АППАРАТНЫЕ ТРОЯНЫ. ЧАСТЬ 1: НОВЫЕ УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ

HARDWARE TROJANS. PART 1: NEW THREATS TO CYBER SECURITY

УДК 621.382, ВАК 05.27.01

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

В первой части цикла обзорных статей, посвященных аппаратным закладкам в интегральных схемах, – аппаратным троянам – рассмотрены потенциальные угрозы кибербезопасности, которые они несут. Анализируются возможные пути их несанкционированного внедрения. Для выработки методов и стратегий борьбы, предупреждения, выявления и противодействия приведена всесторонняя классификация аппаратных троянов.

In the first part of the cycle of reviews dedicated to hardware Trojans in integrated circuits potential threats to cyber security are considered. The possible ways of their unauthorized insertion are examined. For development of methods and strategies of prevention, detection and counteraction, the comprehensive classification of hardware Trojans is presented.

За последние десятилетия электронные системы от компьютеров до средств автоматизации, управления и контроля прочно вошли в нашу повседневную жизнь, и затрагивают все ее стороны. Построение и функционирование таких систем основано на интегральных микросхемах (ИС). ИС являются элементной базой всех современных электронных систем, обрабатывающих информацию в важнейших отраслях, включая финансовый, промышленный, оборонный и транспортный сектор. Проблема надежности и безопасности выполнения ИС своих функций тесно связана с обеспечением кибербезопасности электронных систем. В последнее время в связи с глобализацией и увеличивающейся сложностью ИС, эта проблема приобретает все большую актуальность. Без ее решения электронные системы могут не только не выполнять те функции, которые заложены в них согласно спецификации, но и выступать проводником внешних злонамеренных атак на систему.

В последние годы появились новые потенциальные угрозы безопасности в рассматриваемой сфере, основанные на аппаратных средствах, – так называемые аппаратные закладки или аппаратные трояны, которые представляют собой намеренную злоумышленную модификацию электрической схемы или ее конструкции, приводящую к некорректному функционированию электронного устройства. Подобно программной закладке (программному трояну), аппаратная закладка представляет собой своего рода черный вход в электронное устройство. При этом аппаратный троян обладает дополнительным преимуществом – он постоянно присутствует на самом низком уровне обработки информации, что ведет к сохранению угроз отказа или отклонения от нормального функционирования ИС на протяжении всего времени использования электронного устройства, причем проблему невозможно предотвратить никакими программными или аппаратными средствами защиты. Несанкционированной модификации может быть подвержен любой тип ИС и, это может быть причиной, как несущественных частичных сбоев, так и полного отказа системы. Аппаратный троян может воздействовать на систему самостоятельно, а может активироваться программным обеспечением, в которое преднамеренно заложена такая возможность. Аппаратная закладка может долгое время оставаться бездействующей и активироваться через заданное время, внешним воздействием или

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

некоторыми определенными активными процессами в работе ИС. Спектр аппаратных закладок – их возможности, размеры, механизмы срабатывания, потребляемая мощность – огромен, что в совокупности с увеличивающейся сложностью ИС, как на физическом, так и на функциональном уровнях, предоставляют широкие возможности злоумышленнику для скрытного размещения аппаратных троянов.

Относительная простота внедрения аппаратных закладок в современную ИС не может не вызывать беспокойство. Модификации могут быть внесены в аппаратную часть ИС как на этапе разработки, так и в процессе производства, включая такие стадии как спецификация, проектирование, верификация и изготовление. Более того, аппаратная закладка может быть внесена в уже изготовленную ИС [1]. Ситуация осложняется тем, что современные тенденции в полупроводниковой промышленности характеризуются разделением разработки и изготовления ИС, причем последнее выполняется несколькими фабриками, разбросанными по всему миру, преимущественно в Азии. Привлечение сторонних соисполнителей характерно не только для изготовления ИС, но и для проектирования: разработчики пользуются сторонним программным обеспечением, широко используют готовые блоки (IP-блоки), спроектированными третьей стороной. IP-блоки часто поставляются в бинарном виде и проектируются сторонними фирмами, специализирующимися на определенных технических проектах. Поэтому аппаратный троян может быть простым изменением параграфа в спецификации, дополнительной строкой в исходном коде, написанном на языке описания аппаратуры (HDL), или же модификацией кремниевого кристалла на производственной фабрике, например, небольшим изменением топологии транзистора. Если изменение выполнено в диффузионном слое, то на чипе оно становится практически "невидимым" [2].

В настоящее время проблема аппаратных закладок всесторонне исследуется в мире. Так, политехническим институтом Нью-Йоркского Университета ежегодно проводятся соревнования между командами по внедрению и поиску специальных устройств [3], что способствует развитию технологий предупреждения внедрения и методов обнаружения аппаратных троянов. Агентство по перспективным оборонным научно-исследовательским разработкам США (DARPA) инициировала в 2007 году специальную программу по обеспечению аутентичности используемых в военных системах США микросхем и проводит НИОКР по развитию методов и технологий обнаружения аппаратных закладок [4]. Большинство других публикуемых исследований проводится университетскими группам и в основном посвящены методам предотвращения внедрения троянов при разработке ИС, а также способам их выявления в ИС после изготовления.

Если аппаратный троян когда-либо был внесен в систему, то он присутствует всегда неза-

Over the past decade, electronic systems from computers to automation, control and monitoring tools have become part of our everyday lives and affecting all sides of it. The structure and operation of such systems are based on integrated circuits (IC). IC is a base for all modern electronic systems that process information in key sectors, including finances, industry, defense and transport. The problem of reliability and safety of operation of IC is closely connected with cyber security of electronic systems. Recently, in connection with globalization and the increasing complexity of IC, this issue is becoming increasingly important. Without its solution the electronic systems can not only perform the functions according to their specification, but also to be a conductor for external malicious attacks on the system.

In recent years, there were new potential security threats in this sphere, based on the so-called hardware Trojans – a malicious modifications of electric connection or design, leading to incorrect operation of the electronic device. Hardware Trojan, like software one, is a kind of back door into the electronic device. But hardware Trojan has an additional feature – he is always presented at the lowest level of information processing, which leads to the conservation threats of failure or deviation from normal functioning of the IC for the entire usage time of the electronic device, and the problem cannot be prevented by any software or hardware protection. Any type of IC may be subject to unauthorized modification, and this may be the cause of both minor and serious failures. A hardware Trojan can influence the system independently, or can be activated by the software, in which such possibility was intentionally provided. A

висимо от того, включена она или выключена. Потенциально он может нарушить работу всей системы, если внесен в любую из составляющих ее ИС. Воздействие аппаратных троянов может варьироваться от простых целевых атак до сложных атак, которые обеспечивают точку опоры программным атакам высокого уровня. К целевым, в частности, относятся следующие атаки:

- изменение бита информации, нарушающего целостность хранимых данных;
- ослабление функциональности криптографических ядер;
- атаки, приводящие к утечке конфиденциальной информации.

Система может быть инфицирована несколькими аппаратными закладкам, которые совместными действиями подрывают ее безопасность.

Для полного понимания воздействия аппаратных троянов на системы и их обнаружения необходимо изучение возможностей изменения информации при внедрении закладок, а также возможных механизмов их активации. Поэтому исследования возможных угроз, которые несут трояны, разработка конструкции и методов их внедрения, механизмов активации являются необходимой частью работы в поиске способов предупреждения внедрения, выявления и противодействия аппаратным закладкам для обеспечения безопасности используемых ИС.

При рассмотрении возможных угроз безопасности, исходящих от аппаратной закладки, и определения ее влияния на информационную систему целесообразно структурировать характерные признаки троянов. Для описания таких характерных свойств было предложено несколько классификаций аппаратных троянов. Цели таких классификаций – систематизация изучения, разработка общих методов обнаружения и подходов, обеспечивающих подавление воздействия различных классов троянов, а также сравнение разных методов противодействия. На рис.1 приведена наиболее полная классификация аппаратных троянов, предложенная в статье [5]. В основе этой классификации учитываются как фазы разработки ИС, так и уровни возможного внедрения аппаратных троянов.

Разработка и изготовление ИС, как правило, включают такие этапы, как спецификация ИС, ее разработка, изготовление, тестирование и сборка. Они должны рассматриваться и как стадии, на которых злоумышленник может внедрить аппаратную закладку. На этапе спецификации (подготовки технического задания) определяются характеристики системы, в том числе используемые модели и предполагаемая функциональность ИС. После этого этапа характеристики системы реализуются на стадии проектирования в определенном целевом конструктивно-технологическом базисе с учетом функциональных и физических ограничений. На этапе производства ИС изготавливается комплект фотошаблонов, и проводится цикл изготовления кристаллов ИС на кремниевых пластинах с последующей проверкой их функциональных и физи-

hardware Trojan can long time to remain dormant and be activated after a specified time, by external influence or as a result of defined processes in the operation of IC. Range of hardware Trojans, the capabilities, sizes, principles of operation, power consumption, is huge, which together with the increasing complexity of IC, both on physical and functional levels, offer wide opportunities for the attacker to surreptitiously embed hardware Trojans.

The relative ease of insertion of hardware Trojans into modern IC is an additional cause for concern. Modifications can be made to the hardware both in the development phase and in the production process, including such stages as specification, design, verification and manufacturing. Moreover, a hardware Trojan can be included in already made IC [1]. The situation is complicated by the fact that current trends in the semiconductor industry are characterized by the separation of development and production of IC, and the latter can be done by several factories scattered around the world, mainly in Asia. Engaging third-party subcontractors is typical not only for IC manufacturing, but also for design: developers use third-party software and ready-made blocks (IP cores), designed by a third party. IP cores are often supplied in binary form and are designed by third-party firms specializing in certain technical projects. Therefore, a hardware Trojan can be a simple change of paragraph in the specification, an additional line in the source code written in hardware description language (HDL), or a modification of the silicon chip in a factory, for example, a small change in the topology of the transistor. If the change is made in the diffusion layer, on the chip it becomes practically "invisible" [2].

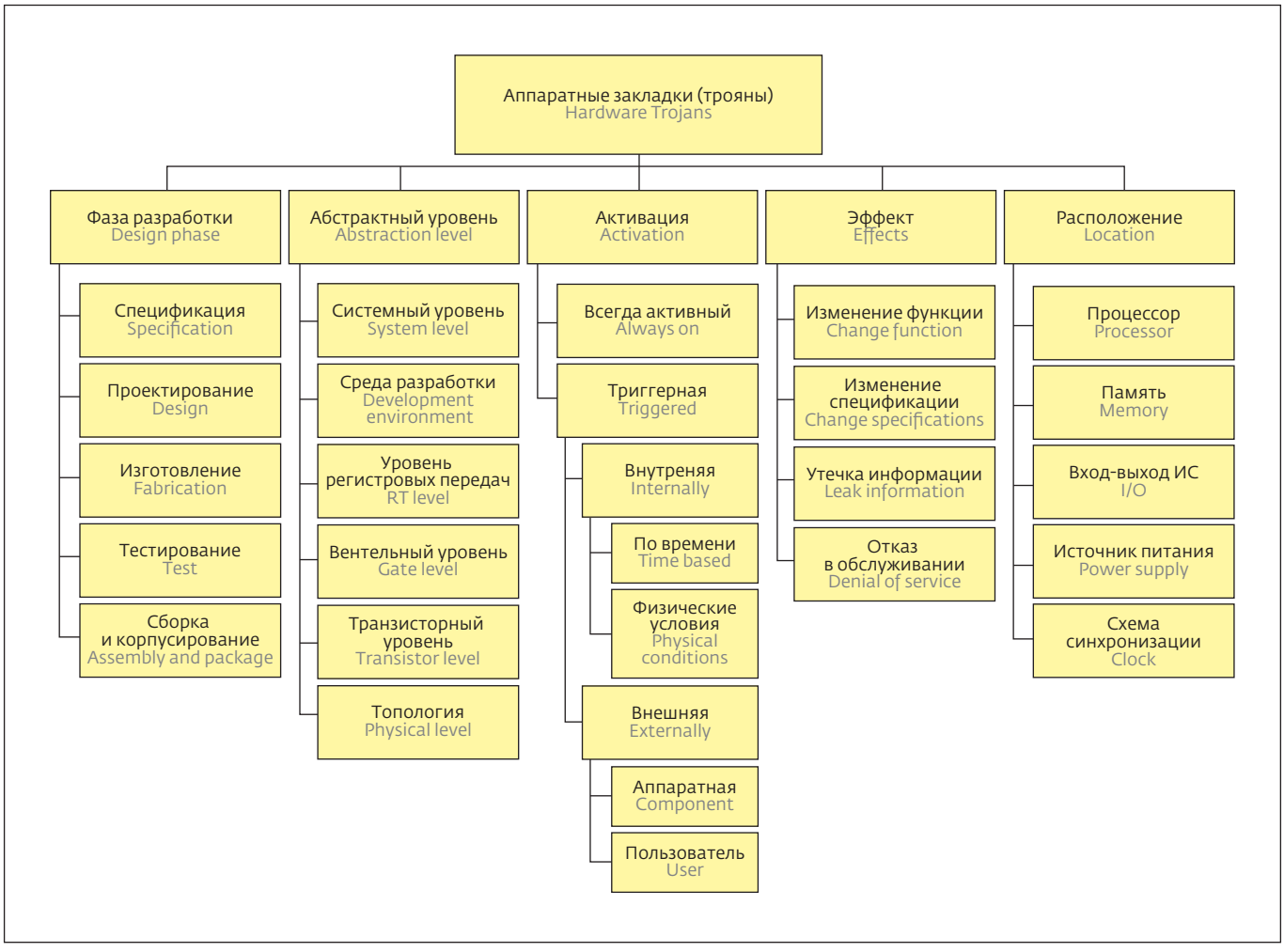


Рис.1. Классификация аппаратных троянов [5]
Fig.1. Classification of hardware trojans [5]

Currently, the problem of hardware Trojans is studied comprehensively in the world. For example, the Polytechnic Institute of New York University annually organizes competitions between teams for insertion and search of special devices [3], which contributes to the development of technologies for preventing the insertion and methods for the detection of hardware Trojans. The Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense has initiated in 2007 a special program to ensure the authenticity of IC used in military systems of the USA and conducts R&D on the development of methods and technologies to detect hardware Trojans [4]. The majority of other published studies is conducted in universities and mainly focuses on how to prevent the insertion of Trojans during the development of IC, as well as on methods for their identification in the IC after fabrication.

If a hardware Trojan was ever inserted into the system, it is always present regardless of whether is the device on or off. If the Trojan is inserted to any of system's IC, he has the potential to disrupt the entire system. The impact of hardware Trojans can range from a simple targeted attacks to complex attacks, which provide the fulcrum for high-level software-based attacks. Target attacks, in particular, include the following:

- change bits of information that violates the integrity of the stored data;
- weakening the functionality of the cryptographic cores;
- attack leading to the leakage of confidential information.

The system can be infected with several hardware Trojans, which joint actions undermine its security.

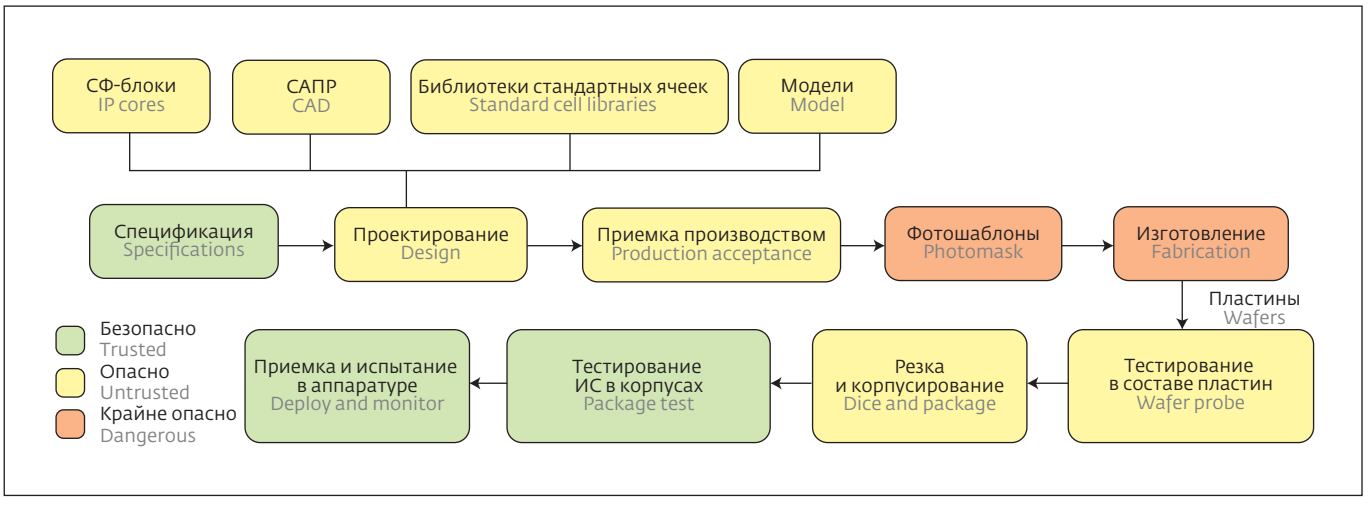


Рис.2. Стадии производства ИС и соответствующие уровни опасности внедрения аппаратной закладки [6]
Fig.2. Stages of IC manufacturing and corresponding levels of risk of insertion of hardware trojans [6]

ческих характеристик. Далее проводится резка пластин на чипы, их корпусирование, тестирование готовых к эксплуатации ИС, испытание и приемка. На рис.2 приведены стадии производства ИС и соответствующие им оценки уровней опасности внедрения аппаратной закладки [6].

Неуязвимыми с точки зрения внедрения аппаратных троянов являются только стадии спецификации, тестирования в корпусе, а также испытания и приемки. Все остальные стадии уязвимы к внедрению аппаратных троянов, и безопасность ИС на них определяется соисполнителями, которые обеспечивают изготовление ИС и ее тестирование, а также поставщиками средств разработки, IP-блоков и библиотек. Но даже стадии, которые отмечены выше как безопасные, могут быть подвержены влиянию злоумышленника, например, возможна настройка аппаратной закладки во время тестирования или во время поставки ИС. Поэтому полный цикл производства ИС должен быть всесторонне исследован с рассмотрением как стратегий эффективной профилактики внедрения троянов, так и технологий их обнаружения.

Трояны могут внедряться в любые элементы информационной системы. Локализация трояна

To fully understand the impact of hardware Trojans on the system and for their detection it is necessary to study the possibilities of data change in case of the insertion of Trojans, and also possible mechanisms of their activation. Therefore, investigation of the possible threats caused by Trojans, development of design and methods of their insertion and activation are a necessary part of the work in finding ways for prevention the insertion, and for detection and countering hardware Trojans to ensure the safety of the used IC.

For consideration of possible security threats caused by hardware Trojan, and determination of its impact on the information system, it is advisable to structure the characteristic signs of Trojans. To describe such characteristic properties several classifications of hardware Trojans were proposed. The purpose of such classifications is the systematization of the study, the development of common detection methods and approaches providing suppression of the effects of different classes of Trojans as well as comparison of different methods of counteraction. Fig.1 shows the most complete classification of hardware Trojans, proposed in the paper [5]. This classification takes into account both the phases of development of IC and levels of the possible insertion of hardware Trojans.

Development and manufacture of IC generally include such steps as specification of IC, its development, production, testing and packaging. They should be considered also as the stages on which the attacker can insert a hardware Trojan. At the specification stage, the characteristics of the system are defined, including used models and the estimated functionality of IC. After this phase the system features are implemented at

может ограничиваться отдельным компонентом, а может быть рассредоточена и на нескольких компонентах, таких как процессор, память, схемы входа-выхода, источники питания или схемы синхронизации. Особенность локализации определяется сложностью проекта ИС, трудностью внедрения и тем эффектом, который должен вызвать аппаратный троян. В связи с этим необходимо исследовать возможные механизмы работы аппаратных троянов, и на характерных примерах рассмотреть последствия, которые можно ожидать от их внедрения. Тем самым можно охарактеризовать угрозы, связанные с аппаратными троянами.

Аппаратные закладки являются относительно новыми угрозами кибербезопасности, при этом они существенно расширяют возможности для атаки на информационные системы. Ранее атаки ограничивались только программными средствами, сосредотачиваясь на слабых местах программного обеспечения. Средства защиты конкретного программного обеспечения разрабатывались исходя из аутентичности аппаратного обеспечения, поэтому общепринятые подходы к защите программными средствами не способны обеспечить безопасность от аппаратных троянов. С этой точки зрения аппаратные закладки представляют достаточно сложную проблему обеспечения безопасности.

Трояны могут быть внедрены в ИС специализированного назначения (ASIC), в коммерческие электронные компоненты, находящиеся в свободной продаже (COTS – Commercial Off The Shelf), микропроцессоры, цифровые сигнальные процессоры или в виде программных изменений в "прошивке" ПЛИС (FPGA). Учитывая, что изменения вносятся на самый низкий уровень системы, типы нарушающего действия могут иметь разнообразный характер. Эти воздействия можно условно классифицировать как изменение функциональности, изменения спецификации, утечка информации или отказ в обслуживании. Специфические аппаратные трояны могут реализовать любое из этих нарушающих воздействий.

Аппаратные трояны, изменяющие функциональность ИС через внедрение дополнительной логической схемы или посредством выключения части существующей логики, непосредственно ставят под угрозу целостность и сохранность информационной системы. Изменение данных в памяти, воздействие на вычислительные операции или на коммуникационный канал являются характерными целями рассматриваемого внедрения. Модификации функциональности могут носить очень разнообразный характер; воздействия этого класса аппаратных троянов ограничены только ресурсами системы, воображением и умением злоумышленника. Например, в [7] представлен сценарий, в котором простая деструктивная аппаратная закладка может вставить ошибку в алгоритм на основе китайской теоремы об остатках при вычислении криптографического алгоритма с открытым ключом (RSA), что приводит к компрометации RSA- ключа.

the design stage on a certain constructive and technological basis taking into account the functional and physical constraints. At the production stage a set of photomasks is prepared, and the manufacturing of the chips on silicon wafers with subsequent verification of their functional and physical characteristics is carried out. Further cutting of wafers, packaging of chips, testing of ready for operation IC and acceptance are carried out. Fig.2 shows the stages of production of IC and corresponding assessment levels of the risk of insertion of the hardware Trojans [6].

Only specification, test in package, and acceptance are invulnerable from the point of view of the insertion of hardware Trojans. All other stages are vulnerable to the insertion of hardware Trojans, and the security of the IC is determined by subcontractors, which provide production of IC and their testing, as well as by suppliers of development tools, IP cores and libraries. But even stages, which are marked above as "safe", can be influenced by an attacker, for example, it is possible to configure a hardware Trojan during testing or supply of IC. Therefore, a complete production cycle of IC needs to be thoroughly investigated with the consideration of strategies to effectively prevent the insertion of Trojans and technologies for their detection.

Trojans can be inserted in any elements of the information system. Localization of a Trojan may be limited to a separate component, and may be dispersed on several components such as processor, memory, input/output circuits, power supply or synchronization circuit. Location is determined by the complexity of the project, the difficulty of insertion, and the effect, which

В работе [5] приводится пример модификации, в результате которой модуль обнаружения ошибок принимает входные сигналы, которые должны быть отклонены.

Непосредственные ошибки в ИС, как например Pentium FDIV (ошибка в модуле операций с плавающей запятой в оригинальных процессорах Pentium выпуска 1994 года), могут быть воспроизведены аппаратной закладкой, причем для предотвращения ее обнаружения может использоваться выборочное включение. Специальные аппаратные трояны могут разрабатываться для изменения порядка выполнения инструкций центрального процессора, утечки данных через побочные каналы, изменения содержимого программируемой постоянной памяти (PROM).

Изменение функциональности системы может быть использовано для поддержки более широких атак. Так, в работе [6] отмечено, что возможности нанесения ущерба безопасности существенно увеличиваются при совместном использовании аппаратной и программной атаки. В качестве примера приведены изменения в центральном процессоре, поддерживающие атаку на программное обеспечение. В итоге предоставление доступа к памяти и модификация программы способствуют расширению полномочий с последующим доступом в систему через черный вход и атакой с кражей пароля.

Изменяющие спецификацию аппаратные трояны характеризуются тем, что искажают параметрические свойства целевой ИС или спецификации, не относящиеся к ее функциональности. Такие параметрические свойства включают синхронизацию или временные характеристики, а также потребляемую мощность ИС. Эффект достигается путем непосредственного изменения внутренних физических свойств – топологии межсоединений и геометрии транзисторных структур. В отличие от аппаратных троянов, которые влияют на функциональность, для этого класса характерны изменения топологии линий разводки и транзисторов, и их разрушительные действия могут приводить к отказам системы [6]. Можно предположить, что в дополнение к рассматриваемым модификациям может быть включена и такая аппаратная закладка, чтобы изменение спецификации имело триггерный или активационный механизм. Для рассматриваемого класса характерны различные типы воздействий на ИС, включая ограничение вычислительных возможностей системы путем внесения в схему генератора системной частоты, модификация вычислительных блоков или ячеек входа-выхода, при которой функциональность этих узлов не изменяется, но ухудшаются пропускные и динамические характеристики. Изменение размещения вентилей или разводки схемы, функционально эквивалентное, но при этом имеющее более высокие паразитные составляющие пассивных элементов, обуславливает ухудшение рабочих характеристик при высокой нагрузочной актив-

should be caused by hardware Trojan. In this regard, it is necessary to investigate the possible mechanisms of operation of hardware Trojans, and to consider, with examples, the effects that can be expected from their insertion. Thus it is possible to describe threats related to hardware Trojans.

Hardware Trojans are relatively new threats to cybersecurity, and they significantly expand the possibilities for attack on the information systems. Previously, attacks were limited to software only, focusing on weak areas of the software. Protection software was developing on the basis of the authenticity of the hardware, so conventional approaches to protecting software are not able to provide security against hardware Trojans. From this point of view, the hardware Trojans are rather complex problem of security.

Trojans can be embedded in the application-specific IC (ASIC), commercial off the shelf (COTS) IC, microprocessors, digital signal processors, or as software changes in the firmware for FPGA. Given that changes are made at the lowest level of the system, the type of violation may varies. These impacts can be classified as a change in functionality, changes in specifications, information leakage or denial of service. Specific hardware Trojans can implement any of these violations.

Hardware Trojans that change the functionality of IC through the insertion of additional logic circuitry or by switch-off of a part of the existing logic directly threaten the integrity and safety of an information system. Changing data in memory, the impact on computing or communication channel are typical goals of the considered insertion. Modification of functionality can be of very diverse nature; the impacts of this class of

ности и проявляется в возникновении временных ошибок. В работе [5] приведены примеры схем с перемычками в виде резистора, следствием которого становятся ошибки типа "закоротки" при некоторых режимах работы, и внесением конденсатора, приводящего к увеличению времени задержки за счет увеличения емкостной нагрузки.

Следующий класс троянов охватывает аппаратные модификации, направленные на скрытную передачу конфиденциальных данных от информационной системы злоумышленнику. Такая передача осуществляется без непосредственного участия системы и без ведома пользователя системы. Механизмы передачи могут задействовать как существующие внутренние и внешние каналы системы, так и побочные каналы. Например, в работе [6] отмечается, что утечка информации может происходить по радиочастотному, оптическому и тепловому побочным каналам. Информацию можно извлечь, анализируя потребляемую мощность ИС, ее шумовые характеристики, а также любые другие функциональные и физические характеристики. Интерфейсы RS232 и JTAG также могут быть использованы в качестве каналов утечки. Например, в работе [8] рассмотрена аппаратная закладка, которая позволяет определять ключи шифрования в беспроводной передаче по изменению амплитуды или частоты, которые возникают из-за вариаций технологии изготовления ИС. В работе [9] с использованием метода передачи сигналов с расширенным спектром информация о ключе шифрования извлекалась из изменения уровня собственных шумов КМОП ИС.

Системная модификация на самом низком уровне предоставляет широкий спектр возможностей для реализации ошибки типа "отказ в обслуживании" (DoS), которые варьируются от частичного проявления ошибки до полного и окончательного отключения системы внедрением так называемого "убивающего ключа" (kill switch) [11]. В работе [6] к этому классу отнесены трояны, которые влияют на обслуживание клиентов вычислительной системы через использование ограниченных ресурсов, таких как вычислительная способность, рабочий диапазон, мощность источника питания. Отмечается, что вносящие ошибку физические эффекты, изменение конфигурации системы или ее отключение могут быть временными или постоянными. Аппаратные закладки этого класса могут потреблять избыточную или всю энергию источника питания (аккумулятора), не позволяя системе перейти в спящий режим [11], или путем введения избыточных буферов в межсоединения ИС [12] уменьшать время работы устройства между подзарядками. Аппаратный троян может быть разработан с целью влияния на управление сигналом разрешения записи в память, перезаписывая существующее значение случайной величиной. Это ведет к побочным сбоям в работе служб или частичному и даже полному отключение системы. Ошибки "отказ в обслуживании",

hardware Trojans are limited only by system resources, imagination and skill of the attacker. For example, in [7] the scenario is presented, in which a simple destructive hardware Trojans can insert an error into the algorithm based on the Chinese remainder theorem for public-key cryptosystem (RSA), which leads to the compromise of the RSA key. In [5] an example of a modification is given, in which the error detection module accepts input signals that should be rejected.

The immediate errors in the IC, as for example the Pentium FDIV (error in the FPU in the original Pentium processors discovered in 1994), can be reproduced by the hardware Trojan, and to prevent its detection the selective switching can be used. Special hardware Trojans can be designed for change in execution order of CPU instructions, data leakage via side channels, change of the contents of a programmable memory (PROM).

Change in the functionality of the system can be used to support wider attacks. So, in paper [6] it is noted that the possibility of damage to the security is substantially increased, when the hardware and software attacks are used together. As an example, the changes in the central processor that supports an attack on software are described. As a result, all memory access and modification of the programme contribute to the empowerment, with subsequent access to the system through the back door and attack with the stolen password.

Hardware Trojans, which modify the specification, distort the parametric properties of the target IC or specifications that are not related to its functionality. Such parametric properties include synchronization, timing and power consumption of IC. The effect is achieved by directly modifying the internal physical

вызванные аппаратными троянами, могут быть связаны с преждевременным выходом устройства из строя. Так в работе [6] приведена схема, которая генерирует локальную избыточную мощность, что приводит к ускорению процесса старения ИС, сокращая срок ее службы без нарушения функциональности. Там же делается вывод, что с целью увеличения электромиграции возможно изменение химических компонентов в металлизированной разводке, причем эффект от этого может быть аналогичен увеличению напряжения питания или частоты синхронизации, что ведет к снижению времени наработки на отказ ИС.

***

Несанкционированные злоумышленные модификации ИС могут стать большой проблемой для обеспечения кибербезопасности электронных систем во всем мире, в особенности систем, задействованных в военной сфере и системах безопасности. В настоящее время военные ведомства многих стран не скрывают беспокойства в связи с расширяющимся аутсорсингом в области разработки и производства интегральных электронных компонентов, и зависимости новейших разработок от электронных компонентов, находящихся в свободной продаже. Аппаратные трояны угрожают нарушением целостности данных и функций, выполняемых любой вычислительной системой, которая содержит интегральные электронные компоненты. Суть возможных угроз заключается в функциональных и технических модификациях характеристик ИС, утечке конфиденциальной информации, а также атаках типа "отказ в обслуживании". Для предотвращения таких угроз необходима разработка комплексных методов и стратегий борьбы с аппаратными троянами, их предупреждения и выявления, а также мер противодействия им, что будет рассмотрено в последующих статьях цикла публикаций.

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

ЛИТЕРАТУРА

1. **Abramovici M., Bradley P.** Integrated circuit security: new threats and solutions //Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies. ACM, 2009. С. 55.
2. **Becker G.T.** et al. Stealthy dopant-level hardware trojans //Cryptographic Hardware and Embedded Systems-CHES 2013. Springer Berlin Heidelberg, 2013. С. 197–214.
3. Embedded System Challenge https://esc.isis.poly.ed
4. http://www.darpa.mil/Our_Work/MTO/Programs/Trusted_Integrated_Circuits_(TRUST).aspx
5. **Rajendran J.** et al. Towards a comprehensive and systematic classification of hardware trojans // Circuits and Systems (ISCAS), Proceedings of

properties – interconnection topology and geometry of transistor structures. In contrast to hardware Trojans, which affect the functionality, this class is characterized by changes in the topology of the wirings and transistors, and their destructive actions can lead to system failures [6]. We can assume that in addition to the considered modifications it may be activated hardware Trojans, which ensures change of the specifications with trigger or activation mechanism. Different types of impacts on IC are typical for this class, including limitation of computational capabilities of the system by insertion in the circuit of the system frequency generator, the modification of the computational units or input/output cells when the functionality of these nodes not change, but throughput and dynamic characteristics worsen. A change of the location of gates or wiring in the circuit may be functionally equivalent, but with a higher parasitic components of passive elements that leads to the performance degradation at high load and manifests in the appearance of transient errors. Paper [5] contains the examples of circuits with jumpers in the form of a resistor, a consequence of which are errors (short-circuits) in some modes, and addition of the capacitor, resulting in an increase in delay time due to the increase in capacitive load.

The next class of Trojans covers hardware modifications for transmission of confidential data from the information system to the attacker. Such transmission is carried out without direct participation of the system and without the knowledge of its user. The transfer mechanism can use existing internal and external channels, and side channels. For example, in [6] it is noted that leakage of information may occur via RF, optical and thermal side channels. Information

2010 IEEE International Symposium on. IEEE, 2010. С. 1871–1874.
6. **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.
7. **Agrawal D.** et al. Trojan detection using IC fingerprinting //Security and Privacy, 2007. SP›07. IEEE Symposium on // IEEE, 2007. С. 296–310.
8. **Jin Y., Makris Y.** Hardware Trojans in wireless cryptographic integrated circuits // Design & Test, IEEE. Iss. 99. 2013. С. 1.
9. **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.
10. **Adee S.** The hunt for the kill switch // Spectrum, IEEE. 2008. Т. 45. № 5. С. 34–39.
11. **Wolff F.** et al. Towards Trojan-free trusted ICs: Problem analysis and detection scheme // Proceedings of the conference on Design, automation and test in Europe. ACM, 2008. С. 1362–1365.
12. **Karri R.** et al. Trustworthy hardware: Identifying and classifying hardware trojans // Computer. 2010. Т. 43. № 10. С. 39–46.

can be extracted by analyzing the power consumption of IC, its noise characteristics, as well as any other functional or physical characteristics. RS232 and JTAG interfaces can also be used as channels of leakage. For example, in [8] a hardware Trojan is described that allows to define the encryption keys in the wireless transmission with use of data about changing of the amplitude or frequency that occur due to variations of manufacturing technology. In [9], the information about the encryption key was retrieved from the change of the noise level of the CMOS IC using the signal transmission method with an expanded range.

System modification at the lowest level provides a wide range of opportunities for implementation of "denial of service" (DoS) errors, which range from the partial manifestation of the errors to the complete system shutdown by the insertion of so-called kill switch [11]. According to [6], this class includes Trojans that affect customer service in computer system through the use of limited resources such as computational capacity, operating range, power supply. It is noted that harmful physical effects, a change in system configuration or her shutdown may be temporary or permanent. Hardware Trojans of this class can consume excessive or the entire energy of the power supply (battery), not allowing the system to go into sleep mode [11], or by introducing excess buffers in the interconnects of IC [12] reduce the operating time of the device between charges. A hardware Trojan can be designed to distort the signal that enable writing to the memory by overwriting the existing value with a random value. This leads to collateral disruptions of services or partial, and even full system shutdown. DoS errors caused by hardware Trojans, can lead to premature failure of the device. Paper [6] describes a circuit that generates a local excess capacity, which leads to accelerating of aging of the IC, reduces its service life without breaking functionality. It is concluded in the same paper that to increase electromigration the change in the chemical components in the metallic wiring is possible, and the effect of this may be similar to increasing the voltage or frequency of synchronization that reduced the error-free running time of IC.

***

Unauthorized, malicious modification of the IC can become a big problem for the cyber security of electronic systems worldwide, in particular of systems for the military and security applications. Currently, the military departments of many countries do not hide the concern in connection with the expanding outsourcing in the field of development and production of integrated electronic components, and dependence of the latest developments from the COTS electronic components. Hardware Trojans threaten with violation of the integrity of the data and the functions performed by any computing system, which includes integral electronic components. The essence of possible challenges is in the functional and technical modifications of the characteristics of the IC, leakage of confidential information, as well as DoS attacks. To prevent such threats it is necessary to develop integrated methods and strategies against hardware Trojans, for their prevention and detection as well as responses to them that will be discussed in subsequent parts of this series of publications.

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.

ЯЧЕЙКА ОЗУ, УСТОЙЧИВАЯ К ВОЗДЕЙСТВИЮ ВНЕШНИХ ФАКТОРОВ

RAM CELL THAT IS RESISTANT TO EXTERNAL FACTORS

УДК 621.382, ВАК 05.27.01

Н.Малашевич / N.Malashevich@tcen.ru*
*N.Malashevich**

Показана возможность реализации блоков однопортовых и двухпортовых оперативных запоминающих устройств (ОЗУ) повышенной стойкости к внешним факторам для базовых кристаллов (БК) серий 5521 и 5529. Рассмотрена ячейка памяти ОЗУ. Приведены результаты моделирования и испытаний микросхем ОЗУ на основе БК серии 5521 и 5529.

The article shows the feasibility of single-port and dual-port blocks of random access memory (RAM) on gate arrays (GA) of 5521 and 5529 families, which has an increased resistance to external factors. RAM memory cell is considered. Results of modeling and testing the RAM chips on the GA of the 5521 and 5529 families are given.

Активное развитие космической отрасли требует создания качественно новой электронной компонентной базы (ЭКБ), удовлетворяющей требованиям повышенной стойкости к основным дестабилизирующим факторам космического пространства. К таким факторам относятся: ионизирующее излучение, широкий температурный диапазон от –60 до 125°С, воздействие тяжелых заряженных частиц.

При создании бортовой аппаратуры космических систем используется широкая номенклатура ЭКБ общего и специального назначения (более 700 типов). Одними из наиболее востребованных и наиболее уязвимых по отношению к факторам космического пространства компонентов являются ОЗУ. Радиационностойкие ОЗУ выполняются в виде заказных интегральных схем (ИС), сложно-функциональных (СФ) блоков в составе систем на кристалле (СнК) или на базе программируемых логических интегральных схем (ПЛИС). В современных СнК объем памяти может превышать 50% площади кристалла ИС [1–3]. В то же время специализированные микросхемы при малых тиражах выпуска оптимально реализовывать на основе базовых матричных или базовых кристаллов (БМК или БК). Наличие ОЗУ в составе БК позволяет существенно расширить область их применения, улучшить функциональные и эксплуатационные характеристики аппаратуры. Однако разрешенные для применения в космических аппаратах БК с интегрированными (встроенными) в них блоками ОЗУ пока не созданы. В настоящее время в России доступна лишь одна серия отечественных БК с возможностью создания модулей памяти – это БМК серии 1592 емкостью 10, 30, 60 и 100 тыс. вентилей. Максимальная емкость ОЗУ составляет 256×16 или 128×32 бит. Данная серия БМК устойчива к механическим и климатическим воздействиям, стойкость же к специальным факторам не указана.

Интеграция схем памяти в БМК рассматривалась с 1980-х годов в работах авторов [1–3]. Тогда технологический уровень не позволял создать БМК с достаточным объемом памяти. Среди современных отечественных работ по данной тематике следует отметить предложение С.Ф.Тюрина использовать в БМК ячейку памяти с учетверением транзисторов QSRAM [2]. Предполагается, что расчетверение отдельных транзисторов логических элементов обеспечит выигрыш в вероятности безотказной работы по сравнению с резервированием. В России БМК выпускают "Ангстрем", ДЦ "Союз", ФНПЦ "НИИИС им. Ю.Е.Седакова", "НЗПП с ОКБ" и НПК "Технологический центр". Однако на данный момент отсутствуют БМК космического назначения со встроенными в них блоками памяти.

Создание отечественного БК со встроенными блоками ОЗУ космического назначения позволит отказаться от ряда зарубежных ИС, расширить номенклатуру специализированных микросхем, улуч-

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

шить их динамические и функциональные характеристики.

Реализация модуля ОЗУ в составе БК обеспечит следующие преимущества:

- получение стойкости встроенного ОЗУ, сопоставимой со стойкостью БК;
- сокращение потребляемой мощности конечного устройства и увеличение системного быстродействия за счет уменьшения длины и количества межсоединений;
- уменьшение габаритов аппаратуры за счет снижения количества используемых микросхем и уменьшения размеров печатных плат [5].

В НПК "Технологический центр" разработаны серии БК 5521 и 5529 со следующими характеристиками: напряжение питания 3 В ±10% или 3,3 В ±10%, расчетное время задержки на вентиль 110 пс, тактовая частота D-триггера в счетном режиме 500 МГц [4, 5, 9]. Серия 5521 изготавливается по радиационно-стойкой КМОП-технологии с нормами 0,18 мкм на объемном кремнии. Серия 5529 изготавливается по радиационно-стойкой КМОП-технологии с нормами 0,25 мкм на структурах "кремний на изоляторе". Отличительной особенностью указанных серий является возможность реализации в них блоков однопортовых и двухпортовых ОЗУ.

Популярным решением в схемах ОЗУ является классическая 6-транзисторная ячейка с транзисторами связи n-типа (6Tn), увеличение площади которой в 1,2–1,5 раза позволяет существенно повысить стойкость ко всем радиационным факторам [6].

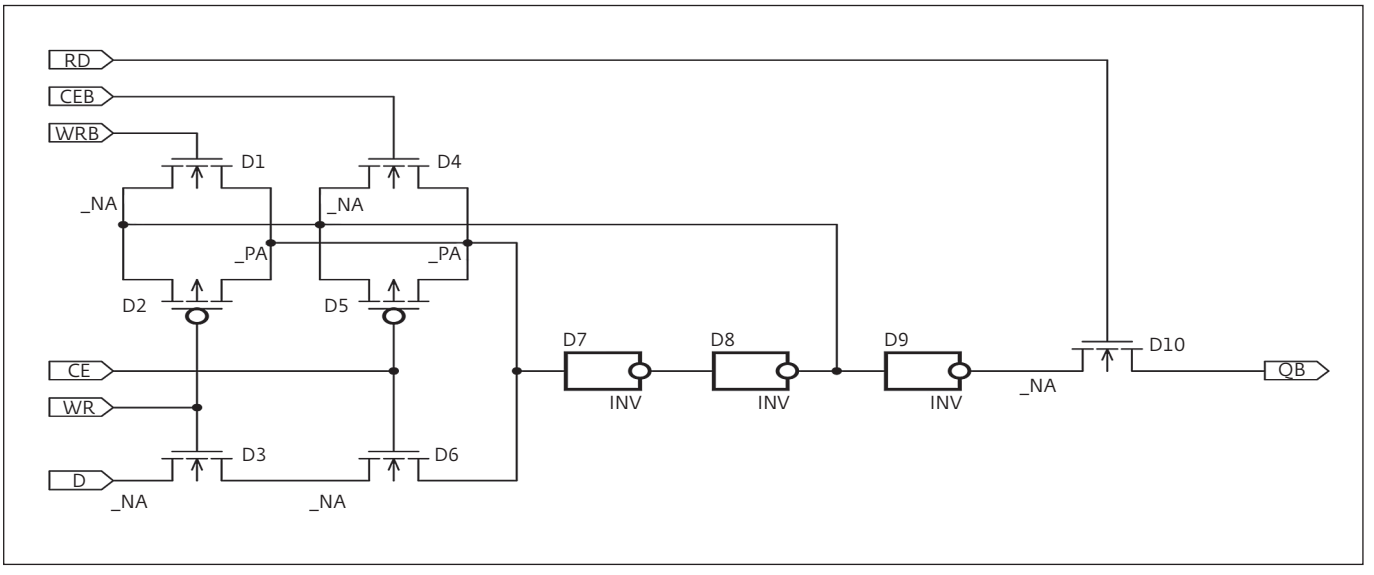
Повышение сбоеустойчивости 6-транзисторного элемента памяти может быть выполнено схемотехническими методами. Так Л.Рокетт, Д.Уайзман и Дж.Вембрукс предложили увеличивать постоянную времени в цепи обратной связи триггера. Между инверторами в составе ячейки памяти добавляли резисторы, конденсаторы, позже диоды и транзисторы [7]. Основными недостатками таких ячеек являются температурная чувствительность, уязвимость при низких температурах и необходимость дополнительной маски для формирования резистора.

Д.Бессо, Р.Велазко и другие исследователи использовали схемы обратной связи для восстановления исходных данных. Основные проблемы при этом – размещение дополнительных транзисторов обратной связи и появление новых чувствительных узлов [8]. Преимуществами этого метода являются температурный запас, запас по напряжению и хорошая устойчивость к одиночным сбоям, вызванным тяжелыми заряженными частицами.

Active development of space industry requires the creation of qualitatively new electronic component base (ECB), which would satisfy the requirements of increased resistance to the main destabilizing factors of outer space. These factors include ionizing radiation, wide temperature range from –60 to 125°C, the influence of heavy charged particles.

For creation onboard equipment of space systems the wide range of electronic components for general and special purposes (over 700 types) is used. One of the most demanded and the most vulnerable to the space factors components is RAM. Radiation resistant RAM is made in the form of custom integrated circuits (IC), hard IP cores in systems on chip (SOC) or on the basis of programmable logic devices (PLD). In up-to-date SOCs the memory size can exceed 50% of the area of the chip [1–3]. At the same time, it is optimum to create specialized ICs in case of small production volumes on the base of gate arrays (GA). The inclusion of the RAM into the GA can significantly expand the scope of their application, to improve the functional and operational characteristics of the equipment. However, GA with integrated (built-in) RAM blocks, which are allowed for use in space vehicles, has not yet been created. Currently only one series of the domestic GA with the ability to create memory modules is available in Russia, it is GA of 1592 family with a capacity of 10, 30, 60 and 100 thousand gates. Maximum RAM capacity is 256×16 or 12827×32 bits. This GA family is resistant to mechanical and climatic influences, but the resistance to special factors is not specified.

Integration of memory circuits in GA was investigated from 1980-ies in the studies of the authors of [1–3]. At that time the technological level didn't allow to create GA with sufficient memory size. Among modern Russian studies on this subject, it should be noted the proposal of S.F. Tyurin to use in the GA a memory cell with quadrupling of QSRAM transistors [2]. It is assumed that quadrupling of individual transistors of the logic elements will ensure a win in the survival probability compared to redundancy. In Russia, GA are manufactured by Angstrem, Design Center "Soyuz", Sedakov Research Institute of measurement systems, Novosibirsk Factory and Design Bureau of Semiconductor Devices and SMC "Technological Centre". However at the moment there are no GA for space industry the built-in memory blocks.



Однопортовая ячейка ОЗУ
Single-port RAM cell

Дж.Уитакер, М.Н.Лю и Дж.Канарис применили дублирование критических узлов (например, DICE-ячейки). Основные преимущества этого метода – запас по температуре и по напряжению, устойчивость к воздействию тяжелых заряженных частиц и высокая производительность. Надежную защиту от сбоя в случае однократной бомбардировки космическими частицами узла схемы обеспечивают временное разнесение тактовых сигналов и тройное модульное резервирование внутри ячейки памяти. В наиболее популярных DICE-ячейках памяти и ячейках с тройным резервированием изменение состояния возможно только при множественных попаданиях тяжелых заряженных частиц. Также им свойственны наличие состязательности сигналов в процессе записи / чтения, необходимость предзаряда шин и вероятность потери данных при чтении.

Сбоеустойчивость элемента памяти может быть повышена и конструктивно-топологическими методами, направленными на уменьшение вероятности появления тиристорного эффекта в КМОП-

The creation of the domestic GA with built-in RAM blocks for space applications will allow to refuse some foreign IC, to expand the range of specialized chips and to improve their dynamic and functional characteristics.

Integration of the RAM into the GA will provide the following benefits:

- resistance of built-in RAM will be comparable to the resistance of GA;
- reduction of power consumption of the target device and increase the system performance by reducing the length and number of interconnections;
- reduction of overall dimensions of equipment by lowering the number of chips used and reduction of the size of printed circuit boards [5].

SMC "Technological Centre" developed 5521 and 5529 families of GA with the following characteristics: power supply voltage is 3 V ±10% or 3.3 V ±10%; calculated delay time for the gate is 110 ps; clock frequency of D-type flip flop in the counting mode is 500 MHz [4, 5, 9]. 5521 family is manufactured using a radiation-resistant 0.18 μm CMOS technology on bulk silicon. 5529 family is manufactured using radiation-resistant 0.25 μm CMOS technology on silicon-on-insulator structures. A distinctive feature of these families is the possibility to obtain single-port and dual-port RAM blocks.

Common solution in RAM design is the classic 6-transistor cell with transistors of n-type (6Tn), increase the area of which by 1.2–1.5 times allows to increase the resistance to all the radiation factors [6].

Increasing failure tolerance of the 6-transistor memory element can be performed by means of schematic design. For example, Rockett L., Wiseman D. and Vembrux J. proposed to increase the time constant in the feedback circuit of the trigger. The resistors, capacitors, and later diodes and transistors were added between inverters in the memory

структурах и снижение влияния дозовых эффектов. Г.Анелли и У.Снойес в своих работах представляют методы снижения влияния накопленной дозы за счет использования транзисторов с кольцевым затвором. В работах Т.Аоки показана возможность подавления тиристорного эффекта благодаря использованию контактов к подложке и n-карману, а также охранных колец.

В основе ячейки ОЗУ (патент РФ на изобретение №2507611), применяемой в БК серий 5521 и 5529, лежит триггер, построенный на двух инверторах, со схемой подтверждения записанных данных (см. рисунок). В процессе записи информации в выбранную ячейку отсутствует состязательность между новыми и старыми данными, поскольку схема подтверждения разрывает обратную связь в триггере.

При записи в ОЗУ с применением ячеек памяти на основе 6-транзисторного ядра и DICE-ячеек на каждую записываемую ячейку приходится большое количество побочно считываемых, поскольку выбирается вся строка, за счет чего снижается сбоеустойчивость. В описываемой ячейке такая ситуация исключается, так как для записи данных используется двухкоординатная выборка по строке (сигнал WR/WRB) и столбцу (сигнал CE/CEB). Двухкоординатная выборка увеличивает размеры ячейки памяти на три транзистора, но существенно повышает ее сбоеустойчивость.

Запоминающий элемент предложенной ячейки памяти изолирован от влияния битовых линий благодаря использованию дополнительного выходного инвертора. Необходимость дополнительного порта при разделении разрядных шин на чтение и запись увеличивает площадь ячейки, однако позволяет полностью исключить влияние операции чтения на состояние запоминающего элемента ячейки. Ячейки ОЗУ интегрированы в САПР "Ковчег" и введены в состав унифицированной библиотеки.

На основе предложенной однопортовой ячейки были разработаны, изготовлены и исследованы микросхемы ОЗУ различной емкости. Например, блок ОЗУ емкостью 4 К × 8 бит, изготовленный по технологии КНИ 0,25 мкм, имеет следующие показатели стойкости:

- пороговые ЛПЭ ОРЭ отказов $L_{ТН.\ ТЭ(КО)}$ не менее 64 МэВ·см^2/мг;
- сечение ОРЭ отказов при ЛПЭ 64 МэВ·см^2/мг не более $4{,}8 \cdot 10^{-8}$ см^2;
- сечение насыщения ОРЭ отказов $\sigma_{SI.ТЭ(КО)}$ не более 0,7 см^2;
- пороговые ЛПЭ ОРЭ сбоев: $L_{ТН.ОС}$ не менее 64 МэВ·см^2/мг;
- сечение ОРЭ сбоев при ЛПЭ 64 МэВ·см^2/мг не более $2{,}3 \cdot 10^{-12}$ см^2/бит.

На основе двухпортовой ячейки ОЗУ на БК серий 5521 и 5529 разработаны микросхемы 5521ТР054А-577 и 5529ТР054А-677, представляющие собой отказоустойчивое синхронное/асинхронное двухпортовое ОЗУ емкостью 32 Кбит с организацией 4 К слов по 8 бит с функцией исправления ошибок данных по алгоритму Хэмминга. В случае отключения функции исправления ошибок данных емкость ОЗУ увеличивается до 64 Кбит с организацией 8 К слов по 8 бит. Микросхемы имеют флаги ошибок, счетчики ошибок

cell [7]. The main disadvantages of these cells are temperature sensitivity, vulnerability at low temperatures and the need for additional mask for forming the resistor.

Bessot D., Velazco R. and other researchers have used feedback circuits to restore the initial data. The main problems here are the placement of additional feedback transistors and the emergence of new sensitive nodes [8]. The advantages of this method are the temperature margin, the voltage margin and good resistance to single failures caused by heavy charged particles.

Whitaker J., Liu M.N. and Canaris J. have applied the duplication of critical units (e.g., DICE cells). The main advantages of this method are the temperature and voltage margins, resistance to influence of heavy charged particles and high performance. Reliable protection of the node from a failure due to the single cosmic particles bombardment is provided by time separation of clock signals and triple modular redundancy in the memory cell. In the most popular DICE memory cells and triple redundant cells the change of a state is possible only at multiple hits of heavy charged particles. Also they are characterized by the signal competitiveness during read/write, need of a precharge of buses and probability of data loss during reading.

Failure tolerance of the memory element can be enhanced using topological design to reduce the probability of latch-up in CMOS structures and the influence of dose effects. Anelli G. and Snoyes W. in their papers present methods to reduce the influence of accumulated dose through the use of annular-gate transistors. Studies by T.Aoki show a possibility of latch-up suppression through the use of contacts to the substrate and the n-pockets, as well as guard rings.

A base for the RAM cell (Russian patent for invention No. 2507611) used in 5521 and 5529 GA families is the trigger that is built on two inverters

Показатели стойкости к воздействию специальных факторов по ГОСТ РВ 20.39.414.2
Indicators of resistance to special factors according to GOST RV 20.39.414.2

Производитель, техпроцесс Manufacturer, process technology	Тип специального фактора по ГОСТ РВ 20.39.414.2 Type of special factor according to GOST RV 20.39.414.2							
	7.И$_1$	7.И$_6$	7.И$_7$	7.И$_8$	7.И$_{12}$	7.И$_{13}$	7.К$_1$	7.К$_4$
СФ-блок ОЗУ 4 К×8 для БК серии 5529 Hard IP core of RAM 4Kx8 for 5529 GA family	4 Ус	6 Ус	3,6×4Ус	2×2 Ус	1,5×2 Р	2×2 Р	0,9×2 К	0,9×1 К
1645РУ1У ПКК "Миландр", КМОП 0,35 мкм 1645РУ1У Milandr, CMOS 0.35 µm	1 Ус	2 Ус	2 Ус	–	–	–	330×1 К	0,2×1 К
1645РУ2Т ПКК "Миландр", КНИ 1 мкм 1645РУ2Т Milandr, SOI 1 µm	5 Ус	5 Ус	4 Ус	–	–	–	5×1 К	0,2×1 К
1657РУ1У НПЦ "ЭЛВИС", КМОП 0,25 мкм 1657РУ1У ELVEES, CMOS 0.25 µm	2×4 Ус	2×4 Ус	2×4 Ус	0,0014×4 Ус	–	–	–	–

и супервизоры питания для каждого порта. Для повышения сбоеустойчивости микросхем 5521ТР054А-577 и 5529ТР054А-677 в блоке управления применяются троированные триггеры со схемой мажорирования, время выборки с включенной функцией исправления ошибок данных не превышает 25 нс.

В таблице представлены показатели стойкости к воздействию специальных факторов по ГОСТ РВ 20.39.414.2 микросхем ОЗУ отечественного производства.

Таким образом, ячейка ОЗУ, разработанная в НПК "Технологический центр", и СФ-блоки на ее основе не уступают по устойчивости к воздействию специальных факторов микросхемам ОЗУ других отечественных производителей. Для повышения сбоеустойчивости блоков ОЗУ на БК серий 5521 и 5529 были применены схемотехнические, топологические и алгоритмические методы. Испытания образцов микросхем серии 5529 подтвердили высокий уровень стойкости ОЗУ к воздействию оди-

with data confirmation (Fig.). During data recording to the selected cell there is no competitiveness between new and old data, because the confirmation circuit breaks feedback in the trigger.

If for record in the RAM memory cells on the basis of a 6-transistor core and DICE cells are used, then there is a large number of side reads for each recorded cell, because the whole row is selected, and thereby failure tolerance decreases. In the described cell such situation is excluded, because for data recording two-coordinate selection of row (WR/WRB signal) and column (CE/CEB signal) is used. Two-coordinate selection increases the size of the memory cell by three transistors, but significantly increases its fault tolerance. The storage element of the proposed memory cell is isolated from the influence of bit lines by using an additional output inverter. The need for additional port to separate bit wires for read and write increases the area of the cell, but allows to completely eliminate the effect of read operations on the state of the storage element of the cell. RAM cells are integrated in Kovcheg CAD and included into the unified libraries.

Based on the proposed single-port cells the RAM chips of different capacities have been designed, manufactured and tested. For example, the RAM module with capacity of 4 K×8 bit, which is manufactured by 0.25 µm SOI technology, has the following resistance characteristics:

- threshold LET SEE for failures $L_{TH.\ ТЭ(КО)}$ is not less than 64 MeV·cm^2/mg;
- cross-section of SEE failures at LET of 64 MeV·cm^2/mg is not more than $4.8 \cdot 10^{-8}$ cm^2;
- saturation cross-section of SEE failures $\sigma_{SI.ТЭ(КО)}$ is not more than 0.7 cm^2;
- threshold LET SEE for errors $L_{TH.\ ОС}$ is not less than 64 MeV·cm^2/mg;

ночных тяжелых заряженных частиц: сбоев и отказов не обнаружено до уровня 64 МэВ·см²/мг. Использование отказосбоеустойчивых блоков ОЗУ в совокупности с применением троированных триггеров позволяет на БК серий 5521 и 5529 реализовать специализированные микросхемы сложностью более 1 млн. условных вентилей, устойчивых к факторам космического пространства [9].

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

ЛИТЕРАТУРА

1. **Miyahara N., Ishikawa K., Hamaguchi S., Horiguchi S., Aoki M.** A composite CMOS gate arrays with 4K RAM and 128K ROM // IEEE Journal of Solid – State Circuits. Vol. SC-21, No. 2. April 1986. P. 228 – 233.
2. **Takahashi T., Kawashima M., Fujita M., Kobayashi I., Arai K., Okabe T.** A 1.4M-Transistor CMOS Gate Array with 4ns RAM // IEEE International SolidState Circuits Conference Digest of Technical Papers. 1989. P. 178–179.
3. **Kuroda T., Fujita T., Nagamatu T.** et al. A High-speed Low-Power 0.3 μm CMOS Gate Array with Variable Threshold Voltage (VT) Scheme // IEEE 1996 Custom Integrated Circuits Conference. 1996. P. 53–56.
4. **Тюрин С.Ф.** Отказоустойчивая статическая оперативная память на основе ячеек БМК // Вестник пермского университета. Математика. Механика. Информатика. 2016. Вып. 1(132). С. 34–39.
5. **Гаврилов С.В., Денисов А.Н, Коняхин В.В., Малашевич Н.И., Федоров Р.А.** Семейство серии базовых матричных кристаллов // Известия ВУЗов. ЭЛЕКТРОНИКА. 2015. № 5(101). С. 497–504.
6. **Герасимов Ю.М., Григорьев Н.Г., Гусев В.В., Кобыляцкий А.В., Петричкович Я.Я.** Радиационно-стойкие КМОП СБИС ОЗУ по технологии объемного кремния // Проблемы разработки перспективных микро- и наноэлектронных систем (МЭС). 2014. № 3. С. 171–176.
7. **Быстрицкий А., Подъяпольский С., Телец В., Цыбин С.** ПЛИС для космических применений. Архитектурные и схемотехнические особенности // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2005. № 6. С. 44–48.
8. **Коняхин В.В., Денисов А.Н., Федоров Р.А., Вильсон А.Л., Бражников С.С., Коновалов В.С., Малашевич Н.И., Росляков А.С.** Микросхемы для аппаратуры космического назначения : Практическое пособие / Под общ. ред. А.Н. Саурова. – М.: ТЕХНОСФЕРА, 2016. 388 с.
9. **Malashevich N., Makarceva M., Fedorov R.** Radiation-Hardened Gate Array with Embedded SRAM // Radiation and Its Effects on Components and Systems (RADECS), 2015 15th European Conference on Year: 2015. P. 1–4, DOI: 10.1109/RADECS.2015.7365656. IEEE Conference Publications.

- cross-section of SEE errors at LET of 64 MeV·cm²/mg is not more than $2.3 \cdot 10^{-12}$ cm²/bit.

On the basis of dual-port RAM cell on 5521 and 5529 GA families the 5521TP054A-577 and 5529TP054A-677 chips are developed, which are a fault-tolerant synchronous / asynchronous dual port RAM with a capacity of 32 kbit (4 K words of 8 bits each) and error correction according using Hamming algorithm. If the error correction is disabled, the RAM capacity increases to 64 kbit (8 K words of 8 bits each). The chips have the error flags, error counters and power supply supervisors for each port. To improve the failure tolerance of 5521TP054A-577 and 5529TP054A-677 chips, the triggers with triple modular redundancy are used in the control unit, and the access time with enabled error correction does not exceed 25 ns.

The table presents indicators of resistance to special factors according to GOST RV 20.39.414.2 for RAM of domestic production.

Thus, the RAM cell, which is designed in SMC "Technological Centre", and hard IP cores based on it are not inferior in terms of special resistance to the RAM modules of other domestic producers. To improve the failure tolerance of the RAM blocks on 5521 and 5529 GA families the schematic design, topological and algorithmic methods have been applied. Tests of samples of 5529 chips confirmed the high level of resistance of RAM to the effects of single heavy charged particles, and failures were not discovered until level of 64 MeV·cm²/mg. Use of fault-tolerant RAM blocks in conjunction with the use of tripled triggers allows to create specialized chips on 5521 5529 GA families with complexity more than 1 million conventional gates, which are resistant to space conditions [9]. ■

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

МИКРОСХЕМА ЗАЩИТЫ ОТ ТИРИСТОРНОГО ЭФФЕКТА

MICROCHIP FOR THYRISTOR EFFECT PROTECTION

УДК 621.382, ВАК 05.27.01

В.Коняхин, Р.Фёдоров* / R.Fedorov@tcen.ru*
V.Konyahin, R.Fedorov**

Рассматривается проблема радиационной стойкости электронной компонентной базы, работающей в условиях воздействия внешних космических факторов. Описаны принцип действия, структура и схема включения микросхемы защиты от тиристорного эффекта, предназначенной для применения в аппаратуре космического назначения.

This paper describes the radiation hardness problem of electronic component database operating under the external space environment exposure. It describes the operation principles, structure and connection layout of the latch-up protection circuit designed for space-related equipment.

При создании оборудования космического назначения остро стоит вопрос снижения рисков отказа аппаратуры из-за воздействия внешних космических факторов. Высокая стоимость устройств предъявляет особые требования к их надежности. На первый план вышла задача по увеличению сроков эксплуатации космических аппаратов с нынешних 3–5 до 10–12 лет при размещении радиоэлектронной аппаратуры не в герметконтейнере, а на открытой платформе [1]. В условиях радиационного облучения наиболее опасное воздействие на микросхемы оказывает эффект тиристорной защелки, который обусловлен возникновением паразитных биполярных транзисторов на основе КМОП-структур, образующих паразитный тиристор. Определенные внешние факторы, в частности воздействие тяжелых заряженных частиц, могут приводить к отпиранию и фиксации этого тиристора в открытом состоянии, что вызывает быстрое нарастание тока потребления с последующим тепловым разрушением микросхемы [2–4].

На основе унифицированной библиотеки ячеек базовых кристаллов серий 5521 и 5529 в НПК "Технологический центр" разработана микросхема защиты от возникновения тиристорного эффекта в КМОП-структурах. Микросхема выполнена в двух модификациях: 1469ТК025, изготовленная по КМОП-технологии "кремний на изоляторе" с топологическими нормами 0,25 мкм, и 1469ТК035, изготовленная по радиационностойкой КМОП-технологии объемного кремния с топологическими нормами 0,18 мкм. Ток потребления составляет не более 1 мА при напряжении питания 3,3 В ±10%. Каждая микросхема содержит внутренний силовой ключ с максимальным рабочим током до 500 мА для 1469ТК025 и 1000 мА для 1469ТК035. Температурный диапазон работы: от –60 до +85°С. Обе микросхемы разрешены для применения в аппаратуре специального назначения [5, 6].

Принцип действия основан на контроле тока потребления защищаемых элементов. Микросхема в автоматическом режиме отслеживает превышение заданного порога напряжения на внешнем резистивном шунте, встроенном в цепь питания защищаемых микросхем. При превышении током потребления порога срабатывания включается режим ограничения тока в нагрузку. Если произошло уменьшение тока нагрузки и восстановление штатного режима, то ограничение снимается и восстанавливается питание защищаемых элементов. В противном случае микросхема полностью отключает питание защищаемых микросхем и через заданный интервал времени снова восстанавливает его.

Дополнительно в микросхеме реализован блок сторожевого таймера, который предотвращает

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

зависание системы. При разрешенной работе сторожевого таймера микросхема отслеживает наличие импульсов на его входе. В случае отсутствия импульсов в течение заданного времени микросхема выключает питание защищаемых микросхем. Временные параметры работы сторожевого таймера задаются внешними элементами.

Для индикации срабатывания защиты от тиристорного защелкивания и перехода сторожевого таймера в режим ожидания предусмотрены дополнительные выводы. Установка задержек срабатывания защиты по току и сторожевого таймера осуществляется путем выбора значений емкостей внешних конденсаторов, которые определяют частоту соответствующих генераторов, реализованных в микросхеме.

Рекомендуемая схема включения микросхемы представлена на рис.1, где: Rизм – низкоомный резистор, предназначенный для отслеживания уровня потребляемого нагрузкой тока; Rн, Cн – эквивалентная нагрузка; C1 – керамический или полярный электролитический конденсатор, заряд которого обеспечивает нормальное функционирование микросхемы во время нарушения работы основного источника питания VDD; C2 – керамический конденсатор, емкость которого определяет частоту тактового генератора, синхронизирующего работу схемы управления защитой от тиристорного защелкивания; C3 – керамический конденсатор, емкость которого определяет частоту тактового генератора сторожевого таймера; C4 – конденсатор емкостью 2 нФ, предназначенный для

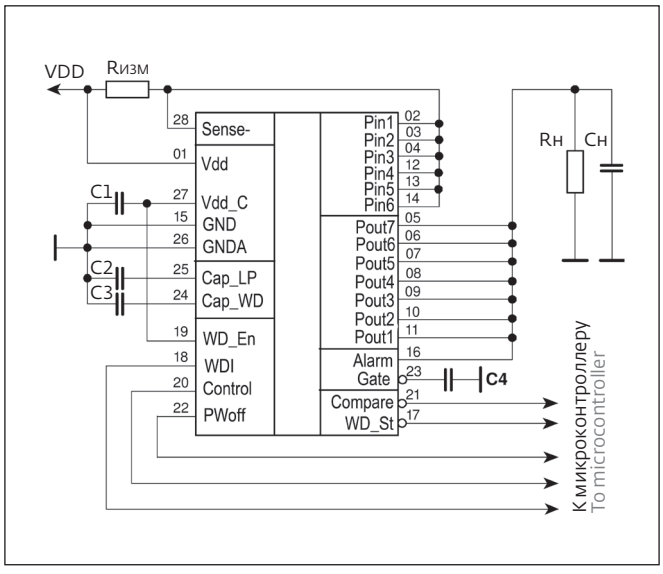


Рис.1. Рекомендуемая схема включения микросхемы
Fig.1. Recommended wiring of the chip

подавления высокочастотных помех на затворе внутреннего силового ключа.

Ток срабатывания защиты $I_{СРАБ}$ определяется номиналом внешнего токосъемного резистора $R_{ИЗМ}$ и рассчитывается по формуле:

$$I_{СРАБ} = \frac{0,1}{R_{ИЗМ}}.$$

Предусмотрена возможность внешнего управления микросхемой с помощью выводов PWoff, Control и WD_En.

For creation of equipment for space applications an important issue is the reduction of risk of hardware failure due to exposure to external cosmic factors. The high cost and complexity of devices caused specific requirements to their reliability. The task of increasing the service life of the spacecraft from the current 3–5 to 10–12 years when placing electronic equipment not in a hermetic container and on an open platform [1] is of particular importance. In conditions of radiation, the most adverse effects on the chip has the thyristor latch-up, which is caused by the occurrence of parasitic bipolar transistors based on CMOS structures forming a parasitic thyristor. Certain external factors, particularly the influence of heavy charged particles, can lead to the opening and locking of this thyristor in an open state, which causes a rapid increase in current consumption with subsequent thermal destruction of the chip [2–4].

SMC "Technological Centre" have developed a microchip for thyristor effect protection in CMOS structures, which is based on the unified library of gate array cells of 5521 and 5529 families. The microchip is made in two versions: 1469TK025 made in 0.25 μm CMOS silicon on insulator technology and 1469TK035 made in radiation-resistant 0.18 μm CMOS bulk silicon technology. The current consumption is not more than 1 mA at a supply voltage of 3.3 V ±10%. Each microchip includes an internal power switch with maximum operating current up to 500 mA for 1469TK025 and 1000 mA for 1469TK035. Operating temperature range is from –60 to 85 °C. Both microchips are approved for use in special-purpose hardware [5, 6].

The principle of operation is based on monitoring the current consumption of the protected elements. The microchip automatically

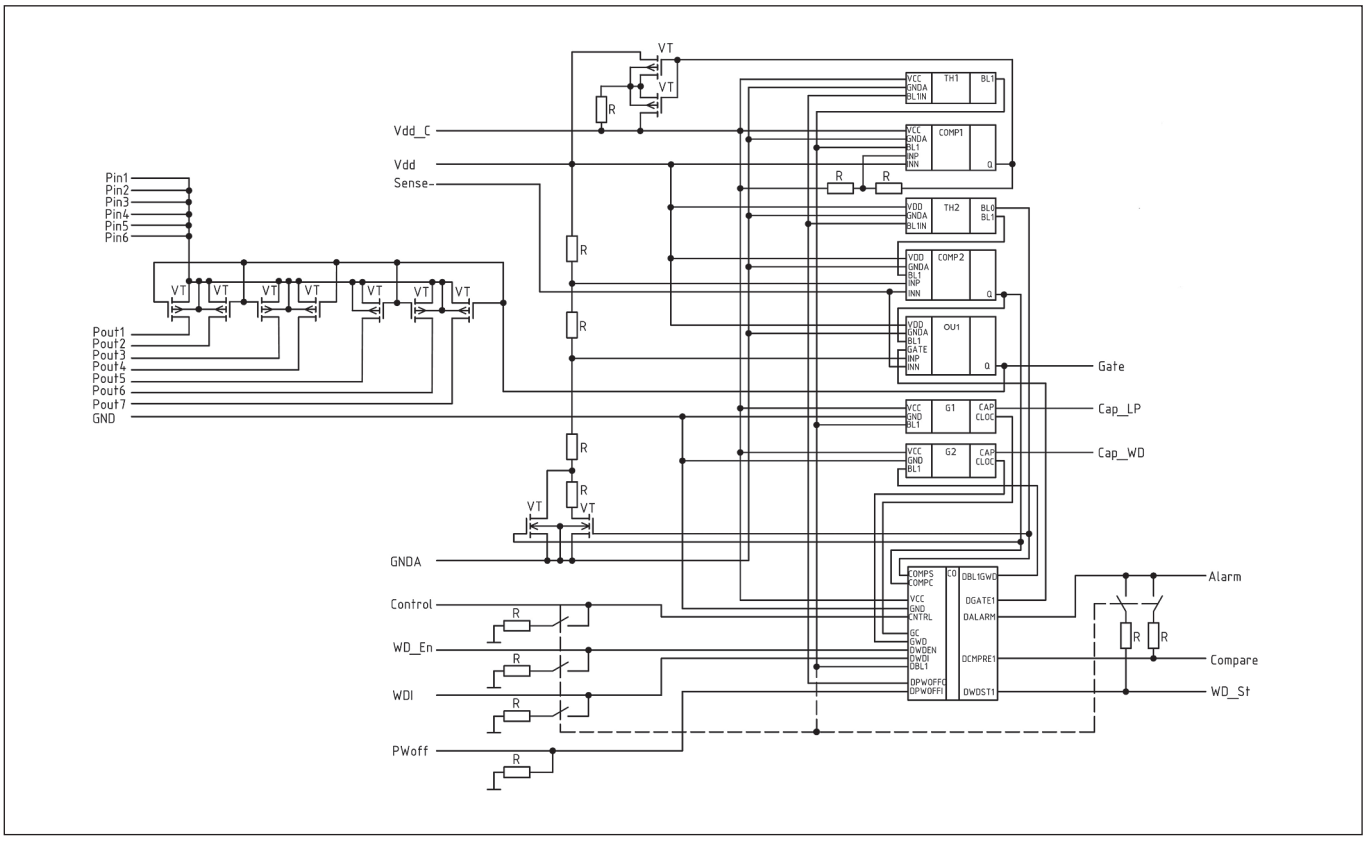


Рис.2. Функциональная блок-схема микросхемы
Fig.2. Functional block diagram of chip

Микросхема имеет два информационных выхода, позволяющих внешним системам управления фиксировать наличие события срабатывания защиты от тиристорного защелкивания (выход Compare) и окончание времени ожидания сторожевого таймера (выход WD_St).

Функциональная блок-схема микросхемы приведена на рис.2. В состав микросхемы входят

monitors the exceeding of specified threshold of the voltage on external shunt resistor built into the supply circuit of the protected chips. If the current consumption exceeds the threshold, then the current limiting to the load activates. If there was a decrease in the load current and restoration of normal operations, then the constraint is removed and power is restored to the protected components. Otherwise, the microchip completely turns off the power to the protected circuits and after a preset time interval again restores it.

Additionally, the watchdog timer is implemented in the microchip, which prevents system hang. When watchdog timer is enabled, the microchip monitors the pulses at its input. In case of absence of pulses within a predetermined time, the chip turns off the power supply of the protected circuits. Operating parameters of the watchdog timer are set by external components.

For indication of thyristor latch-up protection and standby mode of watchdog timer the additional outputs are provided. Setting the operational delay of overcurrent protection and watchdog timer is accomplished by selecting the values of the capacitances of external capacitors that determine the frequency of appropriate generators implemented in the chip.

Recommended wiring of the microchip is shown in Fig.1, where: Rизм is low ohmic resistor for monitoring current consumption; Rн, Cн are equivalent load; C1 is ceramic or polar electrolytic capacitor, a charge of which ensures the normal functioning of the chip during disruption of the main power supply VDD; C2 is ceramic capacitor, the capacity of which determines the frequency of the clock generator that synchronizes the control circuit of thyristor latch-up protection; C3 is ceramic capacitor whose capacitance determines the

следующие основные узлы: COMP1 – компаратор питания, отслеживающий превышение напряжения на выводе Vdd_C относительно напряжения на выводе Vdd; TH2 – супервизор питания на выводе Vdd; TH1 – супервизор питания на шине Vdd_C; COMP2 – компаратор; OU1 – усилитель; G1 – генератор тактовой частоты схемы управления, частота которого задается встроенным в микросхему резистором и внешним конденсатором, подключаемым к выводу Cap_LP; G2 – генератор тактовой частоты схемы сторожевого таймера, частота которого задается встроенным в микросхему резистором и внешним конденсатором, подключаемым к выводу Cap_WD; CO – цифровая часть микросхемы.

Порог срабатывания, отпускания и режим ограничения по току схемы защиты можно проверить при остановленных генераторах G1 и G2 путем замыкания выводов Cap_LP и Cap_WD на "Общий 0 В". Работу компаратора COMP2 при этом можно наблюдать на выводе Compare, а работу усилителя OU1 – на выводе Gate. Временные диаграммы функционирования компаратора COMP2 и дифференциального усилителя OU1 при имитации тиристорного эффекта и при остановленных генераторах G1 и G2 показаны на рис.3. При работающих генераторах диаграмма будет отличаться от изображенной на рисунке. Имитация тиристорного эффекта для наглядности представлена в виде медленно изменяющегося сопротивления нагрузки.

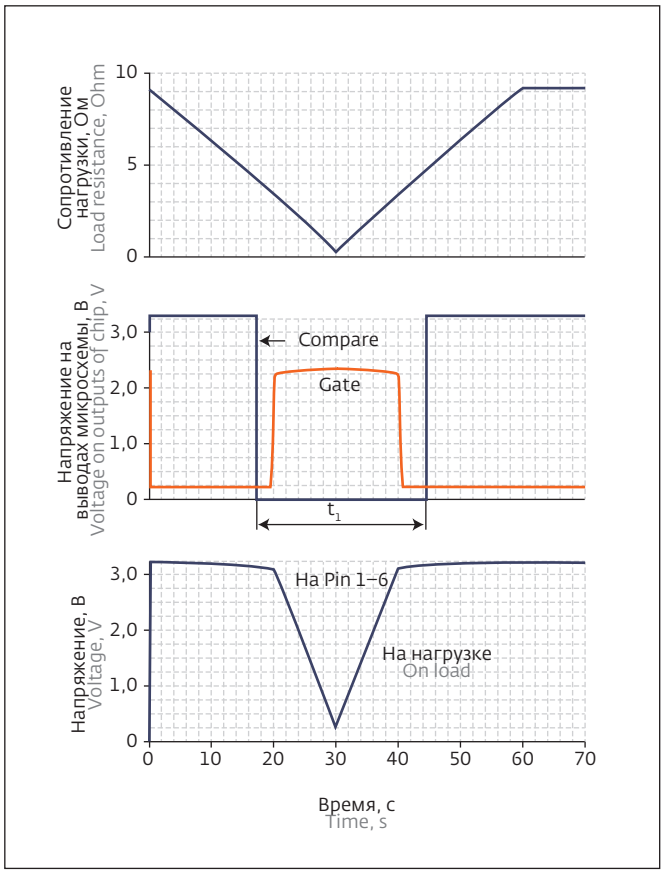


Рис.3. Работа компаратора COMP2 и дифференциального усилителя OU1 при имитации тиристорного эффекта и остановленных генераторах G1 и G2

Fig.3. Operation of comparator COMP2 and differential amplifier OU1 in case of simulation of thyristor effect and stopped generators G1 and G2

frequency of the clock generator of watchdog timer; C4 is capacitor with a capacitance of 2 nF, designed to suppress high frequency noise on the gate of the internal power key.

The protection operating current $I_{СРАБ}$ depends on the value of the external collector resistor $R_{ИЗМ}$ and is is calculated by the formula:

$$I_{СРАБ} = \frac{0,1}{R_{ИЗМ}}.$$

The possibility of external control using the outputs PWoff, Control, and WD_En is provided.

The microchip has two data outputs that allowing external control systems to register the actuation of thyristor latch-up protection (Compare output) and the end of the timeout of watchdog timer (WD_St output).

Functional block diagram of the microchip is shown in Fig.2. The microchip includes the following main components: COMP1 – the comparator of the power supply that monitors voltage at Vdd_C output relative to the voltage at Vdd output; TH2 – the voltage supervisor at Vdd output; TH1 – the voltage supervisor at Vdd_C bus; COMP2 – the comparator; OU1 – the amplifier; G1 – the clock generator of control circuit, which frequency is set by built-in resistor and external capacitor connected to Cap_LP output; G2 – the clock generator of watchdog timer, the frequency of which is set by built-in resistor and external capacitor connected to Cap_WD output; CO – the digital part of the chip.

Thresholds for actuation, release and restriction mode of overcurrent protection can be checked when generators G1 and G2 are turned off by closing Cap_LP and Cap_WD outputs to "Total 0". In this case, the operation of the COMP2 comparator can be observed on the Compare output and the operation of the OU1 amplifier – on Gate output. Timing diagram

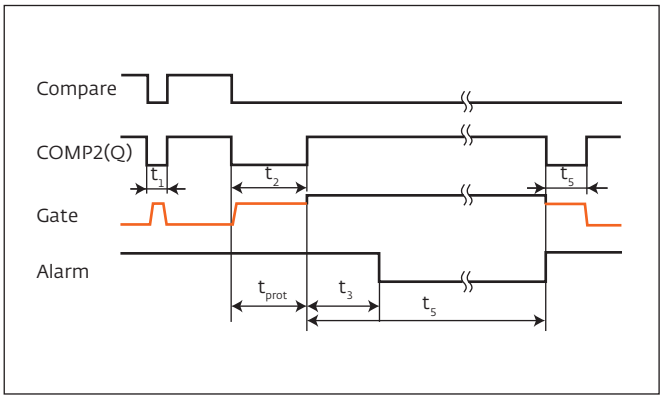


Рис.4. Пример временной диаграммы работы микросхемы при защите от тиристорного защелкивания
Fig.4. Example of timing diagram of chip with latch-up protection

Пороговое значение тока нагрузки, при котором срабатывает защита от тиристорного эффекта, задается сопротивлением шунта в цепи питания, включенного между входами Vdd и Sense-. При превышении порогового значения компаратор COMP2 выдает на вход схемы управления защитой по току сигнал к началу ограничения тока нагрузки, а на выводе Compare появляется низкий логический уровень. Вывод Compare можно использовать для проверки правильности выбора порога срабатывания по току.

Порог начала ограничения тока нагрузки несколько выше порога компаратора COMP2, поэтому рост уровня сигнала на выходе Gate начинается после появления активного низкого логического уровня на выводе Compare. Если длительность сигнала Compare не превышает время tprot (на рис.3 t1 < tprot), то при снижении тока до порога отпускания сигналы Compare и Gate возвращаются в исходное состояние, и питание микросхемы восстанавливается.

На рис.4 показан пример полной временной диаграммы работы микросхемы при защите от тиристорного защелкивания. Если длительность сигнала COMP2(Q) от компаратора COMP2 превышает время tprot, (на рис.4 t2 > tprot), то схема управления защитой по току выдает на дифференциальный усилитель OU1 сигнал блокировки, который переводит вывод Gate в высокий логический уровень, то есть вместо ограничения тока нагрузки происходит полное отключение питания нагрузки. Сигнал на выводе Compare при этом остается в состоянии низкого логического уровня до тех пор, пока не поступят внешние сигналы Control, PWoff или не произойдет восстановление питания. Через время, равное tprot (на рис.4 t3 = tprot), схема управления устанавливает низкий логический уровень на внешнем выводе Alarm. Использование вывода Alarm для включения дополнительного уровня защиты будет рассмотрено ниже.

По истечении времени trec (на рис.4 t4 = 32 tprot = trec) с момента отключения питания нагрузки схема управления восстанавливает высокий логический уровень сигнала Alarm и низкий уровень Gate, и дифференциаль-

of the operation of the comparator COMP2 and the differential amplifier OU1 when simulating latch-up and with turned off generators G1 and G2 is shown in Fig.3. When generators operate, the chart will differ from the one pictured. The simulation of latch-up, for clarity, is presented in the form of slowly changing load resistance.

The threshold value of the load current at which the latch-up protection is activated, is set by the shunt resistor in the power supply circuit connected between the Vdd and Sense- inputs. When the threshold value is exceeded, the comparator COMP2 outputs to the input of the overcurrent protection control circuit the signal to the beginning of the current limitation and low logic level appears at the Compare output. Compare output can be used to check the correctness of the choice of threshold current.

The threshold of the beginning of load current limitation is slightly above the threshold of the comparator COMP2, so the increase in the level of the signal at the Gate output begins after the appearance of an active low logic level on Compare output. If the duration of the Compare signal does not exceed the time tprot (Fig.3: t1 < tprot), then when the current is reduced to the threshold of release, the Compare and Gate signals are returned to its initial state, and the power supply of the chip is restored.

Fig.4 shows an example of a complete timing diagram of the microchip with the latch-up protection. If the duration of the COMP2(Q) signal of the comparator COMP2 exceeds the time tprot (Fig.4: t2 > tprot), then the overcurrent protection control circuit generates blocking signal on differential amplifier OU1, which changes the Gate output to a logic high level, that is, instead of the current limitation a full power-off of the load is

ный усилитель переходит в нормальный режим работы с возможностью ограничения тока нагрузки. Полное восстановление нормального питания нагрузки произойдет при условии спада тока нагрузки ниже порогового уровня (на рис.4 в течение времени t5). На этом цикл защиты от тиристорного защелкивания заканчивается.

При включении питания нагрузки из-за зарядки конденсаторов фильтра питания возможен бросок тока потребления, превышающий порог срабатывания схемы защиты от тиристорного эффекта. Чтобы избежать ошибочного отключения питания, следует выбирать tprot большим, чем длительность пика тока потребления (на рис.4 t5 < tprot).

На рис.5 показан пример временной диаграммы работы сторожевого таймера микросхемы.

При низком логическом уровне на внешнем входе WD_En разрешается работа сторожевого таймера. Блокировка сторожевого таймера осуществляется высоким логическим уровнем WD_En или срабатыванием защиты от тиристорного защелкивания. Если период сигнала WDI не превышает twdt, происходит сброс внутреннего счетчика сторожевого таймера и питание от нагрузки не отключается (на рис.5 t6 < twdt). Если за время twdt период сигнала WDI не завершается, то сторожевой таймер срабатывает и выполняет цикл отключения нагрузки (на рис.5 t7 = twdt). Минимальная

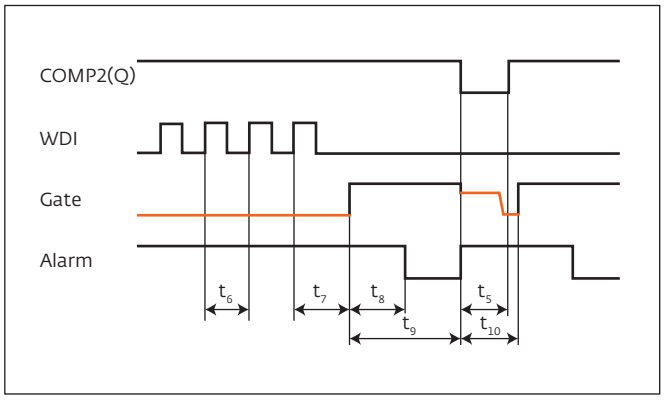


Рис.5. Пример временной диаграммы функционирования сторожевого таймера

Fig.5. Example of timing diagram of operation of watchdog timer

длительность высокого или низкого уровня сигнала на входе WDI должна быть не менее одного периода заданной частоты генератора сторожевого таймера.

При срабатывании сторожевого таймера устанавливается низкий уровень сигнала WD_St. Высокий уровень на выходе WD_St может быть восстановлен подачей высокого логического уровня на вход Control, или на вход PWoff, или сбросом по питанию. По истечении времени twdt с момента срабатывания сторожевого таймера формируется низкий логический уровень на выводе Alarm (на рис.5 t8 = twdt). Длительность отключения питания нагрузки с момента срабатывания сторожевого таймера

executed. In this case, the signal at the Compare output remains at the logic low level prior to the receipt of external Control, PWoff signals, or restoration of load power supply. After a time tprot (Fig.4: t3 = tprot), the control circuit sets the low logic level on the Alarm external output. Using of the Alarm output to activate additional level of protection will be discussed below.

After a time trec (Fig.4 t4 = 32tprot = trec) from the moment of the power-off, the control scheme restores the high logic level of Alarm signal and the low level of Gate, and the differential amplifier goes into normal operation mode with the option of limiting the load current. Full restoration of normal power supply to the load will occur under the condition of the decrease in load current below a threshold level (in Fig.4 during the time t5). At that point, the latch-up protection cycle comes to an end.

At the time of powering on, due to charging of capacitors of the power supply filter, the current inrush is possible, which can exceed the threshold of latch-up protection. To avoid incorrect power-off, it is necessary to set tprot larger than the duration of the current consumption peak (Fig.4: t5 < tprot).

Fig.5 illustrates an example of timing diagram of operation of watchdog timer.

In case of low logic level on WD_En external input, the operation of watchdog timer is permitted. The watchdog timer is locked when WD_En has a high logic level, or if latch-up protection is activated. If the period of WDI signal does not exceed twdt, the internal counter of the watchdog timer resets, and load power supply is not switched off (Fig.5: t6 < twdt). If during the time twdt the WDI signal doesn't complete, then the watchdog timer is activated and performs a cycle of the load

равна 2twdt (на рис.5 t9 = 2twdt). После этого сигнал Alarm возвращается в состояние высокого логического уровня, питание нагрузки восстанавливается, и дополнительная защита отключается.

При включении нагрузки после цикла срабатывания сторожевого таймера из-за зарядки конденсаторов фильтра питания возможен бросок тока потребления, превышающий порог срабатывания защиты. Чтобы этот процесс не вызвал ложного срабатывания защиты от тиристорного защелкивания, tprot должно превышать длительность пика тока потребления (на рис.5 t5 < tprot). Если на вход WDI по-прежнему не поступает периодический сигнал сброса, то цикл отключения по срабатыванию сторожевого таймера повторится через twdt (на рис.5 t10 = twdt). Появление низкого уровня на внешнем входе WD_En приводит к сбросу и выключению сторожевого таймера (то есть производит немедленное восстановление питания нагрузки), но не влияет на сигнал WD_St, высокий уровень которого может быть восстановлен подачей высокого логического уровня на вход Control, или на вход PWoff, или сбросом по питанию.

Высокий уровень на входе PWoff позволяет отключить питание нагрузки в любой момент и на произвольное время, возвращает в исходное состояние все узлы микросхемы и устанавливает все выводы в третье логическое состояние "отключено". Высокий уровень вывода Gate приводит к отключению питания нагрузки. Нормальное функционирование восстанавливается только по низкому уровню на входе PWoff. Следует обратить внимание на необходимость подключения выводов Control, WD_En и WDI к конкретному логическому уровню, так как при активном высоком уровне сигнала PWoff происходит отключение дотяжек этих входов к земле, способное вызвать повышение потребляемого микросхемой тока.

При срабатывании схемы защиты возможно сохранение остаточного питающего напряжения на нагрузке, что может привести к сбоям защищаемых микросхем после восстановления питания. В момент срабатывания дополнительного уровня защиты вывод Alarm отпирает внутренний ключ на основе n-канального МОП-транзистора и обеспечивает полную разрядку цепи питания защищаемых микросхем.

Для индикации состояния микросхемы используются два выхода: Compare и WD_St. Они позволяют определить, имел ли место факт срабатывания защиты по току или по истечении времени ожидания сторожевого таймера. Восстановить первоначальное состояние этих сигналов можно только с помощью входа Control. Для возвращения сигналов Compare и WD_St в исходное состояние необходимо подать на вход Control управляющий сигнал высокого уровня длительностью не менее tprot. Сигналы сброса длительностью менее tprot игнорируются.

shutdown (Fig.5: t7 = twdt). The minimum duration of a high or low signal level on the WDI input must be at least one period of the specified frequency of the generator of watchdog timer.

When the watchdog timer is activated the low level of WD_St signal is set. High level on WD_St output can be restored by applying a high logic level to the Control or PWoff inputs, or by power reset. After the time twdt since the watchdog timer activation a low logic level is formed on Alarm output (Fig.5: t8 = twdt). The length of the load power supply outage after the watchdog timer activation is equal to 2twdt (Fig.5: t9 = 2twdt). After that, the Alarm signal returns to high logic level, the load power supply is restored, and additional protection is disabled. When the load is turned on after an operation cycle of watchdog timer, due to charging of capacitors of the power supply filter, the current inrush is possible, which can exceed the protection threshold. To avoid incorrect activation of latch-up protection, tprot must exceed the duration of the current consumption peak (Fig.5: t5<tprot). If there is no periodic reset signal on WDI input, then the shutdown cycle will be repeated by watchdog timer after twdt (Fig.5: t10 = twdt).

The appearance of low level on the WD_En external input leads to reset or disable of the watchdog timer (with immediate restoration of load power supply), but does not affect the signal WD_St, high level of which can be restored by applying a high logic level to the Control or PWoff inputs, or by power reset.

High level on PWoff input allows to power off load at any time, returns all nodes of a chip to the initial state and sets all outputs to the third logic state "disabled". High level on Gate output shuts off load power supply. Normal operation is restored only at a low level at the PWoff input. It is necessary to

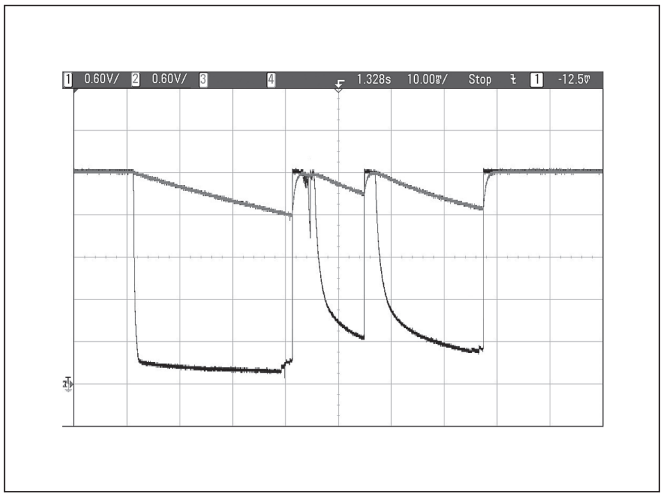


Рис.6. Пример осциллограммы напряжений на выводах Vdd и Vdd_C при нарушениях питания (черный – Vdd, серый – Vdd_C, C1 = 10 мкФ, сторожевой таймер отключен)

Fig.6. Example of oscillogram of voltages on outputs Vdd and Vdd_C in case of power disturbances (black – Vdd, gray – Vdd_C, C1 = 10 μF, watchdog timer disabled)

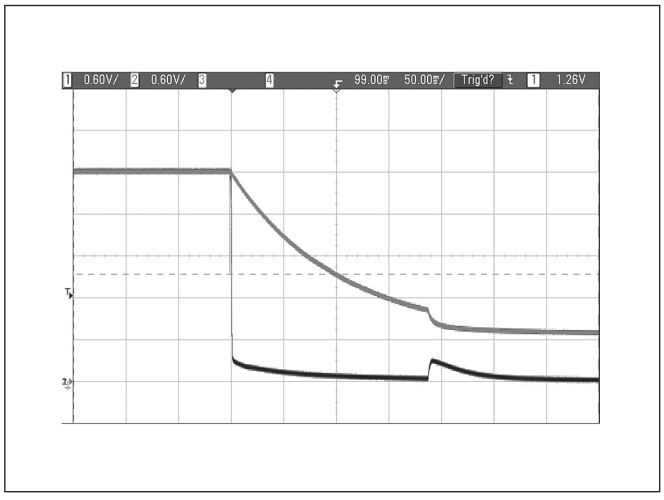


Рис.7. Пример осциллограммы напряжений на выводах Vdd и Vdd_C при аварии питания (черный – Vdd, серый – Vdd_C, C1 = 10 мкФ, сторожевой таймер отключен)

Fig.7. Example of oscillogram of voltages on outputs Vdd and Vdd_C in case of power failure (black – Vdd, gray – Vdd_C, C1 = 10 μF, watchdog timer disabled)

Поскольку существует вероятность кратковременного нарушения питания под воздействием радиационных факторов, предусмотрена возможность резервного питания микросхемы от дополнительного внешнего конденсатора, подключаемого к выводу Vdd_C. Основной источник питания подсоединяется к выводу Vdd. При нормальном функционировании основного источника питания потребляемый ток протекает между выводами Vdd_C и Vdd через внутренние ключи, реализованные на p-канальных МОП-транзисторах. Управление этими ключами осуществляется компаратором COMP1. В случае сбоя основного источника питания происходит снижение напряжения на выводе Vdd, и компаратор COMP1 размыкает ключи. Питание микросхемы в таком случае будет некоторое время поддерживаться за счет внешнего конденсатора C1. Выбор

pay attention to the connection of Control, WD_En and WDI outputs to a specific logic level, as in case of active high level of PWoff signal these inputs disconnect from the ground that can cause increased current consumption of the IC.

When protection circuit is activated, the residual voltage on the load can lead to failure of the protected circuits after power supply restoration. When additional protection is activated, the Alarm output unlocks the internal key based on n-channel MOS transistor and ensures full discharge of the power supply circuit of the protected chips.

For indication of circuits status the Compare and WD_St outputs are used. They allow to determine whether the overcurrent protection or watchdog timer were activated. It is possible to restore an initial state of these signals only by means of Control input. For the return of Compare and WD_St signals in its initial state, it is necessary to apply to the Control input the control signal of high level with duration not less than tprot. The reset signals with duration less than tprot are ignored.

Because there is a likelihood of short-term disturbances of the power supply under the influence of radiation factors, it is provided the possibility of power backup of the IC using an additional external capacitor that is connected to the Vdd_C output. The main power supply is connected to Vdd output. During normal operation of primary power supply the current flows between Vdd_C and Vdd outputs through the internal keys that are implemented on base of p-channel MOS transistors. The comparator COMP1 controls these keys. In the case of a failure of the primary power source the voltage on Vdd output decreases, and a comparator COMP1 opens the keys. In this case, the power supply of the chip will be supported

Характеристики специальных факторов по группам исполнения
Characteristics of special factors for groups of design

Виды специальных факторов Types of special factors	Характеристики специальных факторов Characteristics of special factors	Значения характеристик специальных факторов Values of characteristics of special factors	
		1469ТК025	1469ТК035
	$7.И_1$	$5У_С$	$4У_с$
	$7.И_6$	$6У_С$	$6У_с$
7.И	$7.И_7$	$0,5\times5У_С$	$5\times4У_с$
	$7.И_8$	$1У_С$	$0,013\times1У_С$
	$7.И_{12}$–$7.И_{13}$	$2\times2Р$	$2Р$
7.С	$7.С_1$	$5У_С$	$4У_с$
	$7.С_4$	$5У_С$	$3\times4У_с$
	$7.К_1$	$2К^{1,2}$	$2К$
7.К	$7.К_4$	$1К^{1,2}$	$1К^{1,2}$
	$7.К_{11}$	80 МэВ·см²/мг³	41 МэВ·см²/мг

[1] При совместном воздействии факторов с характеристиками $7.К_1$ и $7.К_4$ / At the combined action of factors with the characteristics of $7.К_1$ and $7.К_4$.
[2] При независимом воздействии факторов с характеристиками $7.К_1$ и $7.К_4$ / At the independent action of factors with the characteristics of $7.К_1$ and $7.К_4$.
[3] По катастрофическим отказам / For catastrophic failures.

номинала этого конденсатора позволяет задать время автономного функционирования микросхемы. Примеры осциллограмм напряжений на выводах Vdd и Vdd_C при нарушении и аварии питания микросхемы приведены на рис.6 и 7.

Из этих рисунков видно, что активизация супервизора питания TH1 произошла через 180 мс после отключения напряжения питания на выводе Vdd.

При отключенной функции сторожевого таймера выводы WDI, Cap_WD и WD_St можно не подключать. Микросхема имеет два информационных выхода типа "открытый сток", позволяющих внешним системам управления определять факты срабатывания защиты от тиристорного защелкивания и завершения времени ожидания сторожевого таймера.

some time by external capacitor C1. Selection of the value of this capacitor allows to set the time of autonomous operation of the chip. Examples of oscillogram of the voltages on Vdd and Vdd_C outputs in case of power disturbances are shown in Fig.6 and Fig.7.

Fig.6 and 7 show that the activation of the voltage supervisor TH1 occurred after 180 ms after disconnection of the power supply at Vdd output.

When the watchdog timer is disabled, the WDI, Cap_WD and WD_St outputs can be not connected. The microchip has two data outputs of "open drain" type, which allows external control systems to register the activation of the latch-up protection and the time-out of watchdog timer.

The microchip performs its functions and stores the values of parameters during and after the impact of special factors with characteristics given in the table in accordance with GOST RV 20.39.414.2-98.

For testing of microchips the SMC "Technological Centre" created measuring stand that allows automated precision analog and digital measurements of elements on the wafers and after the packaging.

Thus, to increase the resistance of electronic component base, which operates in conditions of influence of external cosmic factors, the specialized microchips 1469TK025 and 1469TK035 with the function of latch-up protection are proposed. The microchips successfully passed tests and are produced with VP (military acceptance) quality. Both microchips are made in compact package MK 5123.28-1.01. ■

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

Микросхема выполняет свои функции и сохраняет значения параметров во время и после воздействия специальных факторов со значениями характеристик, приведенных в таблице в соответствии с ГОСТ РВ 20.39.414.2-98.

Для проверки микросхем после изготовления в НПК "Технологический центр" создан контрольно-измерительный стенд, который позволяет проводить прецизионные автоматизированные аналоговые и цифровые измерения элементов как на пластинах, так и после корпусирования.

Таким образом, для повышения стойкости электронной компонентной базы, работающей в условиях воздействия внешних космических факторов, предложены специализированные микросхемы 1469ТК025 и 1469ТК035 с функцией защиты от тиристорного эффекта. Микросхемы успешно прошли испытания и выпускаются с категорией качества ВП. Оба варианта микросхем выполнены в малогабаритном корпусе МК 5123.28-1.01.

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

ЛИТЕРАТУРА

1. **Чумаков А.И., Васильев А.Л., Козлов А.А., Кольцов Д.О., Криницкий А.В., Печенкин А.А., Тараксин А.С., Яненко А.В.** Прогнозирование локальных радиационных эффектов в ИС при воздействии факторов космического пространства // Микроэлектроника. 2010. Т. 39. №2. С. 85–90.
2. **Чумаков А.И.** Действие космической радиации на ИС // Радио и связь. 2004. 320 с.
3. **Holmes-Siedle A., Adams L.** Handbook of Radiation Effects // Oxford university press. 1993. 479 p.
4. **Messenger G.C., Ash M.S.** Single Event Phenomena. – N.Y., Chapman&Hall. 1997. 368 p.
5. **Коняхин В.В., Денисов А.Н., Федоров Р.А., Вильсон А.Л., Бражников С.С., Коновалов В.С., Малашевич Н.И., Росляков А.С.** Микросхемы для аппаратуры космического назначения : Практическое пособие / Под общ. ред. Саурова А.Н. – М.: ТЕХНОСФЕРА, 2016. 388 с.
6. **Гаврилов С.В., Денисов А.Н., Коняхин В.В., Малашевич Н.И., Фёдоров Р.А.** Семейство серии базовых матричных кристаллов // Известия ВУЗов. Электроника. 2015. №5 (101). С. 497–504.

МИКРОСХЕМА ЦИФРОВОЙ ГАЛЬВАНИЧЕСКОЙ РАЗВЯЗКИ
DIGITAL GALVANIC ISOLATION CIRCUIT

УДК 621.382, ВАК 05.27.01

А.Лукьянов, Р.Фёдоров* / A.Lykyanov@tcen.ru, R.Fedorov@tcen.ru*
A.Lykyanov, R.Fedorov**

Рассматриваются особенности проектирования микросхем гальванической развязки. На основе унифицированной библиотеки ячеек серии базовых кристаллов 5521 показана разработка микросхемы двухканальной трансформаторной гальванической развязки, приводится описание основных функциональных блоков и принципов работы.

This paper presents the features of the galvanic isolation circuit design. It shows the development of a dual-channel transformer galvanic isolation circuit and describes the main functional units and the principles of their operation on the basis of the unified cell library of 5521 gate array family.

В настоящее время при разработке систем передачи сигналов управления, приема данных измерительного и медицинского оборудования инженеры сталкиваются с необходимостью использования гальванической развязки, которая позволяет осуществить передачу энергии между электрическими цепями без электрического контакта.

Гальваническая развязка позволяет решить следующие задачи:

- защитить оборудование и людей от поражения электрическим током;
- повысить помехоустойчивость систем;
- осуществить сопряжение электрических цепей с разными питающими напряжениями.

Наиболее широкое распространение получили три основных метода реализации гальванической развязки [1]:

- оптический;
- емкостной;
- трансформаторный.

В основе оптической гальванической развязки (оптрона) лежит принцип передачи информации через изолирующий барьер световым потоком с помощью светодиодов и фотоприемников. Пример конструкции оптрона приведен на рис.1.

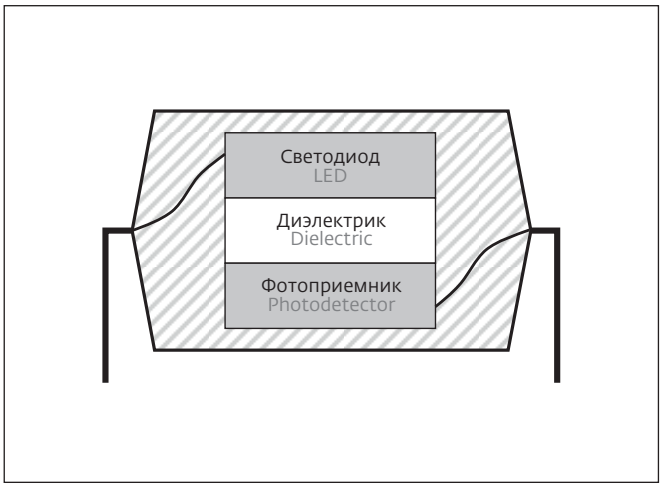


Рис.1. Пример конструкции оптрона
Fig.1. Example of design of optocoupler

Оптическая гальваническая развязка имеет большое напряжение изоляции (до 7000 В) и высокую устойчивость к воздействию синфазных помех между входом и выходом (около 15 кВ/мкс). Верхняя рабочая частота оптронов, оптимизированных под высокочастотную передачу цифровых сигналов, достигает нескольких десятков МГц, например 100 Мбит/с в микросхеме HCPL-090J-000E фирмы Avago Technologies. Оптроны устойчивы к электрическим и магнитным полям. Недостатками оптронов являются высокая рассеиваемая мощность (150–200 мВт на канал), относительно низкая скорость передачи, деградация структуры светодиодов с течением времени. При изготовлении светодиодов используются материалы (GaAs), которые не позволяют напря-

° НПК "Технологический Центр" / SMC "Technological Centre".

мую интегрировать их в рамках одного технологического процесса с микроконтроллером или драйвером.

В основе емкостной гальванической развязки (рис.2) лежит принцип работы электрического конденсатора. Емкостные изоляторы блокируют постоянный ток с помощью диэлектрика между двумя проводниками. Переменное электрическое поле высокой частоты позволяет передать сигналы через диэлектрический барьер. К достоинствам емкостных гальванических развязок можно отнести высокую скорость передачи (например, 150 Мбит/с у микросхемы SI84xx фирмы Silicon Labs), низкую рассеиваемую мощность (примерно 30 мВт/канал), высокую устойчивость к воздействию синфазных помех между входом и выходом (около 25 кВ/мкс) и невосприимчивость к магнитным полям. Напряжение изоляции у емкостной гальванической развязки не превышает 4000 В. К особенностям емкостной гальванической развязки можно отнести технологическую сложность изготовления конструкции конденсаторов.

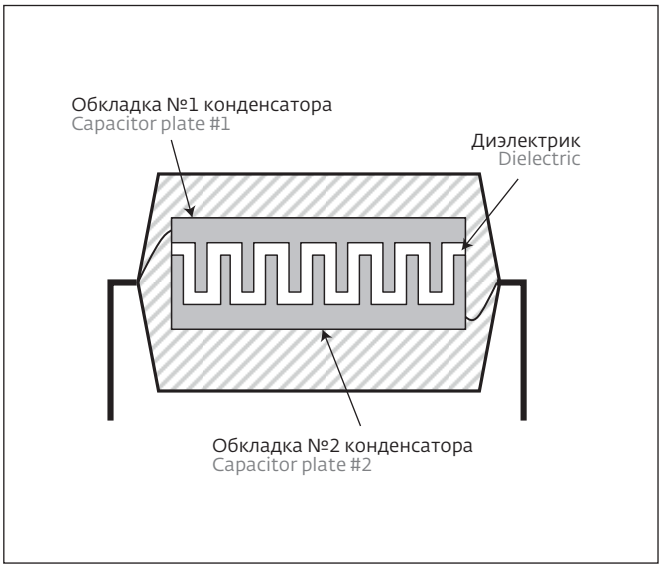


Рис.2. Пример конструкции емкостной развязки
Fig.2. Example of a design of capacitive decoupling

Трансформаторный метод обеспечивает развязку с помощью изоляции между двумя катушками индуктивности. Требуемый сигнал переменного тока передается через взаимную индуктивность обмоток трансформатора. Традиционные трансформаторы имеют большие размеры, но с увеличением частоты сигнала появляется возможность уменьшения их габаритов. Так поступила фирма Analog Devices в своих гальванических развязках серии ADuM [2]. Развязка состоит из двух кристаллов, размещенных в одном корпусе. Кристаллы изготавливаются по обычной КМОП-технологии, на одном из кристаллов размещается трансформатор на полиимидных слоях, как показано на рис.3.

Трансформаторная развязка позволяет работать со скоростью до 100 Мбит/с. Напряжение изоляции достигает 4000 В. Из-за отсутствия магнитного сердечника развязка невосприимчива к постоянным магнитным полям,

Currently, the developers of transmission systems for control signals and data acquisition of measuring and medical equipment are faced with the necessity of the use of galvanic isolation, which enables the transfer of energy between circuits without an electrical contact.

The galvanic isolation allows to solve the following tasks:

- protection of equipment and people from electric shock;
- increasing the noise immunity of the system;
- coupling of electrical circuits with different supply voltages.

The most widespread are three main methods of galvanic isolation [1]:

- optical;
- capacitive;
- transformer.

The basis of optical galvanic isolation is the principle of information transfer across an isolation barrier by means of light flux using LEDs and photodetectors. Example of optocoupler design is shown in Fig.1.

Optical galvanic isolation (optocoupler) has a high isolation voltage (up to 7000 V) and a high resistance to common-mode interference between input and output (about 15 kV/μs). The upper operating frequency of optocouplers, which are optimized for high frequency transmission of digital signals, reaches several tens MHz, for example 100 Mbit/s in the chip HCPL-090J-000E of Avago Technologies. Optocouplers are resistant to electrical and magnetic fields. The disadvantages of optocouplers are high power dissipation (150–200 mW per channel), the relatively low transfer rate, the degradation of LEDs over time. Materials (GaAs), used in the manufacture of LEDs, don't allow to integrate them directly within a single workflow

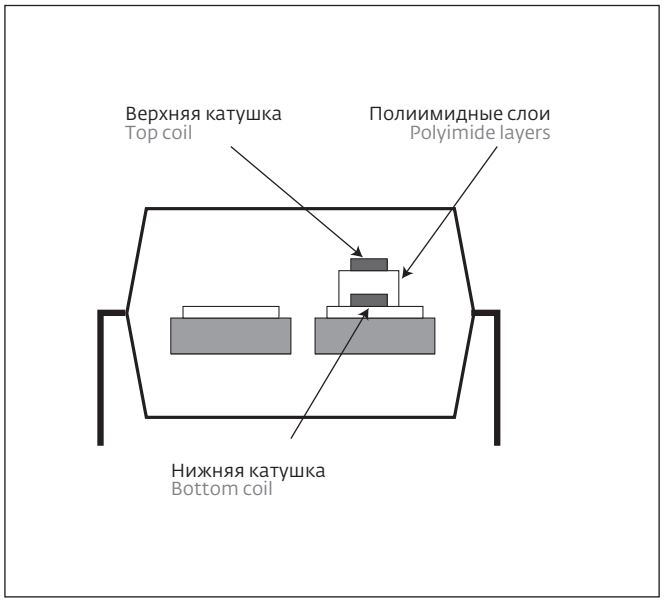


Рис.3. Пример конструкции трансформаторной развязки фирмы AD

Fig.3. Example of design of transformer decoupling designed by AD

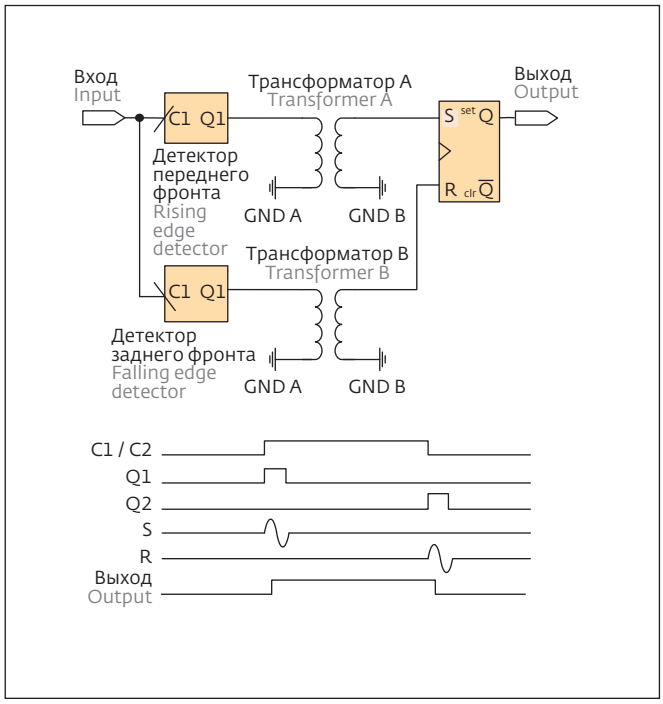


Рис.4. Схема передачи информации "установка / сброс" с двойным трансформатором

Fig.4. Information transmission scheme "set / reset" with dual transformer

а малый размер способствует низкой восприимчивости к переменным магнитным полям.

При реализации микросхемы трансформаторной гальванической развязки, выполненной на КМОП-технологии, можно использовать три основных принципа передачи информации:

- "установка/сброс";
- амплитудная модуляция;
- полярность импульсов.

Схема передачи информации "установка/сброс" с двойным трансформатором приведена на рис.4. Достоинством этой схемы является простота реализации, недостатком – большая занимаемая площадь на кристалле, поскольку для одного канала требуется два трансформатора.

with the microcontroller or driver.

The capacitive galvanic isolation (Fig.2) is based on the working principle of an electrical capacitor. Capacitive isolators block DC current through the dielectric between the two conductors. The alternating electric field of high frequency allows to transmit signals through the dielectric barrier. The advantages of capacitive galvanic isolation include high transmission speed (for example, 150 Mbit/s in SI84xx chip of Silicon Labs) low power dissipation (about 30 mW/channel), high resistance to common-mode interference between input and output (about 25 kV/μs) and immunity to magnetic fields. Isolation voltage of the capacitive galvanic isolation is not more than 4000 V. A feature of capacitive galvanic isolation is the technological complexity of manufacturing of capacitors.

The transformer design provides isolation by using the isolation between the two inductors. The required AC signal is transmitted through mutual inductance of the transformer windings. Traditional transformers are large in size, but with increasing signal frequency, the possibility of reduction of their overall dimensions appears. This was done by Analog Devices in their galvanic isolations of ADuM family [2]. The isolation consists of two chips placed in a single package. The chips are made by conventional CMOS technology, a transformer on polyimide layers is placed on one of the chips, as shown in Fig.3.

Transformer isolation allows to work at speeds up to 100 Mbps. Isolation voltage reaches 4000 V. Due to the lack of the magnetic core the isolation is immune to constant magnetic fields, and the small size contributes to low

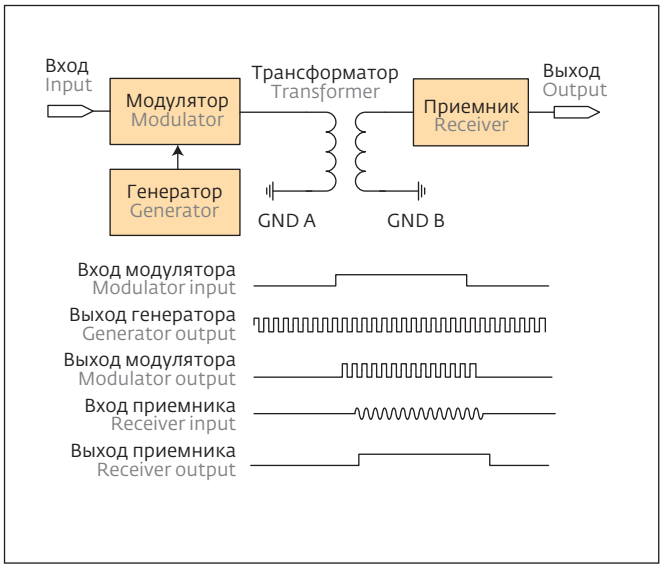


Рис.5. Схема передачи информации при амплитудной модуляции

Fig.5. Information transmission in case of amplitude modulation

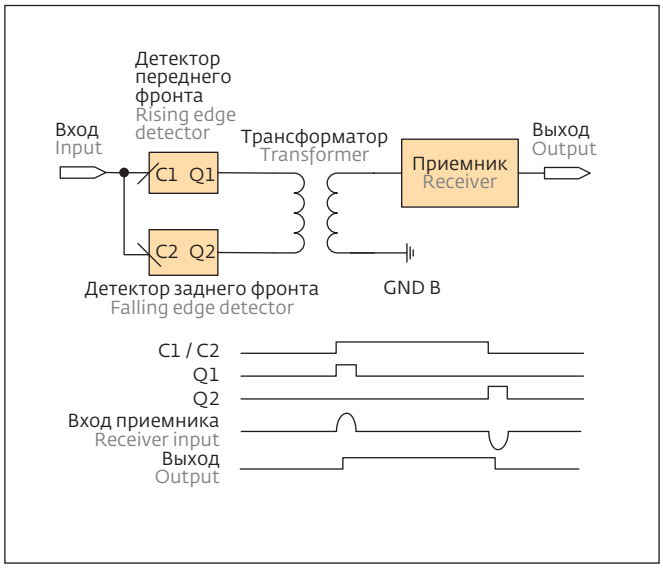


Рис.6. Схема передачи информации на основе полярных импульсов

Fig.6. Information transmission scheme based on polar impulses

Схема передачи на основе амплитудной модуляции (рис.5) является несколько сложнее в реализации, но занимает меньшую площадь, поскольку использует один трансформатор.

В схеме передачи информации на основе полярных импульсов (рис.6) также используется один трансформатор. Достоинством этой схемы является низкая потребляемая мощность.

В рамках одного КМОП-технологического процесса возможно изготовление трансформаторной гальванической развязки и схемы управления на двух кристаллах. Это позволяет достичь значения напряжений изоляции порядка 4 000 В и обеспечить устойчивость к воздействию синфазных помех между входом и выходом, на уровне 15 кВ/мкс.

В НПК "Технологический центр" на основе унифицированной библиотеки ячеек серии базовых кристаллов 5521 была разработана заказная микросхема двухканальной гальванической развязки.

sensitivity to alternating magnetic fields.

In the transformer galvanic isolation IC made by CMOS technology, it is possible to use the three main principles of information transfer:

- set/reset;
- amplitude modulation;
- polarity of pulses.

The information transmission scheme "set/reset" with dual transformer is shown in Fig.4. The advantage of this scheme is simplicity of implementation, the disadvantage is large footprint on the chip, since each channel requires two transformers.

Transmission scheme based on amplitude modulation (Fig.5) is somewhat more complicated to implement, but takes less space because it uses a single transformer.

The information transmission scheme based on polar pulses (Fig.6) also uses a single transformer. The advantage of this design is low power consumption.

In single CMOS workflow it is possible to manufacture transformer galvanic isolation and control circuitry on the two chips. This allows to achieve values of voltage isolation about 4 000 V and to provide resistance to common-mode interference between input and output (at the level of 15 kV/μs).

SMC "Technological Centre" have developed a custom microcircuit of dual-channel galvanic isolation on the basis of unified library of gate array cells of 5521 family. The microcircuit is manufactured by 0.18 μm radiation-resistant CMOS process on bulk silicon. Supply voltage is 3 V ±10% or 3.3 V ±10% [3, 4]. The microcircuit is made in the body 5123.28-1 in the form of microassembly of two chips: a transmitter and a receiver.

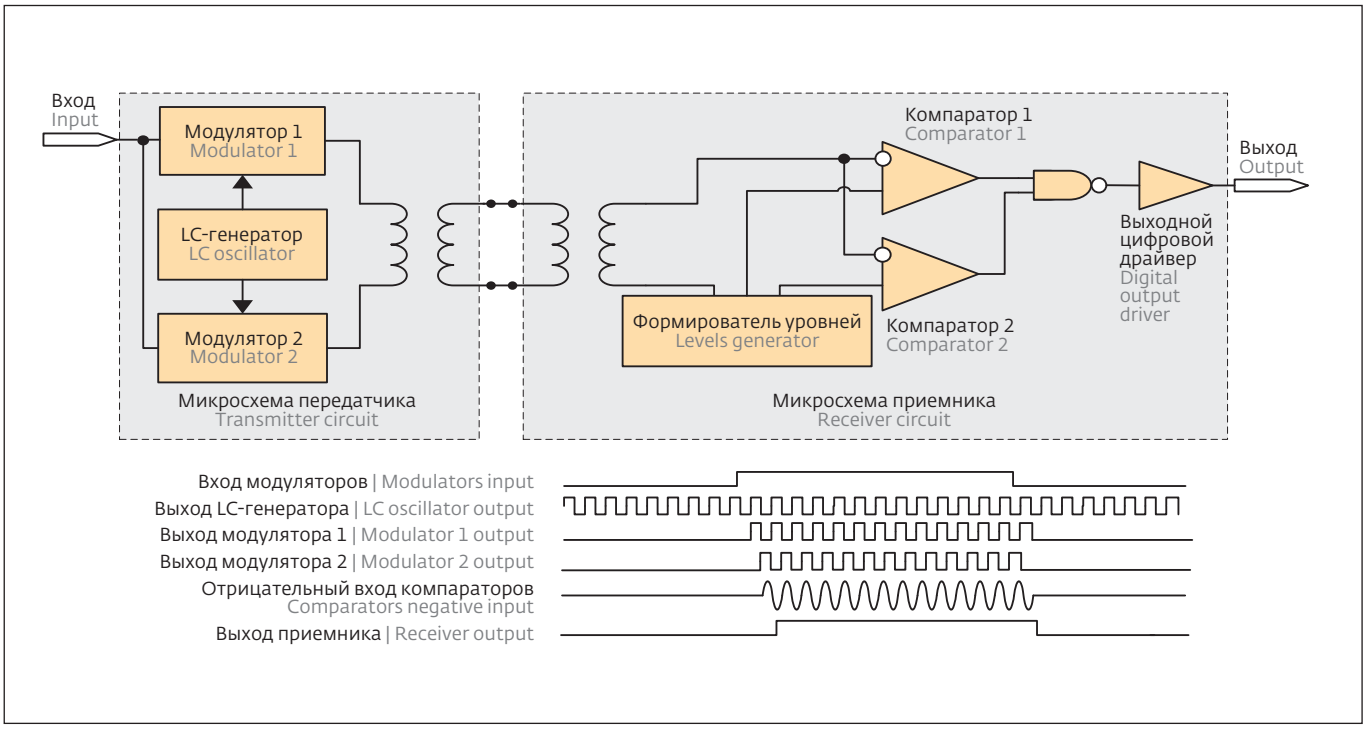


Рис.7. Структурная схема одного канала микросхемы трансформаторной гальванической развязки
Fig.7. Structural diagram of one channel of transformer galvanic isolation circuit

Микросхема изготавливается по радиационностойкой КМОП-технологии с нормами 0,18 мкм на объемном кремнии. Напряжение питания составляет 3 В ±10% или 3,3 В ±10% [3, 4]. Микросхема выполнена в корпусе 5123.28-1 в виде микросборки из двух кристаллов: передатчика и приемника.

При передаче информации используется амплитудная модуляция в связи с простотой ее реализации и высокой скоростью, около 100 Мбит/с. Структурная схема одного канала микросхемы трансформаторной гальванической развязки показана на рис.7. Передатчик содержит

Amplitude modulation is used to data transfer in connection with the simplicity of its implementation and high speed of about 100 Mbps. Structural diagram of one channel of the transformer galvanic isolation is shown in Fig.7. The transmitter contains an LC oscillator and two modulators. The receiver circuit includes two comparators, block of comparison levels formation for the comparators, combinational logic and the digital output driver.

LC oscillator generates for two modulators the carrier frequency of 800 MHz. The output signals of the modulators are a function of multiplying the input signal and the carrier frequency, which is supplied to the modulators with phase shift of 180°. The signals from the modulators are transferred to primary winding of the first transformer.

The input of the receiver receives a signal from the secondary winding of the second transformer. Signal detection is carried out using high frequency comparators and combinational logic circuit.

The transformers in the microcircuits of receiver and transmitter are placed in the upper layers of metallization (Fig.8). To increase the isolation voltage, two transformers are used in a single channel, which are connected in series with wire conductors. The substrates of the transmitter and receiver circuits are isolated from each other.

The main parameters of the galvanic isolation circuit developed in the SMC "Technological Centre" are presented in the table in comparison with ADUM1100 chip of Analog Devices. ■

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 8.537.2016/БЧ.

Сравнение характеристик микросхем
Comparison of characteristics of circuits

Параметр Characteristic	Analog Devices ADUM1100	Микросхема НПК ТЦ SMC TC circuit
Скорость передачи данных, Мбит/с Data transmission speed, Mbit/s	До 100	До 200
Ток потребления на канал, мА Current consumption per channel, mA	16	15
Напряжения питания, В Supply voltage, V	3,0–5,5	2,7–3,6
Задержка распространения, нс Propagation delay, ns	28	4,7
Количество каналов Number of channels	1	2
Напряжение изоляции, В Isolation voltage, V	4000	4000

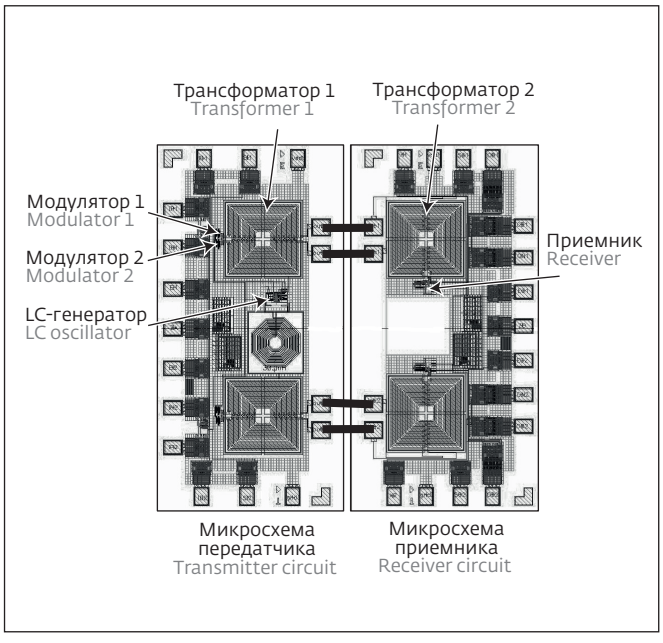


Рис.8. Топология микросборки двухканальной трансформаторной гальванической развязки, разработанной в НПК "Технологический центр"
Fig.8. Topology of microassembly of dual channel transformer galvanic isolation developed in SMC "Technological Centre"

LC-генератор и два модулятора. Схема приемника включает два компаратора, блок формирования уровней сравнения для компараторов, комбинационную логику и выходной цифровой драйвер.

LC-генератор формирует для двух модуляторов несущую частоту 800 МГц. Выходные сигналы модуляторов являются функцией умножения входного сигнала и несущей частоты, которая подается на модуляторы со сдвигом по фазе 180°. Сигналы с модуляторов поступают на первичную обмотку первого трансформатора.

На вход приемника поступает сигнал со вторичной обмотки второго трансформатора. Детектирование сигнала осуществляется с помощью высокочастотных компараторов и схемы на комбинационной логике.

Трансформаторы в микросхемах приемника и передатчика выполнены в верхних слоях металлизации (рис.8). Для увеличения значения напряжения изоляции в одном канале используется два трансформатора, последовательно соединенные проволочными проводниками. Подложки микросхем передатчика и приемника при этом изолированы друг от друга.

В таблице указаны основные параметры разработанной в НПК "Технологический центр" микросхемы гальванической развязки в сравнении с микросхемой-аналогом ADUM1100 фирмы Analog Devices.

Статья подготовлена при финансовой поддержке Минобрнауки России в рамках выполнения государственного задания 8.537.2016/БЧ.

ЛИТЕРАТУРА

1. **Cory Lynn Fandrich.** An On-Chip Transformer-Based Digital Isolator System. University of Tennessee, Knoxville 2013.
2. http://www.analog.com/media/en/technical-documentation/technical-articles/MS-2234.pdf
3. **Коняхин В.В., Денисов А.Н., Федоров Р.А., Вильсон А.Л., Бражников С.С., Коновалов В.С., Малашевич Н.И., Росляков А.С.** Микросхемы для аппаратуры космического назначения : Практическое пособие / Под общ.ред.Саурова А.Н. – М.: ТЕХНОСФЕРА, 2016. 388 с.
4. **Гаврилов С.В., Денисов А.Н., Коняхин В.В., Малашевич Н.И., Федоров Р.А.** Семейство серий базовых матричных кристаллов // Известия ВУЗов. Электроника. 2015. №5(101). С. 497–504.

СОЗДАНИЕ ЭЛЕМЕНТОВ ОДНОКРАТНОГО ПРОГРАММИРОВАНИЯ ДЛЯ БК СЕРИЙ 5521 И 5529

CREATING ONE-TIME PROGRAMMABLE ELEMENTS FOR 5521 AND 5529 GATE ARRAY FAMILIES

УДК 621.382, ВАК 05.27.01

А.Семенов, С.Белостоцкая* / A.Semenov@tcen.ru, S.Belostotskaya@tcen.ru*
A.Semenov, S.Belostotskaya**

Рассматривается пример разработки элементов однократного программирования в виде плавких перемычек (ПП) для базовых кристаллов серий 5521 и 5529. Представлены экспериментальные данные полученных образцов плавких перемычек. Показана возможность применения сложного функционального блока металлической ПП в составе микросхемы.

This paper describes an example of one-time programmable elements design in the form of fusible links (FL) for 5521 and 5529 gate array families. The experimental data of the obtained samples of FL are presented. The applicability of the IP cores of FL as part of the chip is also shown.

Элементы однократного программирования широко востребованы в интегральных схемах, где требуется подстройка электрических параметров или режимов работы после изготовления. Такими микросхемами, как правило, являются источники опорного напряжения, ПЛИС и ПЗУ. Наличие сложного функционального блока (СФ-блока) однократного программирования в библиотеке функциональных ячеек базовых кристаллов (БК) серии 5521 и 5529 [1, 2] позволяет увеличить номенклатуру разрабатываемых микросхем и область их применения.

Элементом однократного программирования, или плавкой перемычкой (ПП) называется соединительный элемент, который по умолчанию замкнут накоротко. Для получения требуемой конфигурации схемы часть перемычек при подаче большого тока разрушается (пережигается) и цепь размыкается. Преимуществом элементов однократного программирования является малая занимаемая площадь на кристалле [3].

В НПК "Технологический центр" ведется разработка СФ-блока ПП для применения в БК серии 5521. Данная серия БК изготавливается по радиационностойкой КМОП-технологии с нормами 0,18 мкм на объемном кремнии. Напряжение питания составляет 3 В ±10% или 3,3В ±10%.

При разработке структуры ПП необходимо, чтобы максимальное значение напряжения пережигания ПП не превышало значения допустимого напряжения питания микросхемы.

Для реализации ПП были выбраны имеющиеся в технологии КМОП 0,18 мкм слои металлизации

Таблица 1. Технологические параметры разработанных ПП
Table 1. Technological parameters of developed FL

Тип ПП Type of FL	Толщина, мкм Thickness, μm	Поверхностное сопротивление, Ом/кв Surface resistance, Ω/sq	Минимальная ширина проводника Wmin, мкм Minimum width of conductor Wmin, μm
Металл Metal	0,5	0,072	0,32
n+ полицид n+ policide	0,2	8	0,18

° НПК "Технологический Центр" / SMC "Technological Centre".

Таблица 2. Результаты пережигания металлических ПП с параметрами L=1,7 мкм, W=0,32 мкм

Table 2. Results of burnout of metal FL with L=1.7 μm, W=0.32 μm

№ образца Sample number	1	2	3	4
Ток пережигания, мА Burnout current, mA	200	175	175	190
Напряжение пережигания, В Burnout voltage, V	1,05	1,27	1,28	1,3
Сопротивление до пережигания, Ом Resistance before burnout, Ω	0,4	0,4	0,4	0,4
Сопротивление после пережигания, ГОм Resistance after burnout, GΩ	> 1	> 1	> 1	> 1

Таблица 3. Результаты пережигания металлических ПП с параметрами L=1,0 мкм, W=0,32 мкм

Table 3. Results of burnout of metal FL with L=1.0 μm, W=0.32 μm

№ образца Sample number	1	2	3	4
Ток пережигания, мА Burnout current, mA	250	250	233	225
Напряжение пережигания, В Burnout voltage, V	1,05	1,27	1,28	1,3
Сопротивление до пережигания, Ом Resistance before burnout, Ω	0,22	0,22	0,22	0,22
Сопротивление после пережигания, ГОм Resistance after burnout, GΩ	> 1	> 1	> 1	> 1

Таблица 4. Результаты пережигания полицидных ПП с параметрами L=1,7 мкм, W=0,18 мкм

Table 4. Results of burnout of policide FL with L=1.7 μm, W=0.18 μm

№ образца Sample number	1	2	3	4
Ток пережигания, мА Burnout current, mA	10	10	10	10
Напряжение пережигания, В Burnout voltage, V	4	3,93	4,1	4,2
Сопротивление до пережигания, Ом Resistance before burnout, Ω	75	75	75	75
Сопротивление после пережигания, кОм Resistance after burnout, kΩ	20	15	12	17

Таблица 5. Результаты пережигания полицидных ПП с параметрами L=1,0 мкм, W=0,18 мкм

Table 5. Results of burnout of policide FL with L=1.0 μm, W=0.18 μm

№ образца Sample number	1	2	3	4
Ток пережигания, мА Burnout current, mA	10	10	10	10
Напряжение пережигания, В Burnout voltage, V	3,4	3,66	3,23	3,36
Сопротивление до пережигания Ом Resistance before burnout, Ω	45	45	45	45
Сопротивление после пережигания, кОм Resistance after burnout, kΩ	18,2	21	19	18

и полицида. В табл.1 представлены параметры тестовых структур ПП, разработанных по КМОП-технологии 0,18 мкм.

Было заложено по два варианта с разной длиной ПП. Ширина ПП выбиралась минимально допустимой. После изготовления тестовых структур были

The one-time programmable elements are widely demanded in integrated circuits if the adjustment of electrical parameters or operation modes after manufacture are required. Such circuits typically include a reference voltage sources, PLD and ROM. The presence of one-time programmable IP core in the library of functional cells of 5521 and 5529 gate array families [1, 2] allows to increase the range of the developed microchips and their application area.

One-time programmable element or fusible link (FL) is the connecting element, which by default is shorted. To obtain the required schema configuration a part of the links is destroyed (burned) by applying high current and the circuit is opened. The advantage of the one-time programmable elements is a small footprint on the chip [3].

SMC "Technological Centre" develops IP core of FL for use in 5521 gate array family. The gate array family is manufactured by 0.18 μm radiation-resistant CMOS process on bulk silicon. Supply voltage is 3 V ±10% or 3.3 V ±10%.

In designing the FL structure it is necessary that the maximum voltage of the FL burnout does not exceed the permissible supply voltage of the chip.

For the implementation of FL the metallization and policide layers that are available in the 0.18 μm CMOS process were chosen. Table.1 presents the parameters of the test structures for FL, developed by 0.18 μm CMOS technology.

Samples with two different length of FL were studied. Minimum admissible values of width of FL were chosen. Fabricated test structures were tested for burnout of FL. The results are presented in tables

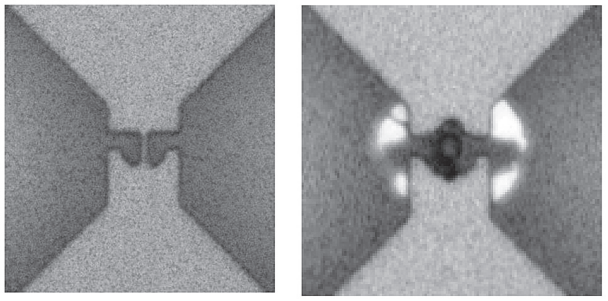


Рис.1. Металлическая ПП до (a) и после (b) пережигания
Fig.1. Metal FL before (a) and after (b) burnout

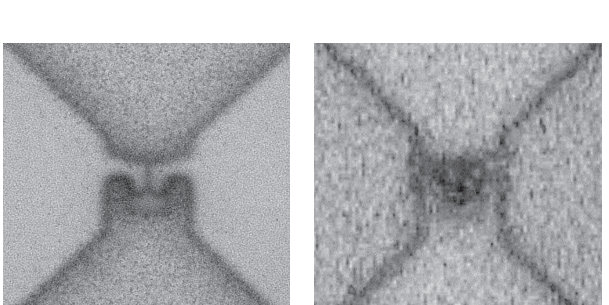


Рис.2. Кремниевая ПП до (a) и после (b) пережигания
Fig.2. Silicon FL before (a) and after (b) burnout

проведены исследования по пережиганию ПП. Результаты представлены в табл.2–5. Конструкции ПП ранее были рассмотрены в [4] и [5].

Фотографии металлических ПП до и после пережигания представлены на рис.1. По результатам контроля электрофизических параметров ПП можно сделать следующие выводы. Металлические ПП имеют большое остаточное сопротивление (более 1 ГОм), что позволяет применять их при подстройке сопротивления в аналоговых блоках и в устройствах однократного программирования. Для пережигания металлических ПП требуется ток около 200–25 мА, коммутация которого требует применения аналоговых ключей на МОП-транзисторах с большим значением ширины канала. Это может стать лимитирующим фактором в случаях, когда имеются ограничения на размер кристалла микросхемы.

Снимки кристаллов кремниевых ПП до и после пережигания представлены на рис.2. Кремниевые ПП имеют остаточное сопротивление 12–20 кОм и небольшие токи пережигания около 10 мА. Для подстройки аналоговых блоков из-за большого разброса остаточного сопротивления и низкого его номинала кремниевые ПП малопригодны. Данные ПП могут найти применение в микросхемах с функцией однократного программирования.

СФ-блок металлической плавкой перемычки был использован при разработке микросхемы супервизора напряжения питания 5521ТР015-710. Матрица из металлических ПП, входящая в состав блока стабилизатора напряжения, с помощью регистра управления дает возможность однократно программировать

2–5. Design of PP was previously considered in [4] and [5].

Photos of metal FL before and after burnout are presented in Fig.1. The results of the control of electro-physical parameters of FL allow us to draw the following conclusions. Metal FL have great residual resistance (>1 GΩ), allowing to use them for adjusting the resistance in the analog blocks in a one-time programmable devices. Burnout of metal FL requires current of about 200–250 mA, switching of which requires the use of analog keys on MOS transistors with a large channel width. This can become a limiting factor in cases of restrictions on the size of the chip.

Photos of the silicon FL before and after burnout are shown in Fig.2. Silicon FL have a residual resistance of 12–20 kΩ and a small burnout currents of about 10 mA. Due to the large scatter of the residual resistance and its low values the silicon FL are not suitable to adjust analog blocks. Such FL can be used in circuits with one-time programmable function.

IP core of metal FL was used to develop IC of supply voltage supervisor 5521TP015-710. The matrix of metal FL, as a part of the voltage regulator, allow to program the value of the reference voltage of stabilizer using the control register. Fig.3 shows a fragment of the topology of the matrix of metal FL in the above mentioned chip.

Thus, the analysis of the experimental data for the samples of the fusible links confirms the possibility of using them for one-time programming as a part of chips developed on 5521 gate array family. ■

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

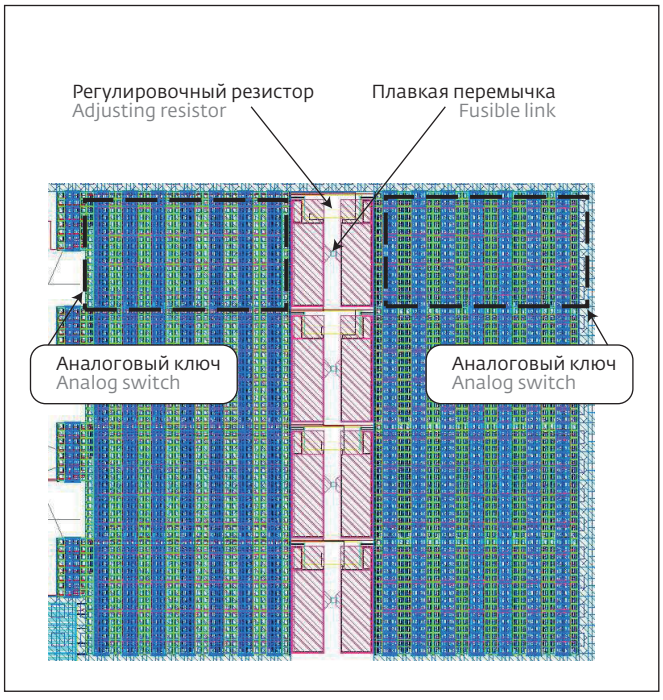


Рис.3. Фрагмент топологии матрицы металлических ПП в составе микросхемы супервизора напряжения питания 5521ТР015-710

Fig.3. Fragment of topology of matrix of metal FL in structure of IC of supply voltage supervisor 5521TP015-710

значение опорного напряжения стабилизатора. На рис.3 представлен фрагмент топологии матрицы металлических ПП в вышеуказанной микросхеме.

Таким образом, анализ экспериментальных данных образцов плавких перемычек подтверждает возможность использования их для однократного программирования в составе микросхем, разрабатываемых на БК серии 5521.

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

ЛИТЕРАТУРА

1. **Коняхин В.В., Денисов А.Н., Федоров Р.А., Вильсон А.Л., Бражников С.С., Коновалов В.С., Малашевич Н.И., Росляков А.С.** Микросхемы для аппаратуры космического назначения : Практическое пособие / Под общ.ред.Саурова А.Н. – М.: ТЕХНОСФЕРА, 2016. 388 с.
2. **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.
3. **Рабаи Ж.М., Чандракасан А., Николич Б.** Цифровые интегральные схемы. Методология проектирования / 2-е изд, пер. с англ. – М.: Вильямс, 2007. 912 с.
4. **William Jeong-Ho Kim, Du-Hwi Kim, Liyan Jin, Pan-Bong Ha, and Young-Hee Kim.** Design of 1-Kb eFuse OTP Memory IP with Reliability Considered. Journal of semiconductor technology and science. 2011. Vol. 11. No. 2.
5. **Tonti R.** eFuse Design and Reliability. IBM Semiconductor Research and Development Corporation. 1000 River Street, Essex Junction VT 05452.

KEYSIGHT TECHNOLOGIES РАСШИРИЛА ФУНКЦИИ ACM 9500

Компания KeysightTechnologies объявила о добавлении новых функций в быстродействующий атомно-силовой микроскоп 9500.

Новые возможности реализованы благодаря программной системе KeysightNanoNavigator, графический интерфейс которой упрощает работу пользователей микроскопа. Последняя версия NanoNavigator поддерживает функцию QuickSense – режим построения изображения, позволяющий выполнять количественную оценку наномеханических свойств широкого круга образцов. QuickSense позволяет быстро и просто устанавливать амплитуду и частоту модуляции, захватывать отдельные силовые кривые и измерять адгезию и жесткость. Все данные собираются в то время, пока микроскоп 9500 строит изображения топографии образца, что позволяет точно определять флуктуации локальных механических свойств в наномасштабе.

Новая версия NanoNavigator поддерживает контроль потенциалов и циклическую полярографию для электрохимических приложений, что дополняет собственные возможности построения изображения системы 9500. Функции контроля окружающей среды (газов, жидкостей и воздуха) и температуры облегчают реализацию проектов, относящихся к материаловедению, биологии и измерению электрических параметров.

Кроме того, последняя версия NanoNavigator поддерживает AFM-SECM – методику сканирующей зондовой микроскопии компании Keysight, которая предназначена для исследования поверхностной химической активности и изучения процессов на границе раздела жидкость-твердое тело и жидкость-жидкость. Окислительно-восстановительные реакции с участием активных частиц и их кинетические свойства очень важны для новых исследований, простирающихся от анализа биохимических сигналов (например, в живых клетках и тканях) до проблем материаловедения в таких областях, как технологии топливных элементов, катализ, зондирование и химия окружающей среды.

KeysightTechnologies

МИКРОСХЕМА УПРАВЛЕНИЯ МАТРИЧНЫМИ БУКВЕННО-ЦИФРОВЫМИ LED-ДИСПЛЕЯМИ (7 × 5)

CONTROL CIRCUIT FOR MATRIX ALPHANUMERIC LED-DISPLAYS (7 × 5)

УДК 621.382, ВАК 05.27.01

Д.Мамонов / dimitriy32ru@yandex.ru*
*D.Mamonov**

Рассматриваются особенности проектирования радиационно-стойкой микросхемы 5521ТР034-726 управления восемью матричными буквенно-цифровыми дисплеями (7×5) на основе базового кристалла серии 5521, выполненного по технологии 0,18 мкм. Объясняются принципы организации динамического управления светодиодными индикаторами, а также приводится описание основных функциональных блоков устройства.

The paper describes the design features of radiation-resistant circuit 5521TR034-726 for control of eight matrix alphanumeric displays (7 × 5) based on 5521 gate array family that is manufactured by 0.18 μm process. It explains the mechanisms of LED displays dynamic control and describes the main functional units of the device.

В качестве элементов индикации в современных цифровых комплексах используются жидкокристаллические панели, полупроводниковые электролюминесцентные и электрохромные индикаторы. Каждый из указанных типов индикаторов, основанных на различных физических принципах, предъявляет определенные требования к амплитудам управляющих напряжений, виду тока, плотности размещения на лицевых панелях приборов и внешней освещенности.

Высокие технические характеристики полупроводниковых индикаторов обеспечили их успешное применение в аппаратуре различного назначения. Особой популярностью пользуются матричные знакосинтезирующие индикаторы с динамическим управлением, пришедшие на смену сегментным индикаторам.

Матричные индикаторы относятся к классу знакосинтезирующих приборов, в которых информация, предназначенная для зрительного восприятия, отображается с помощью нескольких дискретных элементов, сгруппированных по строкам и столбцам. Матричным индикатором считается устройство, объединенное в законченном конструктивном корпусе.

Эргономические исследования показали, что 35-элементная матрица обеспечивает удовлетворительное восприятие знаковой информации, в частности, прописных и строчных букв русского алфавита, знаков и цифр, букв греческого и латинского алфавитов [1].

К основным преимуществам матричных индикаторов по сравнению с сегментными относят широкие возможности и высокое качество отображения символов. Недостатки матричных индикаторов: сложность конструкции, стоимость, а также меньшая надежность вследствие большего количества элементов. При соединении многоразрядных индикаторов, расстояние между пикселями на швах отличается от расстояния в пределах одного индикатора, что накладывает ограничения на использование таких индикаторов для формирования единого изображения.

По способу управления матричные индикаторы делятся на два вида: статические и динамические (мультиплексные).

Статический способ подразумевает непосредственное управление каждым пикселем матрицы. Каждый элемент отображения имеет собственную ячейку памяти и светодиодный драйвер. Данный способ управления

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

используется в матрицах с большим размером пикселя, когда мощность и стоимость драйвера значительны. Также статическая схема применяется в устройствах с высокими требованиями к электромагнитному излучению. Однако подобный подход рационален только при небольшом разрешении (4×4 пикселя), поскольку при больших размерах значительно увеличивается количество управляющих элементов и схем ввода данных.

Для упрощения схемы управления, а также снижения количества выводов индикатора, разработан динамический способ управления, активно используемый в 35-элементых матрицах. Динамический способ подразумевает поочередное включение различных групп элементов отображения путем подачи напряжения с частотой более 20 Гц, при этом человеческий глаз воспринимает экран как непрерывно светящийся объект.

Матричные структуры выпускаемых буквенно-цифровых дисплеев позволяют осуществить управление только в режиме стробирования (динамическое управление). Структура матрицы предполагает два способа стробирования: по строкам или по столбцам.

Анализ рынка матричных буквенно-цифровых LED-дисплеев показал, что наиболее востребованными устройствами являются индикаторы типа HDSP-2131, разработанные компанией Avago Technologies [2]. В России подобные дисплеи выпускаются, но пока нет отечественных функциональных аналогов микросхем управления восьмьюразрядными буквенно-цифровыми дисплеями, поэтому возникла необходимость создания такой микросхемы.

В НПК "Технологический центр" на основе базового кристалла (БК) 5521ТР03 серии 5521 была разработана микросхема 5521ТР034-726 управления восьмью матричными буквенно-цифровыми дисплеями (7×5). БК серии 5521 изготавливаются по радиационно-стойкой КМОП-технологии с нормами 0,18 мкм на объемном кремнии. Напряжение питания 3 В ±10% или 3,3 В ±10% [3].

Разработка поведенческой модели микросхемы 5521ТР034-726, тестовых воздействий для ее проверки и топологическое проектирование осуществлялись средствами САПР БИС "Ковчег" [4]. При этом применялась унифицированная параметризованная библиотека функциональных ячеек серий БК 5521 и 5529.

В процессе разработки были сформулированы основные функциональные требования к микросхеме управления:

- вывод на дисплей ASCII-таблицы символов;
- возможность программирования 16-ти символов;
- функция мигания;
- настройка яркости дисплея;
- функция тестирования;
- функция очистки;
- возможность выбора тактовой частоты (использование внешнего сигнала или внутреннего генератора частоты на 1 МГц).

LCD panels, semiconductor electroluminescent and electrochromic indicators are used as display elements in a modern digital complexes. Each of these types of indicators based on different physical principles, is characterized by certain requirements to the amplitudes of the control voltages, type of current, density of placement on the front panels of devices and ambient light.

High technical characteristics of semiconductor indicators ensured their successful application in the equipment of various purpose. Especially popular are the matrix character indicators with dynamic control, which replace the segment indicators.

The dot matrix indicators belong to the class of character indicators, which display the visual information by means of several discrete elements, grouped in rows and columns. The dot matrix indicator is a device, which is combined into a finished constructive package.

Ergonomic studies have shown that the 35-element matrix provides a satisfactory perception of signs, in particular, uppercase and lowercase letters of the Russian alphabet, signs and numbers, letters of the Greek and Latin alphabets [1].

The main advantages of dot matrix indicators compared to the segment ones include a wide possibilities and high quality display of characters. Disadvantages of dot matrix indicators are the complexity of the design, cost, and also lower reliability due to the greater number of items. When connecting multi-bit indicators, the distance between the pixels at the seams differs from the distance within the indicator, which imposes restrictions on the use of such indicators to form a single image.

Depending on the method of control, the dot matrix

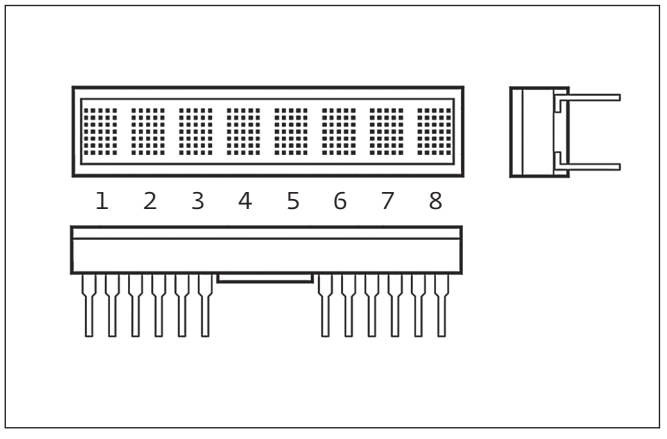


Рис.1. Конструкция индикатора
Fig.1. Indicator design

Конструкция индикатора, для которого разрабатывалась микросхема управления, представлена на рис.1 и состоит из восьми светодиодных матричных дисплеев по 35 пикселей в каждом. Микросхема управления дисплеями располагается на нижней стороне устройства в бескорпусном исполнении.

Функциональная схема устройства представлена на рис.2, где:

- "8×8 РЕГИСТР ОТОБРАЖАЕМЫХ СИМВОЛОВ" – регистр 8×8, который хранит адреса отображаемых символов;
- "РЕГИСТР СИМВОЛОВ И ОЗУ" – блок регистров для программирования пользовательских символов;

Таблица 1. Адреса регистров данных
Table 1. Addresses of data registers

$\overline{FL}$	A4	A3	Тип памяти Memory type	A2-A0
1	0	0	РЕГИСТР СИМВОЛОВ REGISTER OF SYMBOLS	
1	0	1	ОЗУ RAM	Адрес строки Address of row
1	1	0	РЕГИСТР РЕЖИМОВ РАБОТЫ REGISTER OF OPERATION MODES	–
1	1	1	8×8 РЕГИСТР ОТОБРАЖАЕМЫХ СИМВОЛОВ 8×8 REGISTER OF DISPLAYED CHARACTERS	Адрес символа Address of symbol

- "БЛОК УПРАВЛЕНИЯ" – блок задания сетки частот и сигналов управления;
- "ДЕШИФРАТОР ASCII" – дешифратор ASCII-таблицы символов;
- "ВЫХОДНОЙ ДРАЙВЕР" – выходной драйвер управления индикаторами.

Адреса регистров данных и режимов работы представлены в табл.1 и 2 соответственно.

Основным регистром, отвечающим за тип отображаемой информации, является блок "8×8 РЕГИСТР ОТОБРАЖАЕМЫХ СИМВОЛОВ". Данный

indicators are divided into two groups: static and dynamic (multiplex).

The static method means direct control of each pixel of the matrix. Each display item has its own memory cell, and a LED driver. This method of control is used in matrices with a large pixel size, when power and cost of drivers are significant. Also, the static scheme is applied in devices with high requirements for electromagnetic radiation. However, this approach is reasonable only at small resolution (4×4 pixel), since at larger sizes the number of control elements and circuits of the data input significantly increases.

To simplify control, and to reduce the number of indicator terminals, a dynamic control method is developed, which is actively used in 35-element matrixes. The dynamic method involves sequential activation of various groups of elements by applying a voltage with a frequency greater than 20 Hz, while the human eye perceives the screen as a continuously glowing object.

The matrix structures of the produced alpha-numeric displays allow to use only the gating mode of control (dynamic control). The matrix structure allows two methods of gating: by row or by column.

Analysis of market of matrix alphanumeric LED displays showed that the most popular devices are the indicators of the type HDSP-2131, developed by Avago Technologies [2]. In Russia, such displays are available, but there are no domestic analogues of functional chip for control of eight-bit alphanumeric displays, therefore there was a need of creating such a chip.

SMC "Technological Centre" on the basis of the gate array 5521TP03 of the 5521 family has

Таблица 2. Режимы работы регистров данных
Table 2. Operation modes of data registers

$\overline{RST}$	$\overline{CE}$	$\overline{WR}$	$\overline{RD}$	Режим Mode
1	0	0	0	–
		0	1	Запись Recording
		1	0	Чтение Reading
		1	1	–

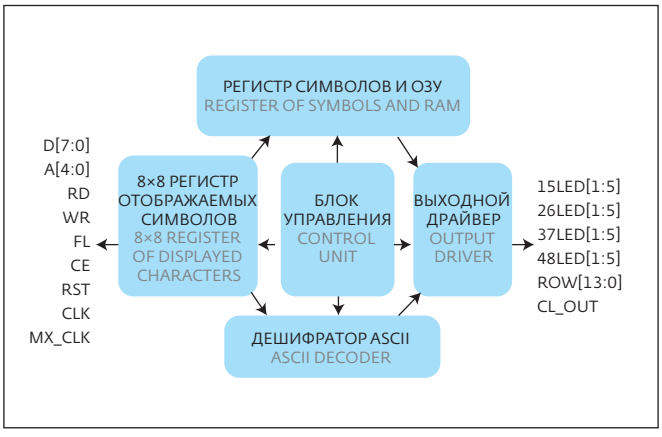


Рис.2. Функциональная схема микросхемы 5521ТР034-726
Fig.2. Functional diagram of 5521TP034-726 circuit

регистр хранит восемь адресов символов, номер каждого из которых соответствует номеру дисплея на индикаторе. В зависимости от значения D[7] происходит выбор типа информации для отображения:

- если D[7] = 0, то на дисплее отображается один из 128 символов ASCII-таблицы (адрес символа задается шиной D[6 : 0]). За декодирование символа отвечает блок "ДЕШИФРАТОР ASCII";
- если D[7] = 1, то на дисплее отображается один из 16-ти ранее запрограммированных пользовательских символов, (адрес символа задается шиной D[3 : 0]). Для программирования символов используются "РЕГИСТР СИМВОЛОВ И ОЗУ".

Запись символа в память осуществляется за восемь циклов. На первом этапе в "РЕГИСТР СИМВОЛОВ" записывается значение внешней шины данных D[7 : 0], четыре младших разряда которой и задают адрес раздела ОЗУ, в который будет производиться запись символа. Каждый раздел представляет собой матрицу ячеек памяти (7 × 5). На втором этапе осуществляется построчное заполнение раздела памяти за семь циклов, при этом номер строки определяется внешней шиной A[2 : 0], а значение строки задается шиной D[4 : 0].

Восьмибитовый "РЕГИСТР РЕЖИМОВ РАБОТЫ" отвечает за выполнение пяти режимов: использование регистра мигания, мигание, тестирование, очистка и регулировка яркости индикатора.

Регистр мигания отвечает за мигание каждого из дисплеев индикатора – хранящееся

developed a chip 5521TP034-726 for control eight dot matrix alphanumeric displays (7×5). Gate array of 5521 family is manufactured by radiation-resistant 0.18 μm CMOS process on bulk silicon. Supply voltage is 3 V ±10% or 3.3 V ±10% [3].

Development of a behavioral model of the chip 5521TP034-726, tests for its verification and the topological design was carried out Kovcheg CAD [4]. At that a unified library of functional cells of 5521 and 5529 gate array families was used.

During the development, the key functional requirements for the control chip were defined:

- display ASCII table of characters;
- ability to program 16 characters;
- blinking function;
- adjusting the brightness of the display;
- test function;
- cleanup function;
- ability to select the clock frequency (using an external signal or an internal oscillator with frequency of 1 MHz).

The design of the indicator, for which the control chip was developed, is presented in Fig.1 and consists of eight LED dot matrix displays with 35 pixels each. Control chip is located on the bottom side of the device in die form.

Functional diagram of the device is shown in Fig.2, where:

- 8×8 REGISTER OF DISPLAYED CHARACTERS is a register of 8×8, which stores the address of the displayed symbols;
- REGISTER OF SYMBOLS AND RAM is a block of registers for programming custom characters;
- CONTROL UNIT is a block to set the grid frequency and control signals;
- ASCII DECODER is the decoder for ASCII characters;

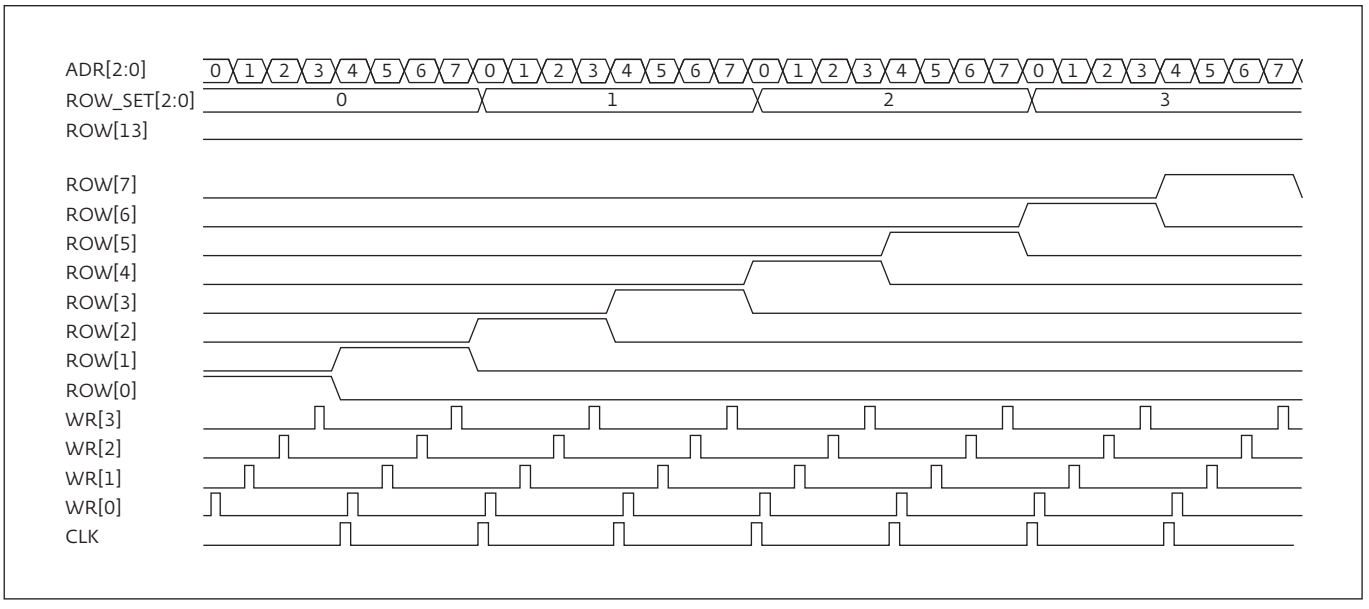


Рис.3. Временная диаграмма работы БЛОКА УПРАВЛЕНИЯ
Fig.3. Timing diagram of operation of CONTROL UNIT

в нем значение внешней шины данных D[7 : 0] определяет использование (D[n] = 1) или же не использование (D[n] = 0) функции мигания для n-го дисплея. Сигналом разрешения на использование данной функции является бит D[3] = 1, записанный в "РЕГИСТР РЕЖИМОВ РАБОТЫ", а при D[3] = 0 содержимое регистра мигания игнорируется.

Заставить мигать все дисплеи одновременно можно и без использования функции регистра мигания. Если записать бит D[4] = 1 в "РЕГИСТР РЕЖИМОВ РАБОТЫ", то активируется функция глобального мигания, при использовании которой все восемь дисплеев мигают одновременно. Содержимое регистра мигания при этом игнорируется. Частота мигания в обоих случаях составляет 2 Гц.

При D[6] = 1 запускается функция тестирования, которая заключается в отображении прямого и обратного шашечного узора на всех

- OUTPUT DRIVER is output driver of indicators control.

Addresses of data registers and operating modes are presented in table 1 and 2, respectively.

The main register, which is responsible for the type of displayed information is the 8×8 REGISTER OF DISPLAYED CHARACTERS block. This register stores eight addresses of symbols, the number of each of which corresponds to a display number on the indicator. The choice of the type of information on display depends on the value of D[7]:

- if D[7] = 0, then the display shows one of the 128 characters of the ASCII-table (address of the symbol is specified by the bus D[6 : 0]). The ASCII DECODER block is responsible for decoding of the symbol;
- if D[7] = 1, then the display shows one of 16 pre-programmed custom characters (address of the symbol is specified by the bus D[3 : 0]). REGISTER OF SYMBOLS AND RAM is used for programming of symbols.

The entry of a character in the memory is performed in eight cycles. At the first stage in REGISTER OF SYMBOLS the value of the external data bus D[7 : 0] is recorded, four low-order digits of which set the address of the RAM section, in which the symbol will be recorded. Each section is a matrix of memory cells (7×5). The second stage involves the line-by-line filling of memory section during seven cycles, while the line number is determined by the external bus A[2 : 0] and the value of the line is specified by the bus D[4 : 0].

Eight-bit REGISTER OF OPERATION MODES is responsible for the implementation of the five modes: the use of the register of blinking, blinking,

дисплеях одновременно. Длительность отображения для каждого из символов составляет 2 с. По окончании тестирования бит D[5] блока "РЕГИСТР РЕЖИМОВ РАБОТЫ" устанавливается в "1", данный бит доступен только для чтения.

При D[7] = 1 запускается функция очистки блоков "8×8 РЕГИСТР ОТОБРАЖАЕМЫХ СИМВОЛОВ" и регистра мигания, а также происходит предустановка всех ячеек памяти блока "РЕГИСТР ОТОБРАЖАЕМЫХ СИМВОЛОВ". После завершения очистки D[7] устанавливается в "0".

Наибольший интерес с точки зрения схемотехнической реализации представляет функция настройки яркости индикатора. В ходе изучения научно-технической литературы было установлено, что основным подходом к реализации данной функции является изменение скважности управляющих светодиодами индикаторов по принципу: чем выше скважность, тем больше яркость. Действительно, степень яркости свечения светодиода определяется его инерционными свойствами и зависит от времени воздействия на него электрического тока.

За регулировку яркости дисплея отвечает значение шины D[2 : 0] в блоке "РЕГИСТР РЕЖИМОВ РАБОТЫ". Зависимость скважности стробирующих сигналов от значения шины D[2 : 0] представлена в табл.3.

Таблица 3. Зависимость скважности стробирующих сигналов от значения шины D[2 : 0]

Table 3. Dependence of gating signal ratio on bus value D[2 : 0]

D2	D1	D0	S %
0	0	0	100
0	0	1	81
0	1	0	63
0	1	1	38
1	0	0	25
1	0	1	13
1	1	0	6
1	1	1	100

В разработанной микросхеме для вывода информации на дисплеи используется стробирование по строкам. За формирование временной диаграммы и управляющих сигналов отвечает "БЛОК УПРАВЛЕНИЯ" (рис.3).

Обработка восьми дисплеев происходит построчно, по группам (с 0 по 3 и с 4 по 7). Шина адресов ADR[2 : 0] последовательно принимает значения от 0 до 7, тем самым производя считывание данных из блока "8×8 РЕГИСТР ОТОБРАЖАЕМЫХ СИМВОЛОВ". При этом на предварительный регистр отправляются строки соответствующего символа (ранее запрограммированного или же одного из ASCII-таблицы). Запись в предварительный регистр отображения осуществляется сигналами WR[3 : 0].

По завершению каждого цикла перебора адресов на шине ADR[2 : 0] изменяется номер

testing, cleanup and adjusting the brightness of the indicator.

The register of blinking is responsible for each of the blinking displays of the indicator. The stored value of the external data bus D[7 : 0] specifies the use (D[n]=1) or not use (D[n] = 0) of the blinking function for n-th display. A signal of permission to use this function is the bit D[3]=1 recorded in the REGISTER OF OPERATION MODES. If D[3] = 0 then the contents of the register of blinking is ignored.

It is possible to force to blink all displays simultaneously without use of functions of the register of blinking. If to set D[4] = 1 in REGISTER OF OPERATION MODES, the global function of blinking is activated, when all eight displays are blinking simultaneously. In this case the contents of register of blinking is ignored. The blinking frequency in both cases is 2 Hz.

If D[6] = 1, then test function starts, which displays the direct and inverse checkerboard pattern on all displays simultaneously. The duration of display for each of the characters is 2 seconds. At the end of the test D[5] of REGISTER OF OPERATION MODES is set to "1", this bit is read-only.

D[7] = 1 activates the cleanup function of 8×8 REGISTER OF DISPLAYED CHARACTERS and register of blinking with preset of all of the memory cells of REGISTER OF DISPLAYED CHARACTERS. After the cleanup is completed, D[7] is set to "0".

From the viewpoint of circuitry implementation, the function of adjusting the brightness of the indicator is of the greatest interest. The study of scientific literature showed that the main approach to the implementation of this function is the

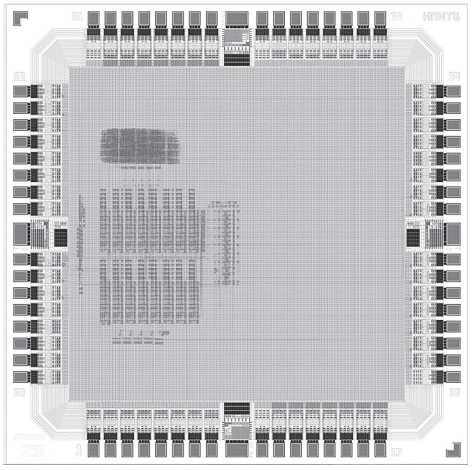


Рис.4. Вид топологии кристалла микросхемы 5521ТР034-726
Fig.4. Topology of 5521TP034-726 circuit

обрабатываемой строки ROW_SET[2 : 0]. Сигналы шины ROW[13 : 0] являются стробами отображаемых данных: ROW[0] – первая строка первой группы символов, ROW[1] – первая строка второй группы символов и т.д. При переходе от ROW[n] к ROW[n+1] вырабатывается сигнал CLK, записывающий данные в выходные регистры из предварительных.

На рис.4 представлена топология кристалла микросхемы 5521ТР034-726. Микросхема 5521ТР034-726 может выпускаться как в отдельных кристаллах, так и в корпусном исполнении (корпус 4239.68-1).

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

ЛИТЕРАТУРА

1. **Васерин Н.Н., Дадерко Н.К., Прокофьев Г.А.** Применение полупроводниковых индикаторов / Под ред. Е.С. Липина. – М.: Энергоатомиздат, 1991. 200 с.
2. HDSP-2133. [Электронный ресурс] / http://www.kontest.ru/datasheet/AVAG0TECHN0L0GIES/HDSP-213x_2179.pdf. Дата обращения 26.09.16.
3. **Коняхин В.В., Денисов А.Н., Федоров Р.А., Вильсон А.Л., Бражников С.С., Коновалов В.С., Малашевич Н.И., Росляков А.С.** Микросхемы для аппаратуры космического назначения : Практическое пособие / Под общ. ред. Саурова А.Н. – М.: ТЕХНОСФЕРА, 2016. 388 с.
4. САПР БИС "Ковчег 3.04" [Электронный ресурс] / http://asic.ru/index.php?option=com_content&view=article&id=10&Itemid=30. Дата обращения 26.09.16.

change in the duty ratio of control indicators on the principle: the higher is the ratio, the more is brightness. Indeed, the degree of brightness of the LED is determined by its inertial properties and depends on the time of action of an electric current.

Bus D[2 : 0] in REGISTER OF OPERATION MODES is responsible for adjusting the brightness of the display. Dependence of gating signal ratio on bus value D[2:0] is presented in table 3.

A row gating is used in the designed chip to output information to the displays. The CONTROL UNIT is responsible for the generation of timing diagram and control signals (Fig.3).

Processing of eight displays is carried out line by line, in groups (from 0 to 3 and from 4 to 7). Address bus ADR[2 : 0] sequentially takes values from 0 to 7 and thereby provides reading the data from 8×8 REGISTER OF DISPLAYED CHARACTERS. At the same time, the provisional register receives the row of corresponding character (previously programmed or from the ASCII table). The entry in the provisional register is implemented by the signals of WR[3 : 0].

At the end of each cycle of the enumeration of addresses, the bus ADR[2 : 0] changes the number of processed row ROW_SET[2 : 0]. The signals of ROW[13 : 0] are the gates of displayed data: ROW[0] is the first row of the first group of symbols, ROW[1] is the first row of the second group of symbols, etc. In case of transition from ROW[n] to ROW[n+1] the CLK signal is generated that records the data from the provisional to the output registers.

Fig.4 shows the topology of the chip of 5521TP034-726 circuit. 5521TP034-726 can be fabricated as a single chip and in package 4239.68-1. ■

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