УДК 621.396; 519.718
doi: 10.21685/2307-4205-2025-1-6

ОПРЕДЕЛЕНИЕ НАДЕЖНОСТИ СИСТЕМЫ РАСПОЗНАВАНИЯ ОБЪЕКТОВ С ИСПОЛЬЗОВАНИЕМ ГИБРИДНОЙ ИДЕНТИФИКАЦИИ

И. С. Галишников[1], Д. А. Аминев[2], Л. В. Бунина[3], Д. В. Козырев[4]

[1] Московский государственный технический университет имени Н. Э. Баумана, Москва, Россия
[2, 3] МИРЭА – Российский технологический университет, Москва, Россия
[4] Институт проблем управления имени В. А. Трапезникова РАН, Москва, Россия
[4] Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия
[1] galishnikov.ilya@yandex.ru, [2] aminev.d.a@ya.ru, [3] ludmilabunina@mail.ru, [4] kozyrev-dv@rudn.ru

Аннотация. *Актуальность и цели.* Рассмотрен принцип распознавания объектов с использованием радиочастотной и оптической идентификации. *Материалы и методы.* Раскрыт состав системы гибридной идентификации, основными компонентами которой являются RFID-метки, RFID-считыватели, антенны, устройство фото- и видеофиксации, модуль сопряжения для передачи в центр обработки данных через телекоммуникационную сеть. Раскрыта структурная и электрическая монтажная электрические схемы системы гибридной идентификации. *Результаты и выводы.* Предложена методика расчета надежности системы и на основе данных эксплуатационной интенсивности отказов проведен расчет вероятности безотказной работы. Выявлены самые ненадежные элементы и выработаны рекомендации по повышению надежности посредством горячего резервирования микроконтроллеров. Предложены структурная схема надежности с учетом резервирования и обобщенный алгоритм работы системы распознавания объектов с использованием радиочастотной и оптической идентификации с учетом переключения основного и резервного микроконтроллеров во времени.

Ключевые слова: радиочастотный считыватель, микроконтроллер, идентификация, эксплуатационная интенсивность отказов, вероятность безотказной работы, резервирование

Финансирование: публикация выполнена при поддержке Программы стратегического академического лидерства РУДН (получатель Д. В. Козырев, разработка математической модели).

Для цитирования: Галишников И. С., Аминев Д. А., Бунина Л. В., Козырев Д. В. Определение надежности системы распознавания объектов с использованием гибридной идентификации // Надежность и качество сложных систем. 2025. № 1. С. 44–53. doi: 10.21685/2307-4205-2025-1-6

DETERMINING THE RELIABILITY OF AN OBJECT RECOGNITION SYSTEM USING HYBRID IDENTIFICATION

I.S. Galishnikov[1], D.A. Aminev[2], L.V. Bunina[3], D.V. Kozyrev[4]

[1] Bauman Moscow State Technical University, Moscow, Russia
[2, 3] MIREA – Russian Technological University, Moscow, Russia
[4] V.A. Trapeznikov Institute of Management Problems of the Russian Academy of Sciences, Moscow, Russia
[4] Patrice Lumumba Peoples' Friendship University of Russia, Moscow, Russia
[1] galishnikov.ilya@yandex.ru, [2] aminev.d.a@ya.ru, [3] ludmilabunina@mail.ru, [4] kozyrev-dv@rudn.ru

Abstract. *Background.* The article considers the principle of object recognition using radio frequency and optical identification. *Materials and methods.* The composition of the hybrid identification system is disclosed, the main components of which are RFID tags, RFID readers, antennas, a photo and video recording device, an interface module for transmitting to the data processing center via a telecommunications network. The structural and electrical installation electrical circuits of the hybrid identification system are disclosed. *Results and conclusions.* A method for calculating the reliability of the system is proposed and, based on the operational failure rate data, the probability of failure-free operation is calculated. The most unreliable elements are identified and recommendations are developed for increasing reliability by hot standby of microcontrollers. A structural diagram of reliability taking into account the redundancy and a generalized algorithm for the operation of the object recognition system using radio frequency and optical identification are proposed taking into account the switching of the main and backup microcontrollers in time.

Keywords: radio frequency reader, microcontroller, identification, operational failure rate, probability of failure-free operation, redundancy

© Галишников И. С., Аминев Д. А., Бунина Л. В., Козырев Д. В., 2025. Контент доступен по лицензии Creative Commons Attribution 4.0 License / This work is licensed under a Creative Commons Attribution 4.0 License.

Financing: the publication was supported by the RUDN University Strategic Academic Leadership Program (recipient D. V. Kozyrev, mathematical model development).

For citation: Galishnikov I.S., Aminev D.A., Bunina L.V., Kozyrev D.V. Determining the reliability of an object recognition system using hybrid identification. *Nadezhnost' i kachestvo slozhnykh sistem = Reliability and quality of complex systems.* 2025;(1): 44–53. (In Russ.). doi: 10.21685/2307-4205-2025-1-6

Введение

Система радиочастотной и оптической идентификации объекта предназначена преимущественно для определения движущихся транспортных средств и передачи сведений о них в центр обработки данных в режиме реального времени. Структурная схема такой системы представлена на рис. 1[1] [1–3].

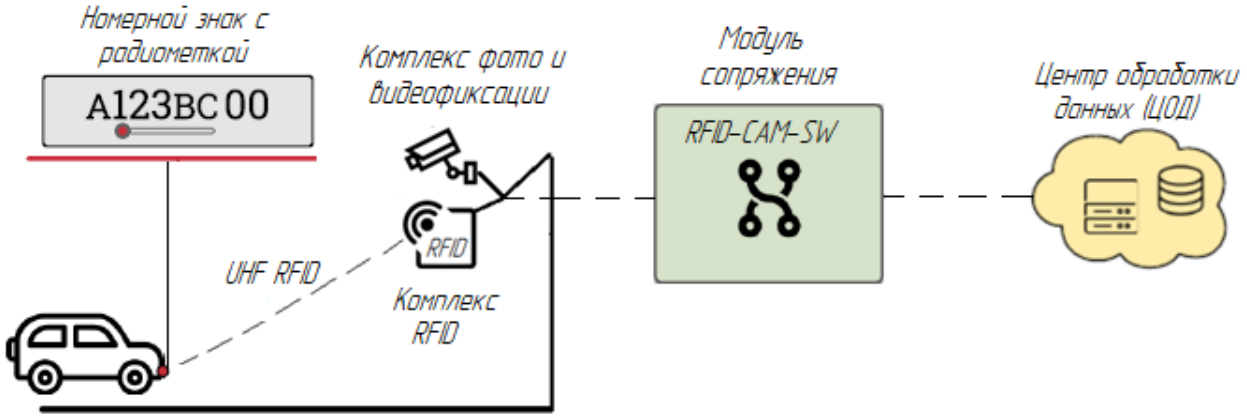

Рис. 1. Структурная схема системы гибридной идентификации

Основными компонентами такой системы являются RFID-метки, RFID-считыватели, антенны, устройство фото- и видеофиксации, телекоммуникационная сеть, модуль сопряжения и центр обработки данных. RFID-метки или транспондеры – это устройства, которыми оснащаются движущиеся объекты. Их назначение – передача записанного идентификатора считывателям. В данной системе применяются пассивные метки, без источника питания. RFID-считыватели – активные устройства, осуществляющие чтение идентификаторов меток и их передачу в центр обработки данных. Устройство фото- и видеофиксации передает в центр обработки данных фотографию движущегося объекта. Телекоммуникационная сеть используется для передачи данных о метках от считывателей в центр обработки данных, а также для доступа к считывателям для их настройки, обслуживания и мониторинга. Центр обработки данных включает информационную систему, в которой собираются данные о прочитанных метках и состоянии работы считывателей. Для взаимодействия комплекса RFID и комплекса фото- и видеофиксации используется модуль сопряжения. Он соединяет зоны контроля антенн RFID и зоны контроля комплекса видеофиксации, совмещает данные от камеры и RFID, а также взаимодействует с базой данных.

Поскольку данная гибридная система впоследствии будет применяться массово и устанавливаться в местах движения транспортных средств с целью выявления нарушений правил дорожного движения, важнейшей задачей является обеспечение ее надежной работы. Для этого необходимо сначала сформулировать исходные данные для расчета надежности, затем провести расчет показателей надежности по выбранной методике и выработать рекомендации по повышению этих показателей.

Исходные данные для расчета надежности

Исходными данными являются функциональная схема системы, схема электрическая монтажная, интенсивности отказов компонентов. На рис. 2 представлена функциональная схема системы распознавания объектов с использованием радиочастотной и оптической идентификации [4, 5]. На данной схеме показано, каким образом идентифицируется транспортное средство. RFID-считыватель

[1] Об утверждении Стратегии безопасности дорожного движения в Российской Федерации на 2018–2024 годы : распоряжение Правительства Российской Федерации № 1-р. от 8 января 2018 г.

через антенны усиления создает электромагнитное поле (ЭМП). Когда метка попадает в зону ЭМП считывателя, на нее попадает высокочастотный сигнал – несущая, в простом случае это синусоида. Метка меняет коэффициент отражения сигнала, тем самым модулирует несущую. Считыватель получает значительно ослабленный, но некий информационный сигнал, и тем самым пытается извлечь из этого сигнала информацию, которую ему хочет сообщить метка. Как правило, метка сообщает свой идентификатор. Затем информация об идентификаторе метки через сетевой интерфейс микроконтроллера передается на модуль сопряжения. Параллельно с этим информацию об оптически распознанном номере транспортного средства передает на модуль сопряжения и комплекс фото- и видеофиксации семейства «Кордон» [5]. Модуль сопряжения проводит сравнение, ранжирование списков полученных номеров и передает полученную информацию в центр автоматической фиксации административных правонарушений.

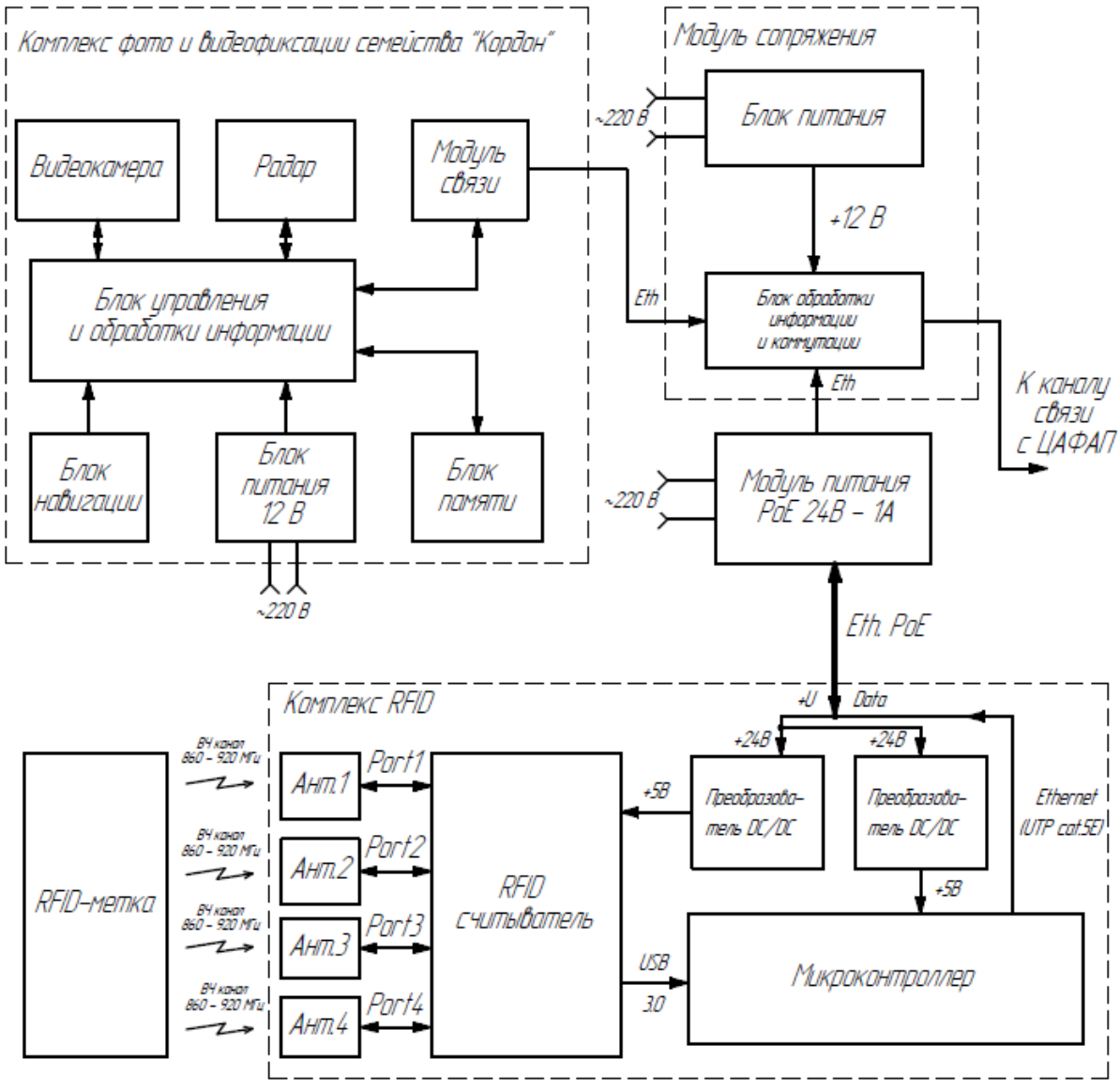

Рис. 2. Функциональная схема системы распознавания объектов
с использованием радиочастотной и оптической идентификации

На рис. 3 представлена схема электрическая монтажная. Схема подключения системы распознавания объектов с использованием радиочастотной и оптической идентификации состоит из следующих компонентов: A1–A4 – антенна RFID (8 дБи, 860–870 МГц); A5 – модуль питания PoE (24 В); A6 – RFID-считыватель (ThingMagic M6e); A7 – блок питания ~220 В / 12 В; A8, A9 – DC/DC-преобразователь 24 В / 5 В; A10 – одноплатный компьютер NanoPi Neo4; A11 – комплекс фото- и видеофиксации семейства «Кордон»; A12 – модуль сопряжения.

Антенны усиления подключаются к RFID-считывателю с помощью коаксиального кабеля, сам считыватель питается от постоянного напряжения 5 В, которое он получает от преобразователя напряжения 24 В / 5 В так же, как и одноплатный компьютер получает 5 В постоянного напряжения от второго DC/DC-преобразователя. Считыватель подключен к одноплатному компьютеру по интерфейсу USB 3.0. Подключение к модулю сопряжения комплекса семейства «Кордон», а также комплекса RFID осуществляется с помощью кабелей Ethernet к соответствующим разъемам RJ-45 модуля сопряжения.

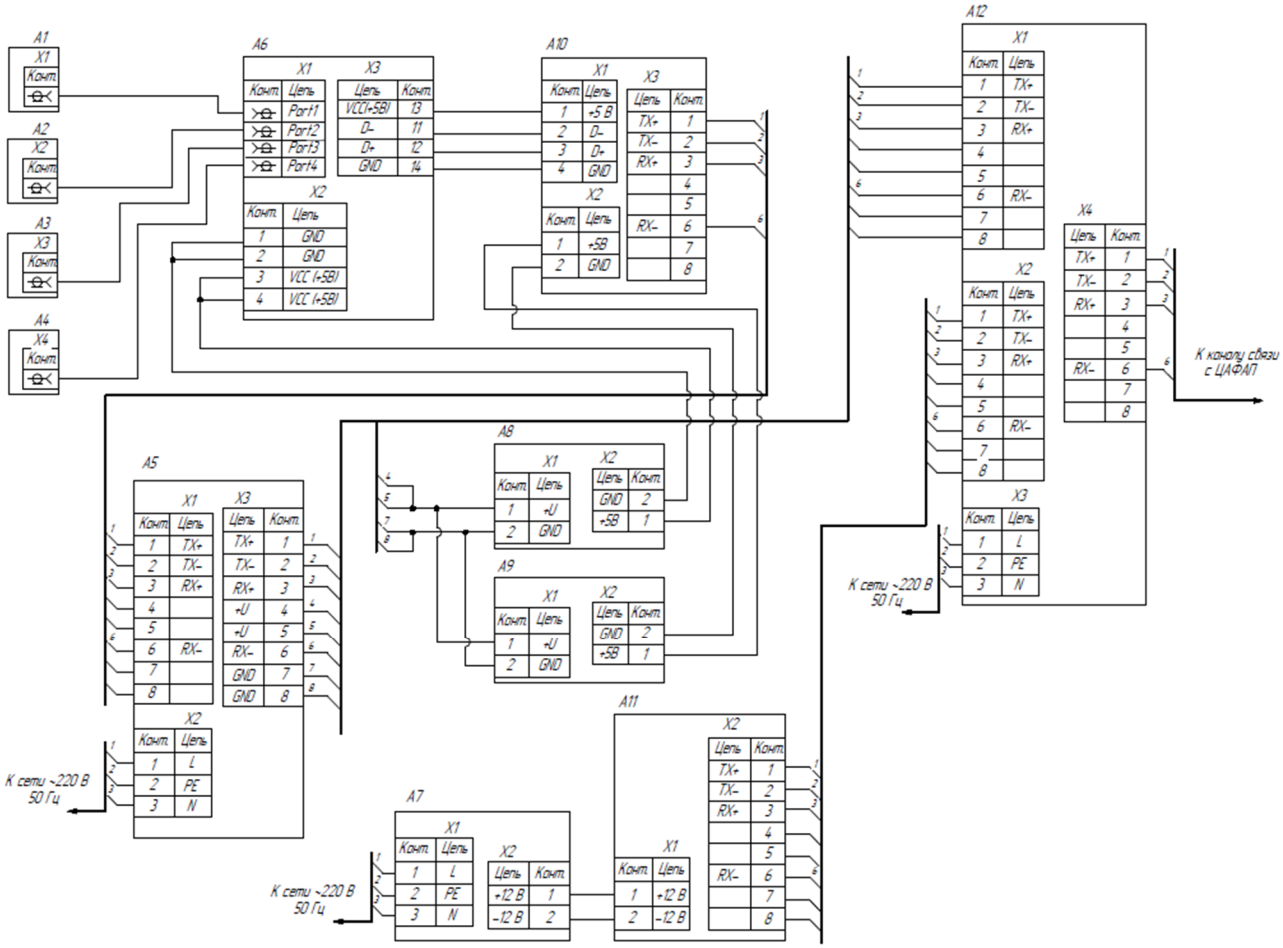

Рис. 3. Схема электрическая монтажная

В табл. 1 представлены интенсивности отказов компонентов системы, полученные на основании экспертных оценок.

Таблица 1

Интенсивности отказов компонентов системы гибридной идентификации

Элемент	Интенсивность отказов, $\lambda \cdot 10^{-5}$ ч$^{-1}$	Количество элементов, используемых в устройстве
Комплекс фото- и видеофиксации семейства «Кордон»	0,28	1
Модуль питания PoE	0,01	2
Сетевой кабель	0,06	9
Проходной адаптер	0,05	4
AC/DC-преобразователь	0,07	1
DC/DC-преобразователь	0,03	2
Блок обработки информации и коммутации	0,15	1
Одноплатный компьютер	0,20	1
RFID-считыватель	0,24	1
Антенна RFID	0,07	4
Коаксиальный кабель	0,08	4

Выбор методики и расчет надежности системы гибридной идентификации

Обозначим через T_i ,$i=\overline{1,N}$ случайные величины (с.в.), определяющие длительности безотказной работы компонентов A1–AN системы гибридной идентификации, и через $T_{\text{сис}}$ – с.в., определяющую время безотказной работы всей системы.

Расчет характеристик надежности проводится с учетом следующих допущений:

– отказ любого из компонентов приводит к выходу из строя всей системы;

– отказы компонентов являются независимыми случайными событиями.

В силу сделанных предположений очевидно, что время работы всей системы $T_{\text{сис}}$ равно минимальной из длительностей работы ее компонентов T_i:

$$T_{\text{сис}} = \min\{T_1, \ldots, T_N\}.$$

Предположим, что с.в. T_i распределены по закону Гнеденко – Вейбулла с параметрами (λ_i, α), т.е. их вероятности безотказной работы равны $e^{-\lambda_i t^\alpha}$ при $t \ge 0$. Этот закон распределения является одним из наиболее важных и популярных в теории надежности, так как он выступает в качестве предельного распределения для максимумов (и минимумов) последовательности независимых и одинаково распределенных с.в. Для расчета характеристик надежности рассматриваемой системы докажем следующее вспомогательное утверждение.

Утверждение 1. Если независимые с.в. T_i распределены по двухпараметрическому закону Гнеденко – Вейбулла с параметрами (λ_i, α), тогда с.в. $T_{\text{сис}}$ также имеет распределение Гнеденко – Вейбулла с параметрами (λ, α), где $\lambda = \sum_{i=1}^{N} \lambda_i$.

Доказательство.

$$\boldsymbol{P}\{T_{\text{сис}} \le t\} = \boldsymbol{P}\{\min T_i \le t\} = 1 - \boldsymbol{P}\{\min T_i > t\} = 1 - \prod_{1 \le i \le N} \boldsymbol{P}\{T_i > t\} =$$

$$= 1 - \prod_{1 \le i \le N} \left(1 - \boldsymbol{P}\{T_i \le t\}\right) = 1 - \prod_{1 \le i \le N} \exp\{-\lambda_i t^\alpha\} = 1 - \exp\left\{-t^\alpha \sum\nolimits_{i=1}^{N} \lambda_i\right\} = 1 - e^{-\lambda t^\alpha}.$$

Таким образом, вероятность безотказной работы системы равна

$$P_{\text{сис}}(t) = \exp\left\{-\int_0^t \sum_{i=1}^{N} \lambda_i(x)\,dx\right\} = e^{-\lambda t^\alpha}, \tag{1}$$

где $\lambda_i(t) = \alpha \lambda_i t^{\alpha-1}$ при $t \ge 0$ – опасность отказа.

Поскольку в качестве исходных данных для расчета характеристик надежности известны интенсивности отказов компонентов системы (табл. 1), то численные расчеты проводились для показательного закона надежности, т.е. при $\alpha = 1$.

В этом случае вероятность безотказной работы системы $P_{\text{сис}}(t)$, состоящей из N компонентов, вычисляется по формуле [6–8]

$$P_{\text{сис}}(t) = \prod_{i=1}^{N} P_i(t) = e^{-\sum_{i=1}^{N} \lambda_i t}, \tag{2}$$

где $P_i(t)$ – вероятность безотказной работы i-го компонента; λ_i – интенсивность отказов i-го компонента, ч$^{-1}$; t – время работы, ч.

Среднее время наработки на отказ системы $T_{\text{ср}}$, состоящей из N компонентов, вычисляется по формуле

$$T_{\text{ср}} = \frac{1}{\lambda} = \frac{1}{\sum_{i=1}^{N} \lambda_i}, \tag{3}$$

где λ – интенсивность отказов системы, ч$^{-1}$; λ_i – интенсивность отказов i-го компонента, ч$^{-1}$.

Для рассматриваемой системы $N = 12$, и согласно табл. 1 интенсивность отказов системы равна

$$\lambda = (0,28 + 0,1 \cdot 2 + 0,06 \cdot 9 + 0,06 \cdot 4 + 0,07 + 0,03 \cdot 2 + \\ + 0,15 + 0,2 + 0,24 + 0,07 \cdot 4 + 0,08 \cdot 4) \cdot 10^{-5} = 2,54 \cdot 10^{-5} \text{ ч}^{-1}.$$

Вероятность безотказной работы схемы за 5000 ч равна

$$P_{\text{сис}}(t) = \exp\left(-2,54 \cdot 10^{-5} \cdot 5000\right) = 0,88.$$

Среднее время наработки системы на отказ равно

$$T_{\text{ср}} = \frac{1}{2,54 \cdot 10^{-5}} = 3,97 \cdot 10^{4} \text{ ч}.$$

Вероятность безотказной работы системы за 5000 ч получилась меньше требуемой, а среднее время наработки на отказ практически достигает значения из технического задания. Из чего можно сделать вывод, что система нуждается в повышении надежности.

Рекомендации по повышению надежности системы

Эксперименты на контроллерах ODROID U3+, ODROID C4, NanoPi Neo3, Raspberry Pi, ODROID U, Beaglebone Black rev C показали, что все они выходят из строя при высоких нагрузках системы, ведь в таких комплексах RFID контроллеры подвергаются интенсивной работе, обрабатывая большое количество данных с RFID-считывателей. Это может привести к перегреву и износу компонентов контроллера, что в конечном итоге может привести к выходу из строя. Также стоит обратить внимание, что вышеуказанные контроллеры не имеют встроенной поддержки резервирования. Это означает, что в случае выхода из строя основного контроллера система может полностью перестать функционировать. Структурная схема надежности с учетом использования резервирования микроконтроллеров представлена на рис. 4.

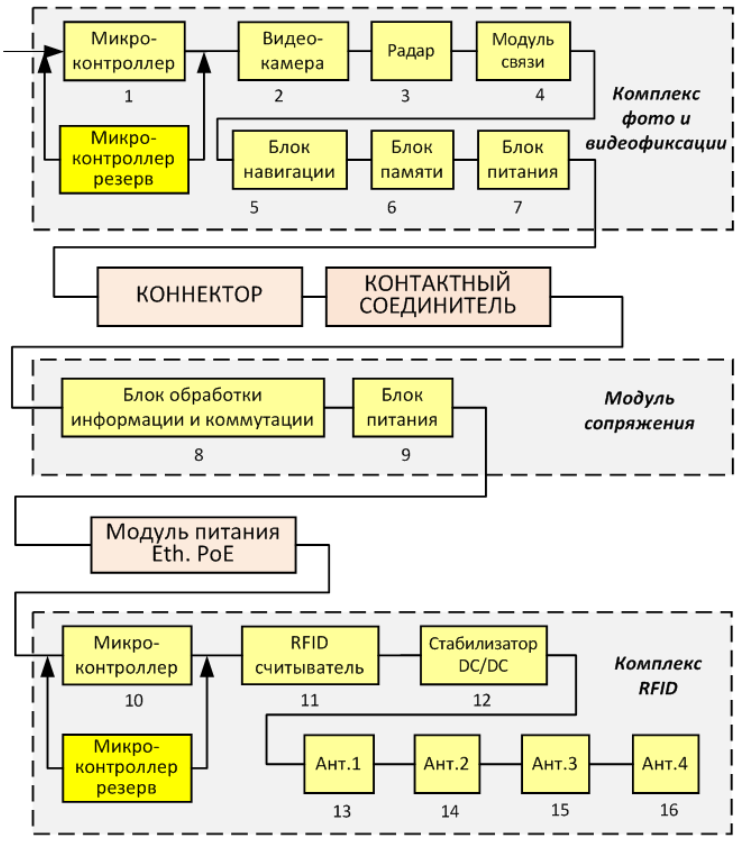

Рис. 4. Структурная схема надежности системы гибридной идентификации с резервированием микроконтроллеров

На рис. 5 представлен алгоритм работы системы распознавания объектов с использованием радиочастотной и оптической идентификации с резервированием микроконтроллеров (красной рамкой отмечены блоки, отвечающие за резервирование).

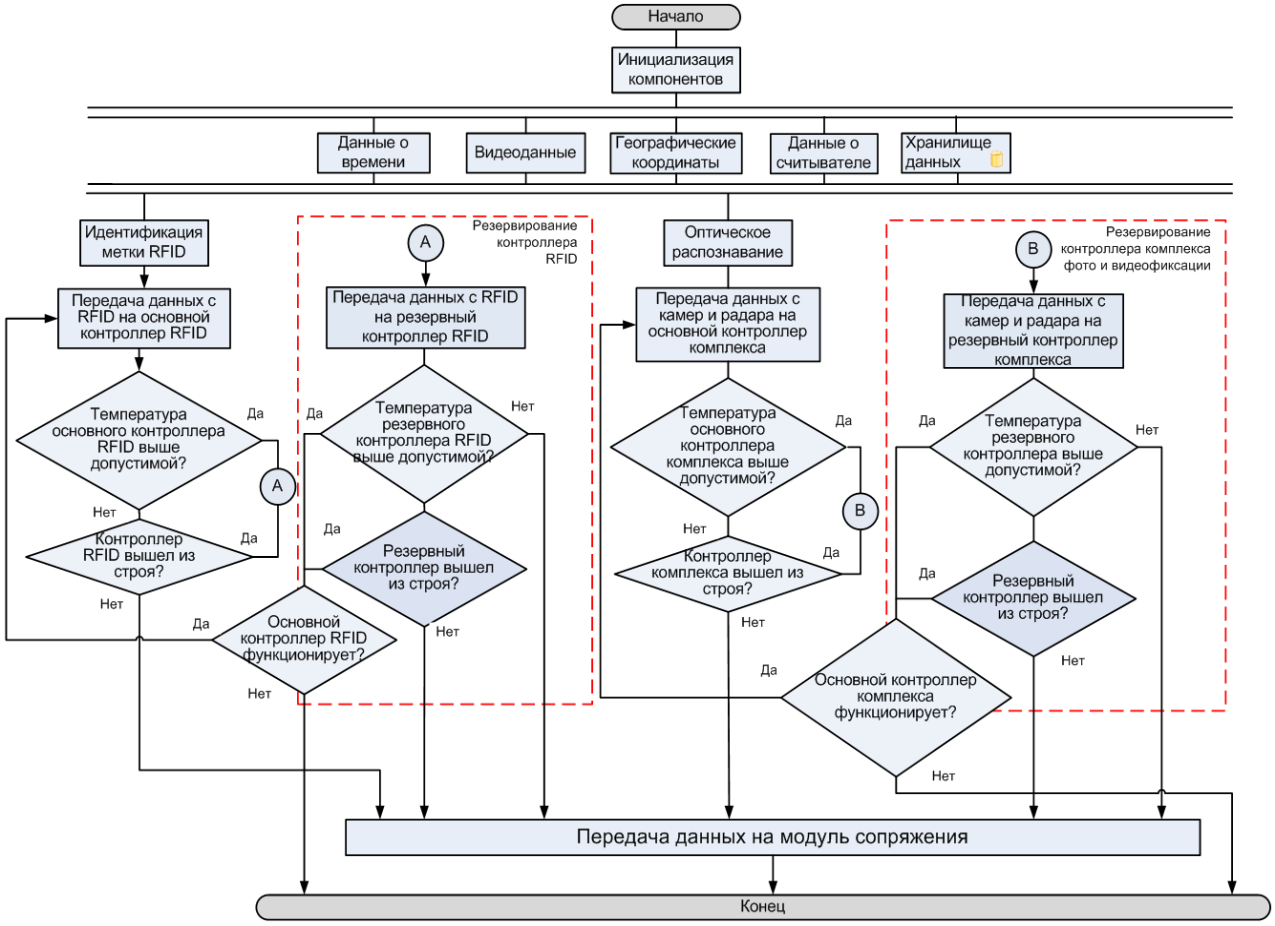

Рис. 5. Алгоритм работы системы распознавания объектов с использованием радиочастотной и оптической идентификации с резервированием микроконтроллеров

Для повышения надежности системы в комплексах RFID рекомендуется использовать резервирование современных контроллеров, таких как NanoPi Neo4. Это позволяет использовать дуэт контроллеров, которые могут автоматически вступать в работу в случае выхода из строя основного контроллера. Такой подход обеспечивает минимальные простои и повышает устойчивость системы к сбоям и выходу из строя контроллеров. Ориентировочный расчет такой системы показал, что вероятность безотказной работы с резервированием микроконтроллера составит 0,98, что является хорошим показателем надежности системы.

После инициализации компонентов параллельно начинаются циклы идентификации метки и оптического распознавания объекта, которые осуществляются непрерывно. Все полученные данные передаются в хранилище, в котором находится информация о прочитанных метках, оптически распознанных объектах, а также база розыскных транспортных средств. Передача информации о прочитанных считывателем метках поступает на основной контроллер одноплатного компьютера, подключенного к RFID-считывателю. Далее осуществляется проверка работоспособности основного контроллера. Если он не вышел из строя и его температура не превышает допустимую предельную температуру, то информация о прочитанных метках поступает на модуль сопряжения. Если же описанные выше условия выполняются, то происходит переключение на резервный контроллер RFID. В случае работоспособности резервного контроллера данные о прочитанных метках также передаются на модуль сопряжения. Если резервный контроллер вышел из строя или его температура превышает максимальную допустимую предельную, проверяется возможность переключения на основной контроллер. Если основной контроллер доступен и функционирует, происходит переключение на него, и данные о прочитанных метках вновь передаются на модуль сопряжения через основной

контроллер, если нет и оба контроллера не работоспособны, то происходит завершение распознавания до устранения причин отказа контроллеров. Использование резервирования контроллера комплекса фото- и видеофиксации, а также передача оптически распознанных объектов функционально осуществляется схожим образом.

После передачи данных с комплекса RFID и оптически распознанных объектов комплексом фото- и видеофиксации на модуль сопряжения происходит сравнение, проверка соответствия и ранжирование списков номерных знаков транспортных. Осуществляется проверка по базе данных розыскных транспортных средств, формирование изображений, журнала XML, цифровой подписи. В итоге сформированные данные направляются в центр автоматической фиксации административных правонарушений [9, 10].

Заключение

Построенная по принципу распознавания объектов с использованием радиочастотной и оптической идентификации гибридная система имеет в составе RFID-метки, RFID-считыватели, антенны, устройство фото- и видеофиксации, модуль сопряжения для передачи в центр обработки данных через телекоммуникационную сеть.

Расчет вероятности безотказной работы по выбранной методике на основе данных эксплуатационной интенсивности отказов позволил выявить, что самыми ненадежными элементами являются микроконтроллеры в составе комплексов RFID и фото- и видеофиксации.

Созданная на основе структурной и электрической монтажной схем структурная схема надежности системы гибридной идентификации, согласно выработанным рекомендациям по резервированию, реализует горячее резервирование микроконтроллеров, и вероятность ее безотказной работы составляет 0,98. Предложенный в рекомендациях энергоэффективный алгоритм обеспечивает переключение основного и резервного микроконтроллеров во времени таким образом, что не влияет на конечный результат идентификации объекта.

Список литературы

1. Larionov A. A., Ivanov R. E., Vishnevsky V. M. A stochastic model for the analysis of session and power switching effects on the performance of UHF RFID system with mobile tags // Procedings of the IEEE International Conference on RFID (Orlando, 2018). Orlando, USA, 2018. P. 1–8.
2. Larionov A. A., Ivanov R. E., Vishnevsky V. M. UHF RFID in Automatic Vehicle Identification: Analysis and Simulation // IEEE Journal of Radio Frequency Identification. 2017. Vol. 1, iss. 1. P. 3–12.
3. Пат. RU 2760058 C1. Способ автоматического контроля дорожного движения и система, его реализующая / Барский И. В., Бондарь Д. В. № 2021118625 ; заявл. 25.06.2021 ; опубл. 22.11.2021.
4. Пат. RU 99207 U1. Автоматизированная система контроля нарушений ПДД на базе широкополосных беспроводных сетей передачи информации и RFID технологии / Вишневский В. М., Манниханов Р. Н. № 2010129975/08 ; заявл. 20.07.2010 ; опубл. 10.11.2010.
5. Свидетельство об утверждении типа средств измерений RU.C.28.002.A № 58736 Федерального агентства по техническому регулированию и метрологии России на комплексы измерительные с видеофиксацией «КОРДОН-М».
6. Aminev D. A., Zhurkov A. P., Polesskiy S. N. [et al.]. Comparative analysis of reliability prediction models for a distributed radio direction finding telecommunication system // Communications in Computer and Information Science (CCIS). 2016. Vol. 678. P. 194–209. doi: 10.1007/978-3-319-51917-3 18
7. Rykov V. V., Kozyrev D. V. Reliability model for hierarchical systems: Regenerative approach // Automation and Remote Control. 2010. Vol. 71, № 7. P. 1325–1336. doi: 10.1134/S0005117910070064
8. Rykov V. V., Kozyrev D. V. Analysis of renewable reliability systems by Markovization method // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. Vol. 10684. P. 210–220. doi: 10.1007/978-3-319-71504-9-19
9. Данилин М. Е., Заяра А. В., Федулов В. Д. Предложения по организации виртуальных испытаний алгоритмов распознавания объектов в системах управления мобильных робототехнических комплексов // Надежность и качество сложных систем. 2023. № 3. С. 100–106.
10. Кошелев Н. Д., Алхатем А., Новиков К. С. [и др.]. Управление искусственных нейронных сетей распознавания раскадровки образов высокого разрешения // Надежность и качество сложных систем. 2022. № 2. С. 85–91.

References

1. Larionov A.A., Ivanov R.E., Vishnevsky V.M. A stochastic model for the analysis of session and power switching effects on the performance of UHF RFID system with mobile tags. *Procedings of the IEEE International Conference on RFID (Orlando, 2018)*. Orlando, USA, 2018:1–8.
2. Larionov A.A., Ivanov R.E., Vishnevsky V.M. UHF RFID in Automatic Vehicle Identification: Analysis and Simulation. *IEEE Journal of Radio Frequency Identification*. 2017;1(1):3–12.
3. Patent RU 2760058 C1. *Sposob avtomaticheskogo kontrolya dorozhnogo dvizheniya i sistema, ego realizuyushchaya = A method of automatic traffic control and a system that implements it*. Barskiy I.V., Bondar' D.V. № 2021118625; appl. 25.06.2021; publ. 22.11.2021. (In Russ.)
4. Patent RU 99207 U1. *Avtomatizirovannaya sistema kontrolya narusheniy PDD na baze shirokopolosnykh besprovodnykh setey peredachi informatsii i RFID tekhnologii = Automated traffic violations control system based on broadband wireless information transmission networks and RFID technology*. Vishnevskiy V.M., Mannikhanov R.N. № 2010129975/08; appl. 20.07.2010; publ. 10.11.2010. (In Russ.)
5. Certificate of type approval of measuring instruments RU.C.28.002.A No. 58736 of the Federal Agency for Technical Regulation and Metrology of Russia for measuring systems with video recording "KORDON-M". (In Russ.)
6. Aminev D.A., Zhurkov A.P., Polesskiy S.N. et al. Comparative analysis of reliability prediction models for a distributed radio direction finding telecommunication system. *Communications in Computer and Information Science (CCIS)*. 2016;678:194–209. doi: 10.1007/978-3-319-51917-3 18
7. Rykov V.V., Kozyrev D.V. Reliability model for hierarchical systems: Regenerative approach. *Automation and Remote Control*. 2010;71(7):1325–1336. doi: 10.1134/S0005117910070064
8. Rykov V.V., Kozyrev D.V. Analysis of renewable reliability systems by Markovization method. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2017;10684:210–220. doi: 10.1007/978-3-319-71504-9-19
9. Danilin M.E., Zayara A.V., Fedulov V.D. Proposals for the organization of virtual tests of object recognition algorithms in control systems of mobile robotic complexes. *Nadezhnost' i kachestvo slozhnykh system = Reliability and quality of complex systems.* 2023;(3):100–106. (In Russ.)
10. Koshelev N.D., Alkhatem A., Novikov K.S. et al. Management of artificial neural networks for recognizing high-resolution image storyboards. *Nadezhnost' i kachestvo slozhnykh system = Reliability and quality of complex systems.* 2022;(2):85–91. (In Russ.)

Информация об авторах / Information about the authors

Илья Сергеевич Галишников
студент,
Московский государственный технический университет имени Н. Э. Баумана
(Россия, г. Москва, ул. 2-я Бауманская, 5, стр. 1)
E-mail: galishnikov.ilya@yandex.ru

Ilya S. Galishnikov
Student,
Bauman Moscow State Technical University
(build. 1, 5 2-ya Baumanskaya street, Moscow, Russia)

Дмитрий Андреевич Аминев
кандидат технических наук, доцент кафедры разработки программных решений и системного программирования,
МИРЭА – Российский технологический университет
(Россия, г. Москва, ул. Стромынка, 20)
E-mail: aminev.d.a@ya.ru

Dmitry A. Aminev
Candidate of technical sciences,
associate professor of the sub-department of development of software solutions and system programming,
MIREA – Russian Technological University
(20 Stromynka street, Moscow, Russia)

Людмила Владимировна Бунина
старший преподаватель кафедры разработки программных решений и системного программирования,
МИРЭА – Российский технологический университет
(Россия, г. Москва, ул. Стромынка, 20)
E-mail: ludmilabunina@mail.ru

Lyudmila V. Bunina
Senior lecturer of the sub-department of development of software solutions and system programming,
MIREA – Russian Technological University
(20 Stromynka street, Moscow, Russia)

Дмитрий Владимирович Козырев
кандидат физико-математических наук,
старший научный сотрудник лаборатории
телекоммуникационных систем,
Институт проблем управления
имени В. А. Трапезникова РАН
(Россия, г. Москва, ул. Профсоюзная, 65);
доцент кафедры теории вероятностей
и кибербезопасности,
Российский университет дружбы народов
имени Патриса Лумумбы
(Россия, г. Москва, ул. Миклухо-Маклая, 6)
E-mail: kozyrev-dv@rudn.ru

Dmitry V. Kozyrev
Candidate of physical and mathematical sciences,
senior researcher of the laboratory
of telecommunication systems,
V.A. Trapeznikov Institute of Management Problems
of the Russian Academy of Sciences
(65 Profsoyuznaya street, Moscow, Russia);
associate professor of the sub-department
of probability theory and cybersecurity,
Patrice Lumumba Peoples' Friendship
University of Russia
(6 Miklukho-Maklaya street, Moscow, Russia)

Авторы заявляют об отсутствии конфликта интересов /
The authors declare no conflicts of interests.
Поступила в редакцию/Received 15.11.2024
Поступила после рецензирования/Revised 16.12.2024
Принята к публикации/Accepted 10.01.2025