments. The title "simulation parameters" contains the fields "SC orbit parameters" and "start date of SC". Data of each experiment contain the heading "title of experiment" and an array of k simulation packages. "Title of experiment" contains the following fields:

- array of names of elements of the chip, simulated in this experiment;
- coordinates of the simulated site of the orbit;
- data on the modulated streams of charged cosmic particles at the site of the orbit;
- comment describing the features of the experiment.

Each modeling package consists of the fields "offset" and "massive of failures". The value of the "offset" describes the time interval between the last fault injection into IC design and fault injection that is described in this package. The offset is measured in cycles of the working clock frequency of the simulated device.

Dimension of an array of failures is equal to the number of elements selected for modeling in this experiment. Each array element contains the code of the fault that corresponds to the

- формирование временных диаграмм внутренних сигналов проекта микросхемы в процессе моделирования.

Исходные данные для данного компонента:

- тип выполняемого этапа моделирования;
- информация о результате выполнения предыдущего этапа моделирования;
- векторы входных воздействий, а также параметры вносимых сбоев для каждого такта моделирования;
- наименования элементов, в которые вносятся сбои;
- список контрольных точек моделируемого проекта микросхемы (выходов внутренних элементов микросхемы, значения сигналов на которых подлежат мониторингу);
- векторы эталонных откликов;
- векторы откликов, полученных в процессе моделирования проекта микросхемы;
- модуль промежуточного представления структуры проекта микросхемы и генерации кода;
- информация об иерархической структуре проекта микросхемы;
- данные о площадях, занимаемых элементами библиотеки ЦАБ.

Результатами работы компонента являются файл отчета, содержащий информацию о результатах выполненного этапа моделирования проекта микросхемы с имитацией сбоев, а также файл формата vcd для отображения временных диаграмм сигналов проекта микросхемы. Файл отчета содержит следующую информацию:

- общее время моделирования;
- количество переданных векторов входных воздействий и векторов эталонных откликов;
- количество полученных в результате моделирования векторов откликов проекта микросхемы;
- результат сравнения массива векторов эталонных откликов и откликов, полученных в процессе моделирования;
- список наименований выходов микросхемы, в которых обнаружены несовпадения значений сигналов с эталонными;
- статистическая информация об обнаруженных несоответствиях для каждого вывода проекта микросхемы и контрольной точки, включающая общее количество обнаруженных несовпадений, а также локализация тактов моделирования, на которых обнаружены несоответствия эталонным значениям;
- статистическая информация о сбоях, внесенных в процессе моделирования (для этапа моделирования с внесением неисправностей);
- результат контроля сбоеустойчивости проекта микросхемы, определяющий влияние сбоев на его работоспособность (для этапа моделирования с внесением неисправностей).

Микросхема считается работоспособной в условиях воздействия источников сбоев в случае совпадения значений сигналов на выходах проекта микросхемы с соответствующими эталонными значениями на каждом этапе моделирования.

moment of the model time determined by the value of the field "offset".

GENERATOR OF TEST INPUTS

Generator of test inputs (TIG) is used to form vectors of input signals during the control of failure stability of the chip. Test inputs are formed at the stage of functional testing on the basis of information about inputs and reference responses obtained during the development of design of the target IC.

Generator of test inputs performs the following functions:

- analysis of the source data on inputs and the reference responses received at the previous stages of development;
- on the basis of the obtained information the arrays of vectors of input signals and a reference responses are generated;
- transfer of vectors of input signals to the component for simulation support that controls other components of the software system.

The source data for the generator of test inputs are:

- source file of data on inputs and reference responses;
- list of the names of the terminals of IC design, which will transmit the input signals;
- list of the names of the terminals of IC design, which will be used for reading of the responses;
- name of the terminal of IC design, which will be used as the clock;
- active front of the clock.

The output data for the generator of test inputs are arrays of vectors of input signals and of vectors of reference responses.

COMPONENT FOR PROCESSING OF SIMULATION RESULTS

Component for processing of simulation results of IC design is intended to control the simulation

ПЕРСПЕКТИВЫ

В статье представлена совокупность программных модулей, входящих в состав экспериментального образца ПАК контроля сбоеустойчивости проекта микросхемы. Эти модули обеспечивают выполнение всех стадий моделирования микросхемы в процессе определения ее сбоеустойчивости. Используемые технические решения позволяют осуществлять гибкий выбор источников возникновения сбоев в микросхеме и получить детальную информацию о локализации критических сбоев, приводящих к отказу моделируемой системы. Использование ПЛИС-прототипирования ускоряет процесс контроля сбоеустойчивости по сравнению с применением программных симуляторов. Расширенный метод внесения неисправностей обеспечивает снижение затрат на определение сбоеустойчивости микросхемы, позволяя отказаться от использования ускорителей частиц.

В качестве основных направлений дальнейшего развития ПАК для контроля сбоеустойчивости, в частности его программной составляющей, можно выделить обеспечение возможности определения скорости восстановления устройства после критического сбоя, поддержку динамической генерации внешних воздействий на основе текущих откликов микросхемы, а также интеграцию более совершенных моделей МВВ, МПУ и МЛН в разрабатываемый комплекс.

Разработка проводилась при поддержке Министерства образования и науки РФ в рамках федеральной целевой программы "Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы". Уникальный идентификатор прикладных научных исследований RFMEFI57715X0161.

ЛИТЕРАТУРА

1. **Petersen E.** Single Event Effects in Aerospace. 1 ed. Wiley-IEEE Press. 2011. P. 520.
2. **Straka M., Kastil J., Kotasek Z.** SEU Simulation Framework for Xilinx FPGA: First Step Towards Testing Fault Tolerant Systems. 14th Euromicro Conference on Digital System Design, 2011.
3. **Pellegrini A., Constantinides K., Zhang D., Sudhakar Sh., Bertacco V., Austin T.** CrashTest: A fast high-fidelity FPGA-based resiliency analysis framework. Computer Design. 2008. ICCD 2008. IEEE International Conference, 2009.
4. **Civera P., Macchiarulo L., Rebaudengo M.** Exploiting FPGA-based techniques for fault injection campaigns on VLSI circuits. Defect and Fault Tolerance in VLSI Systems, 2001. Proceedings. 2001 IEEE International Symposium, 2002.
5. **Burlyaev D., Van Leuken R.** System fault-tolerance analysis of COTS-based satellite on-board computers // Microelectronics Journal. 2014. Vol. 45. P. 1 335–1 341.
6. **Rudrakshi S., Midasala V., NagaKishore Bh.** Implementation of FPGA Based Fault Injection

of the project components with simulated failures by comparing arrays of vectors of responses obtained through simulation in the presence and absence of faults with an array of vectors of reference responses. An array of vectors of reference responses can be obtained as a result of operation of TIG after functional testing of the route of IC design simulation with simulated failures.

Component for processing of simulation results of IC design is aimed to solve the following tasks:

- detection in IC design units, in which fault occurrence is the most likely;
- verification of functional equivalence of the source IC design in the target hardware and IC design in the basis of FPGA at the stage of functional testing, as well as of the equivalence of the last to the modified design with embedded means of fault injection at the stage of modelling with simulated faults;
- control of failure-stability of source IC design based on the simulation results of operability of the modified IC design in the presence of failures;
- determination of the consequences of failure in the operation of the chip;
- generation of report with results of the simulation of the IC design with simulated failures;
- formation of a timing chart of internal signals of the IC design in the modeling process.

The source data for this component:

- type of the performed simulation phase;
- information about the result of the previous stage of the simulation;
- vectors of input signals and the parameters of injected faults for each cycle of the simulation;

Tool (FITO) for Testing Fault Tolerant Designs // IACSIT International Journal of Engineering and Technology. 2012. Vol. 4. № 5. P. 522–526.
7. **Brekhov O., Klimenko A., Kordover K., Ratnikov M.** FPGA-Prototyping with Advanced Fault Injection Methodology for Tolerant Computing Systems Simulation. DCCN 2015. Moscow, 2016.
8. **Klimenko A., Brekhov O.** Hardware-software simulation complex for FPGA-prototyping of fault-tolerant computing systems. Distributed Computer and Communication Networks: Control, Computation, Communications (DCCN-2016), 2016.
9. 1800–2012. IEEE Standard for System Verilog // Unified Hardware Design, Specification and Verification Language. Inc. ed., N.-Y.: IEEE, 2013.
10. **Ахо А., Лам М., Сети Р., Ульман Д.** Компиляторы: принципы, технологии и инструментарий. – ИД "Вильямс", 2008.

- names of elements for fault injection;
- list of control points of IC design (outputs of the internal components of the chip, the values of signals which should be monitored);
- vectors of the reference response;
- •vectors of responses obtained in simulation of the IC design;
- module of the intermediate representation of IC design structure and code generation;
- information about the hierarchical structure of IC design;
- information about areas of elements of the target hardware library.

The results of the operation of the component is the report file that contains information about the results of the modeling stage of IC design with simulated failures, and the file of vcd format to display the time diagrams of signals of IC design. The report file contains the following information:

- total simulation time;
- number of transferred vectors of input actions and vectors of reference response;
- number of obtained vectors of responses of IC design;
- result of the comparison of the array of reference vectors of responses and responses obtained in the simulation;
- list of names of outputs of the chip with mismatch of values of signals with a reference;
- statistical information about the inconsistencies found for each output of IC design and control point, including the total number of detected mismatches and localization of cycles of modeling with mismatches of the reference values;
- statistical information about the faults injected in the simulation process (for stage of simulation with fault injection);
- result of control of the failure tolerance of IC design, which determines the impact of failures on its performance (for stage of simulation with fault injection).

The chip is considered operable in conditions of influence of sources of failures in the case of coincidence of the values of the signals at the outputs of IC design with the corresponding reference values at each stage of the simulation.

PROSPECTS

The paper presents a set of software modules of the prototype of HSS for control of fault tolerance of IC design. These modules provide all simulation stages of IC design in the process of defining its failure-stability. The applied technical solutions allow to realize a flexible choice of sources of failures in the chip and to obtain detailed information about the localization of the critical faults that caused a failure of the simulated system. The use of FPGA prototyping accelerates the control of fault tolerance in comparison with the use of software simulators. An advanced method of fault injection provides a reduction in costs in the determination of the failure tolerance of the chip, allowing to abandon the use of particle accelerators.

As the main areas of further development of the HSS for control of fault tolerance, in particular, of its software component, we can highlight the determining of the speed of recovery of the device after a critical failure, support of dynamic generation of external influences based on current feedback of the chip, as well as the integration of more sophisticated MEI, MET and MFL into the proposed complex. ■

The development was carried out with the support of the Ministry of education and science of the Russian Federation in the framework of the Federal Targeted Programme for Research and Development in Priority Areas of Development of the Russian Scientific and Technological Complex for 2014-2020. Unique identifier of applied research RFMEFI57715X0161.