Обеспечение живучести реконфигурируемой мобильной системы при воздействии электромагнитного излучения высокой мощности

© Рубан И.В. © Чурюмов Г.И. © Токарев В.В. © Ткачев В.Н.
Харьковский национальный университет радиоэлектроники,
Харьков, Украина
ruban_i@ukr.net g.churyumov@ukr.net tokarev.v@ukr.net --tk--@ukr.net

Аннотация

В данной статье представлена реконфигурируемая мобильная система (РМС), состоящая из совокупности объектов, объединенных в единую инфокоммуникационную сеть и нацеленных на комплексное решение задач регистрации, приема, передачи, обработки и временного хранения информации. Топология сети адаптивна и выбирается в зависимости от особенностей решаемой задачи. В качестве объектов РМС выступают беспилотные летательные аппараты (БПЛА), между которыми организованы каналы связи на основе семейства стандарта IEEE 802.11.

Показано, что успех решения задач объектами РМС зависит как от особенностей организации сети, включая ее топологию и архитектуру, так и от внешних факторов естественного (атмосферные осадки, молния и т.п.) и искусственного (воздействие ионизирующего или мощного микроволнового излучения) происхождения. Установлено, что воздействие мощных импульсов электромагнитного излучения оказывает деструктивное действие на полупроводниковую компонентную базу БПЛА. Это приводит к появлению и развитию деградационных процессов в микроструктурных ее элементах и как результат сбоям в работе и нарушению нормальной работы БПЛА. Рассмотрены научные и прикладные вопросы повышения живучести РМС в условиях мощного электромагнитного воздействия. Сделаны выводы в отношении поиска путей повышения живучести как компонентов , так и РМС в целом.

Показано, что представленная РМС может быть использована в различных сферах гражданского (например, сбор информации для оценки и определения последствий чрезвычайных ситуаций, а также в упрощенном варианте концепция «умный дом») и военного применения (проведение разведки, контроля периметра зоны облета и аэрофотосъемки, обеспечения связи и действие в составе артиллерийских комплексов, а также применение радиоэлектронного подавления средств управления и т.п.).

1 Введение

Особую актуальность и практический интерес вызывают исследования в области создания радиоэлектронных систем и средств, генерирующих мощное электромагнитное излучение (ЭМИ) для деструктивного воздействия на полупроводниковую элементную базу. Речь идет о подходах, основанных на новых физических принципах. К исследованиям действий мощного СВЧ-поля в широком частотном диапазоне были причастны в разные годы Нобелевские лауреаты Enrico Fermi и акад. П.Л. Капица [1]. Значительный вклад в развитие теории (нестационарная электродинамика) и практики, в том числе решения метрологических вопросов измерения параметров мощных коротких (сверхкоротких) СВЧ-импульсов были сделаны Dr. C.E. Baum [2].

Так как электромагнитное излучение высокой мощности может привести к выводу из строя радиоэлектронных компонентов реконфигурируемой мобильной системы [3], то актуальной является научно-прикладная задача повышения живучести компонентов и системы в целом путем реконфигурирования программной архитектуры [4-9]. Предполагается, что в этом случае на систему осуществляется воздействие как мощными радиоимпульсами, так и видеоимпульсами (рис. 1). Поэтому для повышения живучести системы в условиях мощного внешнего воздействия необходима перенастройка различных узлов, блоков и изменение функционирование системы в целом.

Анализируя сущность электромагнитного излучения высокой мощности в качестве фактора влияния на реконфигурируемую мобильную систему, важно отметить следующие особенности:

1. Динамика изменения уровня выходной мощности (как средней до десяток-сотен кВт, так и пиковой (импульсной) до единиц МВт).
2. Укорочение длины волны ЭМИ, в частности, за счет новых наработок в освоении миллиметрового и терагерцового диапазонов, а также расширение полосы генерируемых частот и уменьшение длительности импульса

до единиц наносекунд – сотен пикосекунд.

3. Увеличение уровня мощности и укорочение длительности импульса повышает эффективность применения запасенной в импульсе энергии на больших расстояниях.

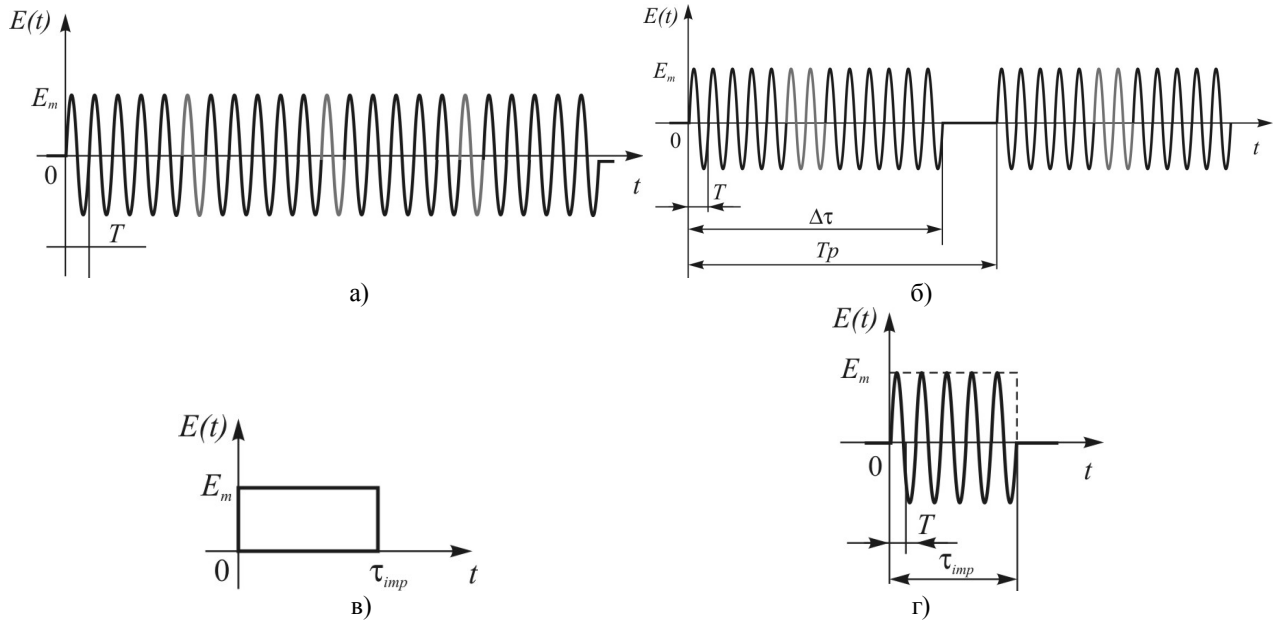

Рис. 1. Осциллограммы идеального непрерывного (а) и импульсных сигналов (б-г)

Целью настоящего доклада является рассмотрение возможных путей защиты реконфигурируемых мобильных систем от воздействия ЭМИ высокой мощности путем программной реконфигурации для повышения их функциональной стойкости.

2 Особенности функционирования реконфигурируемой мобильной системы

Реконфигурируемая мобильная система – это множество компонентов, которые обеспечивают регистрацию, передачу, хранение и обработку различных типов данных, а также находятся в отношениях и связях друг с другом посредством защищенных каналов связи, образуя определённую целостность и единство при выполнении поставленных задач. Такая система характеризуется наличием механизмов реконфигурации, реализуя автоматическую перестройку структуры сети обмена данными внутри системы для максимизации показателей эффективности достижения цели функционирования системы при наличии работоспособных компонентов.

В данной работе рассматривается совокупность таких компонентов: рой БПЛА, главный БПЛА, компонент приема и хранения данных с целью дальнейшей ее обработки (рис. 2). Предполагается, что данные между компонентами рассматриваемой системы (БПЛА – БПЛА, БПЛА – главный БПЛА, главный БПЛА – компонент хранения и обработки данных) передаются через зашифрованные каналы передачи данных.

Тогда, реконфигурируемую мобильную систему можно описать в виде кортежа:

$$S = \{\Psi, X, F\}, \tag{1}$$

где Ψ – совокупность компонентов рассматриваемой системы; X – каналы передачи данных; F – цель системы.

Рассмотрим функции каждого из компонентов системы.

1. Рой БПЛА. Данный компонент представляет собой часть подсистемы «БПЛА – главный БПЛА». Это обосновывается тем, что главный БПЛА выполняет одну из функций – физический транспорт для роя БПЛА. Функциями роя БПЛА являются:

а) регистрация первичных данных согласно поставленной задачи к системе в целом;

б) регистрация электромагнитного излучения высокой мощности;

в) квазимаршрутизация с промежуточным хранением данных при передачи их к главному БПЛА;

г) передача тревожного широковещательного сообщения о электромагнитном излучении высокой мощности с целью обеспечения живучести роя в целом.

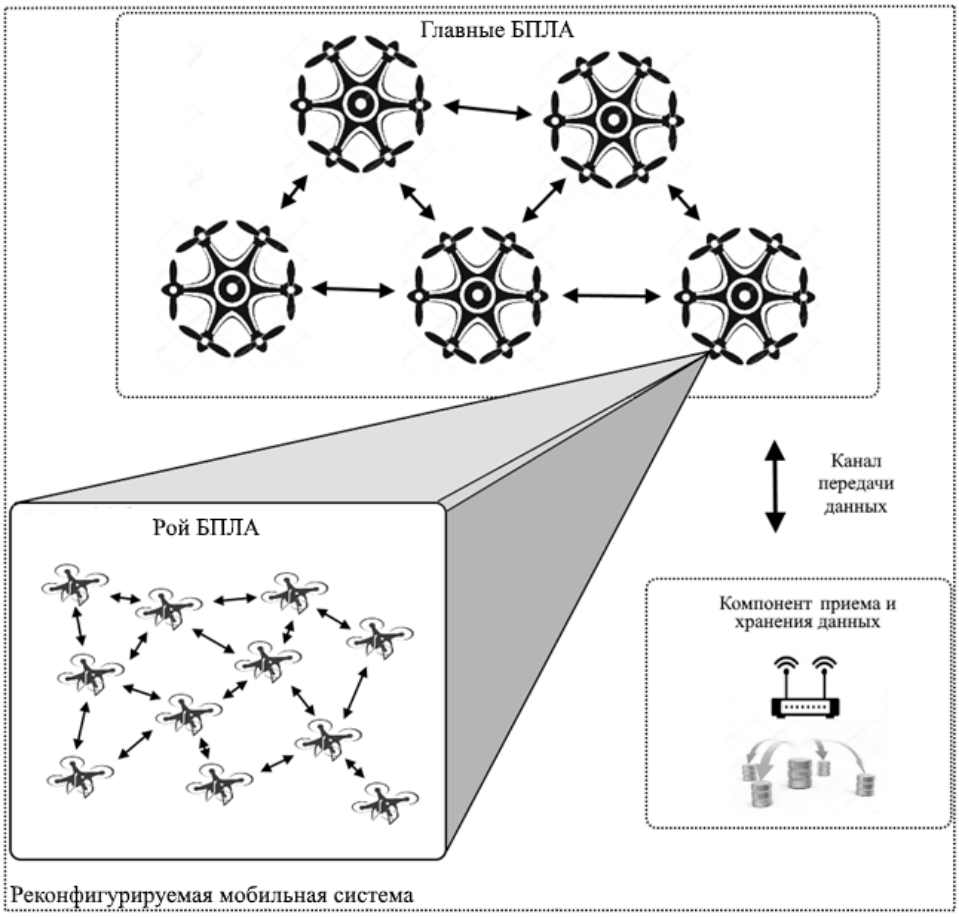

Рис. 2. Реконфигурируемая мобильная система

2. Главный БПЛА можно рассматривать как концентратор данных в отношении роя БПЛА и как систему промежуточного хранения данных в отношении реконфигурируемой мобильной системы. Характеризуется следующими выполняемыми функциями:

а) транспортировка роя БПЛА в заданную точку согласно цели системы;

б) прием и хранение данных от роя БПЛА;

в) ретранслятор команд управления рою БПЛА (при наличии возможности);

г) сбор роя БПЛА после выполнения их задач.

3. Компонент приема и хранения данных рассматривается как стационарный объект системы.

3 Методы повышения живучести реконфигурируемой мобильной системы

Целью средств повышения живучести компонентов реконфигурируемой мобильной системы является обеспечение безопасности данных, хранящихся и обрабатываемых в системе и обеспечение безопасности системы и ее внешней среды при работе с этими данными. Живучесть информационной составляющей реконфигурируемой мобильной системы имеет непосредственное отношение к живучести информационного обеспечения, возможности его восстановления, выполнение им своего функционального назначения при осуществлении мощного электромагнитного воздействия, как на информационное обеспечение, так и на всю систему в целом. Методы и средства обеспечения и повышения живучести информационных компонентов необходимо применять на всех этапах их прохождения в реконфигурируемой мобильной системе.

Для повышения живучести компонентов системы применяются следующие методы:

1. Многократное дублирование данных (реализация избыточности данных). Избыточность вводится искусственно при проектировании систем хранения данных, создании информационных ресурсов с целью повышения надежности системы в условиях работы со сбоями. При этом предполагается регулярное осуществление репликации дублирующих блоков информации с проверкой идентичности.

2. Реализация резервного и архивного копирования данных. Резервное копирование предусматривает создание копии данных в системе хранения данных (основной или резервной). Такое копирование предназначено для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

3. Резервное дублирование целых аппаратно-программных комплексов (БПЛА, главных БПЛА). Так, в реконфигурируемой мобильной системе предусмотрено автоматическое резервное дублирование задающих цель систем. Это позволяет оперативно и в автоматическом режиме переместить все настройки и задачи с отказавшего главного БПЛА, на резервный, который затем принимает на себя функции того, что отказал. Эта функция снижает риск потери системных журналов при отказе компонентов системы.

4. Применение средств хеширования данных (как средство против искажения данных). Наиболее простой способ проверки целостности данных, передаваемых в цифровом представлении, – это метод контрольных сумм. Недостаток этого метода заключается в том, что равенство сравниваемых значений не дает гарантии, что данные остались неизменными. Более совершенный способ цифровой идентификации некоторой последовательности данных – это вычисление контрольного значения ее циклического избыточного кода. Алгоритм контроля CRC уже в течение длительного времени широко используется в системах сетевых адаптеров, контроллеров систем хранения данных и других устройств для проверки идентичности входной и выходной информации. Более высокую надежность, чем при контроле CRC, можно достичь при использовании односторонних алгоритмов хэширования; результатом их работы есть особые значения хеша. Среди односторонних алгоритмов хэширования распространен алгоритм MD5 и алгоритм Secure Hash Algorithm (SHA). Для обеспечения живучести должно осуществляться хранение критических данных в закодированном виде, а их передача осуществляться через зашифрованные канали связи. Таким образом, системы обеспечения живучести информационной составляющей реконфигурируемой мобильной систем должны обеспечивать контроль хешових значений программных модулей.

5. Ограничение доступа к данным. Использование этого метода предполагает наличие развитого периметра безопасности, наличие как централизованного, так и децентрализованного управления, возможность оценивать входные данные, исключать данные опасного содержания. При этом полное ограничение доступа к данным предполагает невозможность получения всех данных подсистемами, для которых явно не установлено соответствующее разрешение. Частичное ограничение доступа к данным предусматривает ограничение доступа на чтение или изменение части свойств данных подсистемам, для которых явно не установлено соответствующее разрешение.

6. Протоколирование событий в системе, ведение системных журналов с целью выявления возможных фрагментов данных, которые подверглись вмешательства. Анализ, контроль и корректировка состояния реконфигурируемой мобильной системы с точки зрения возможного отклонения от штатного режима функционирования по различным направлениям, в том числе по журналам событий, произошедших в системе, протоколами работы программного обеспечения; статистике загрузки каналов связи, загрузки и сбоев аппаратного обеспечения. Следует определить и активизировать имеющиеся в приложениях и операционных системах механизмы протоколирования везде, где это необходимо, а также протоколировать «необходимый минимум» событий.

7. Использование надежных и зашифрованных каналов передачи входных данных. Безопасность должна обеспечиваться шифрованием трафика. Использование нескольких каналов данных должно проходить процедуру сравнения во время занесения в хранилище данных (репликации).

8. Применение систем обнаружения внешнего воздействия (вторжение), с помощью которых можно зафиксировать факт атак на информационную инфраструктуру системы, оценить возможные убытки и выполнить адекватные действия в ответ. При этом внешние воздействия на информационную составляющую сейчас принято считать информационными операциями, соответственно для обеспечения ее живучести необходимо применять методы мониторинга и противодействия информационным операциям.

Следует отметить, что масштабы инфраструктуры, количество информационных процессов и сложность взаимосвязей иногда превышают предел, когда возможно контролировать всю инфраструктуру, видеть взаимосвязи процессов и роль элементов инфраструктуры в каждом процессе. Из-за этого снижается уровень готовности всей реконфигурируемой мобильной системы; качество обслуживания, которое, к тому же, трудно оценивать; при изменениях процессов возникают новые проблемы в инфраструктуре. В этом случае живучесть информационной составляющей реконфигурируемой мобильной системы во многом зависит от организационного обеспечения.

4 Пример обеспечения живучести реконфигурируемой мобильной системы

На практике, например, при обследовании и картографировании больших территорий, возникает задача группового применения технических объектов, которая заключается в том, чтобы обработать данные с территории с минимальным перекрытием областей, которые обрабатываются отдельным техническим объектом группы и с минимальными затратами на перемещение объектов.

Группа представляет собой множество технических объектов, которые выполняют регистрацию, передачу, хранение и обработку данных различных типов, а также взаимодействуют друг с другом через защищенные каналы связи, образуя определенную целостность и единство для достижения общесистемной цели.

Припустим, в среде функционирует группа O з N объектов O_i, которая может обработать некоторую территорию площадью S. Отдельный объект $O_i \in O$ может обработать площадь $S_i = \pi l^2$, где l - радиус области, которую обрабатывает O_i.

Для того, чтобы площадь покрытия, которую обрабатывает группа, была максимальной, необходимо, чтобы величина:

$$R = \sum_{i}^{N} \sum_{i=i+1}^{N} F(T_i, T_j)$$

была минимальной. $T_i \in S$ является точкой, где объект O_i снимает информацию. Это целевая точка объекта $O_i (i = \overline{1, N})$.

Функция $F = (T_i, T_j)$ определяет, как пересекаются зоны обработки *i*-го и *j*-го объектов группы, если объект O_i снимает информацию с точки $T_i \in S$, а объект O_j – с точки $T_j \in S$. Величина R определяет общую площадь сечения зон обработки информации всеми объектами, поэтому, чем меньше будет пересечений между зонами обработки, тем соответственно будет больше общая площадь обработки информации всеми объектами.

При выполнении основной задачи реконфигурируемой мобильной системой в случае идентификации ЭМИ высокой мощности БПЛА проводится оценка необходимости реконфигурации программной архитектуры для обеспечения функциональной стойкости универсальной мобильной реконфигурируемой системы.

Как показано на рис. 3., в случае возникновения вышеописанной ситуации применительно к БПЛА, данные в электромагнитного излучения посредством сети роя БПЛА передаются к главному БПЛА (выделенный маршрут на рис. 3). Главный БПЛА после приема и обработки тревожного широковещательного сообщения принимает решение о реконфигурации программной архитектуры модели поведения роя БПЛА. Например, при загрузке конфигурационного файла с моделью поведения о сборе роя БПЛА, данная команда передается посредством функций квазимаршрутизации в сети роя БПЛА.

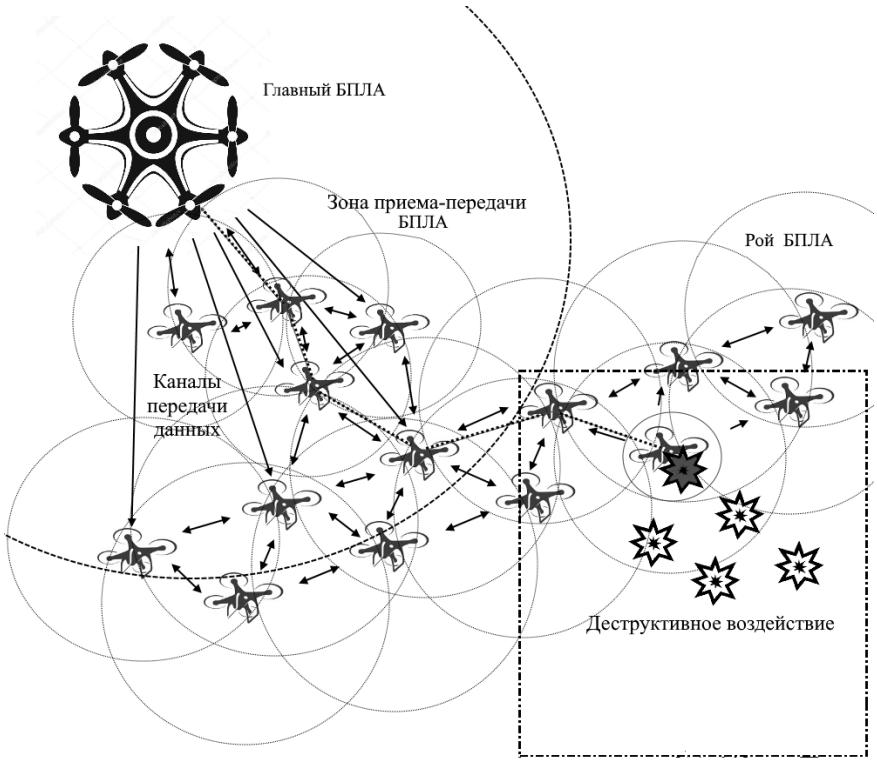

Рис. 3. Пример обеспечения живучести реконфигурируемой мобильной системы

5 Выводы

Проведенный детальный анализ процесса генерации мощного СВЧ излучения показывает, что развитие данного направления проводится в направлении дальнейшего повышения уровня мощности (как непрерывной, так и импульсной), расширение полосы усиливаемых частот, укорочение длины волны и улучшения массогабаритных параметров СВЧ-генераторов.

Показано, что среди возможных направлений применения мощного импульсного СВЧ-излучения есть сферы, которые связаны с военными технологиями, а также с применением мощного СВЧ-излучения в качестве противодействия электромагнитному терроризму. Установлено, что в последнее время особый интерес вызывает появление данных о создании радиоэлектронного ЭМО и его применении в системах РЭБ и РЭП для функционального поражения полупроводниковой элементной базы РЭА и РТС потенциального противника, в том числе компьютерной техники и сетей, активных ФАР РЛС и т.п.

Установлено, что для повышения качества функционирования мобильной РЭС в условиях деструктивных воздействий целесообразно:

а) применить традиционные способы защиты от предполагаемых деструктивных воздействий (СВЧ излучения)

б) разработать и внедрить автоматические средства восстановления работоспособности РЭС за счет средств компенсации;

в) внедрить такие механизмы обеспечения живучести, как реконфигурация, реорганизация, процедуры изменения стратегии управления, механизм постепенного изменения функциональности.

В данной работе заложены научно-методические основы обеспечения живучести реконфигурируемой мобильной системы при воздействии электромагнитного излучения высокой мощности. В дальнейшем предполагается проведение исследований других способов обеспечения живучести подобного класса систем. Спектр возможных сфер применения универсальных систем чрезвычайно широкий, за счет гетерогенности факторов воздействия.

Исследования проводятся в рамках выполнения фундаментальной научно-исследовательской темы «Создание научно-методических основ обеспечения живучести сетевых систем обмена информацией в условиях внешнего воздействия мощного СВЧ-излучения» на базе научно-учебной лаборатории Моделирования систем кафедры Электронных вычислительных машин ХНУРЭ.

Список литературы

1. Капица П.Л. Электроника больших мощностей. – М.: Изд-во АН СССР. 1962. – 195 с.
2. Baum C. E., “Reminiscences of High-Power Electromagnetics”, *IEEE Trans. EMC*, May 2007, pp 211-218.
3. Чурюмов Г.И. СВЧ электроника больших мощностей: современное состояние, перспективы развития и особенности применения. Прикладная радиоэлектроника, т. 15, № 4, 2016, сс. 270-300.
4. Радченко В.А. Мобильная подсистема «Мультикоптер-сенсорная сеть» в компьютерной системе хранения BIG DATA / В.А. Радченко, Д.А. Руденко, В.Н. Ткачев, В.В. Токарев // Системи управління, навігації та зв’язку. – Полтава. – 2017. - №4(44). – С. 102-105.
5. Радченко В.А. Проблема передачі даних типу BIG DATA у мобільній системі «Мультикоптер–сенсорна мережа» / В.А. Радченко, В.О. Лебедев, В.Н. Ткачев, В.В. Токарев // Системи управління, навігації та зв’язку. – Полтава – 2017. – №2 (42). – С.154-157.
6. Tkachov V. Method for transfer of data with intermediate storage / V. Tkachov, V. Savanevych // Problems of Infocommunications Science and Technology, 2014 First International Scientific-Practical Conference. – 14-17 Oct. 2014, Kharkiv. – 2 p. DOI: 10.1109/INFOCOMMST.2014.6992315.
7. Mukhin V., Loutskii H., Barabash O., Kornaga Ya and Steshyn V. (2015), Models for Analysisand Prognosticationof the Indicatorsof the Distributed Computer Systems Characteristics //International Reviewon Computers and Software (IRECOS), Vol. 10, N 12, pp. 1216 – 1224.
8. Mukhin V. et al. The Method of Variant Synthesis of Information and Communication Network Structures on the Basis of the Graph and Set-Theoretical Models //International Journal of Intelligent Systems and Applications. – 2017. – Т. 9. – №. 11. – С. 42.
9. Filimonchuk T. et al. Development of information technology of tasks distribution for grid-systems using the grass simulation environment // Восточно-Европейский журнал передовых технологий. – 2016. – №. 3 (9). – С. 45-53.

Provision of Survivability of Reconfigurable Mobile System on Exposure to High-Power Electromagnetic Radiation

© Igor V. Ruban © Genadiy I. Churyumov © Volodymyr V. Tokarev © Vitaliy M. Tkachov
Kharkiv National University of Radio Electronics,
Kharkiv, Ukraine
ruban_i@ukr.net g.churyumov@ukr.net tokarev.v@ukr.net --tk--@ukr.net

Abstract

This paper presents a reconfigurable mobile systems (RMS) consisting of the objects that are combined in single info communication network and purposed to the complete solution of problems of a registration, reception, transmission, processing and temporary storage of information. A topology of network is adaptive and is chose as required by application. As the objects of the PMS one consider the vehicles (drones) between of which there are the channels of communication organized on basis of the IEEE 802.11 standard.

It has been shown that successful solutions of the tasks by the RMS objects depends of the features of organization of the network including its topology and architecture as well as from influence of outside factors both natural (for example, atmospheric precipitations, lightning, and etc.) and artificial (for example, exposure of ionization or high-power microwave radiation). It has been found that impacting the high-power microwave pulses has a destructive effect to the semiconductor components of the drones. The scientific and technology issues of raising the survivability of the drones in conditions of acting the high-power microwave radiation have been considered. The conclusions as to search of the ways for raising the survivability not only the components of the drones but the PMS system in total are done.

It has been shown that the PMS may be used in the different spheres of activity both for the civil (for example, collection of information for assessing and determining the consequences of emergencies, as well as in its simplified version as the concept of "smart home") and for the military applications (reconnaissance, perimeter monitoring of the overflight area and aerial photography, communication and operation as part of artillery systems, as well as the use of electronic suppression of various control systems, etc.).