УДК 681.3: 629.7
DOI: 10.24412/2071-6168-2021-9-379-384

ФИЗИКА ОТКАЗОВ ЭЛЕКТРОННЫХ ЦИФРОВЫХ УПРАВЛЯЮЩИХ СИСТЕМ

А.Н. Привалов, В.А. Шаров

Исследуются электронные цифровые управляющие системы. Отмечается, что с точки зрения надежности подобные системы имеют иерархическую четырехуровневую структуру, верхний уровень которой представлен самой системой, а на нижнем уровне находятся электронные элементы системы. Показано, что при работе системы на нижнем уровне возникают как перемежающиеся отказы (сбои), так и отказы оборудования, которые могут приводить к отказу системы в целом. Отказы нижнего уровня разделены на статические и динамические. Статические отказы связаны с выходом входных и выходных сигналов за уровень порогов, которые разделяют их диапазон на зоны логического нуля, неопределенного значения и логической единицы. Динамические отказы связаны, в основном с эффектом гонок. С применением математического аппарата сетей Петри-Маркова построена математическая модель возникновения отказов на верхних иерархических уровнях, из которой получено выражение для времени наработки до отказа электронной цифровой управляющей системы.

Ключевые слова: надежность, отказ, иерархическая структура, сеть Петри-Маркова.

В настоящее время при управлении различными объектами широко применяются электронные цифровые управляющие системы (ЭЦУС) [1, 2]. Увеличение роли цифровой техники породила техническую проблему обеспечения надежности систем управления [3, 4, 5]. Для обеспечения требуемых показателей надежности на этапе проектирования необходимо иметь адекватную модель их оценки, которая учитывает особенности функционирования аппаратных средств системы, вытекающие из цифрового характера управления [6, 7, 8]. Таким образом, потребности в широком внедрении ЭЦУС и отсутствие общей теории анализа и расчета эффективности и отказоустойчивости указанных систем, объясняет необходимость и актуальность исследований, в данной области.

Под электронными цифровыми управляющими системами ниже будут пониматься технические средства, в которых взаимодействие между узлами и блоками осуществляется посредством передачи/приема цифровых сигналов. Под цифровыми, в контексте решаемой задачи, понимаются сигналы, принимающие два значения, которые при технической реализации кодируются, как правило, хорошо различающимися значениями информативных параметров сигнала: высоким и низким уровнем постоянных напряжений (потенциальные элементы цифровых устройств), сменой фазы сигнала на 180^0 (фазовые элементы), наличием или отсутствием импульса (импульсные), изменением частоты модуляции и т.п. В ряде технических комплексов ЭЦУС имеют настолько значительный вес, что их сбои и отказы приводят, как минимум, к затруднениям в выполнении целевых функций комплекса, а в отдельных случаях могут привести к серьезным авариям и даже техногенным катастрофам.

Иерархическая структура типовой ЭЦУС приведена на рис. 1. Иерархия представлена следующими уровнями:

0 - уровень цифрового управляющего комплекса;

1 - уровень отдельных подсистем, обеспечивающих определенные функции комплекса;

2 - уровень узлов и блоков ЭЦУС, состоящих из элементов;

3 - уровень элементов (интегральных схем, транзисторов, резисторов, и т.п.).

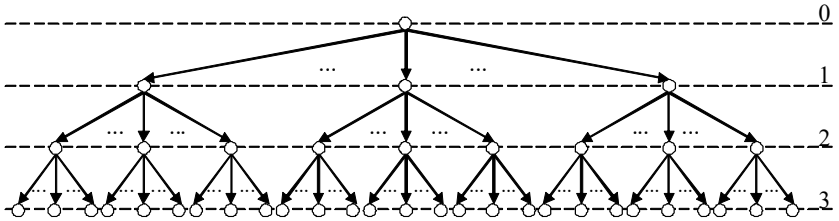


Рис. 1. Иерархическая структура ЭЦУС

На нижнем уровне иерархии ЭЦУС находятся элементы. Наиболее распространенными в настоящее время являются потенциальные элементы, в которых значения *TRUE* и *FALSE* закодированы в виде соответствующих уровней напряжений:

$$u := \begin{cases} TRUE \text{ when } u_n \geq u \geq u^1; \\ FALSE \text{ when } 0 \geq u \geq u^0, \end{cases}$$

где u_n - напряжение питания элементов, u^0 - пороговое напряжение значения *FALSE*; u^1 - пороговое напряжение значения *TRUE*.

В диапазоне $u^0 < u < u^1$ сигнал может быть воспринят элементами цифровых управляющих устройств и как *TRUE*, и как *FALSE*.

Зоны уровней сигналов *u* для потенциальных элементов приведены на рис. 1.

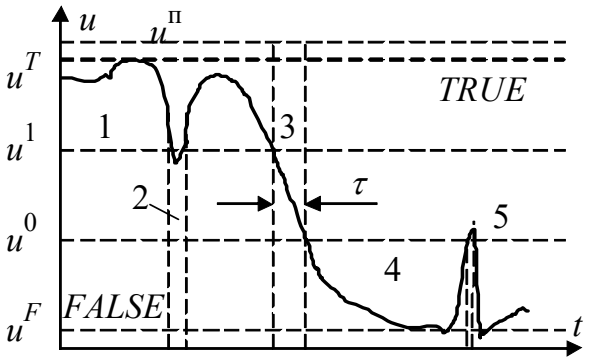


Рис. 2. Зоны уровней сигналов потенциальных элементов

Отказы э лементов могут возникнуть как в их статическом положении, так и при переключении.

К основным статическим параметрам относятся:

напряжение u^T, соответствующее состоянию *TRUE*;

напряжение u^F, соответствующее состоянию *FALSE*;

пороговое состояние логического элемента u^1, малые отклонения от которого могут привести к переходу выходного сигнала элемента из состояния *TRUE* в неопределенное состояние;

пороговое состояние логического элемента u^0, малые отклонения от которого могут привести к переходу выходного сигнала элемента из состояния *FALSE* в неопределенное состояние;

логический перепад $\Delta_u = u^T - u^F$;

допустимое напряжение статической помехи по цепи питания, которое указывается в паспорте на логический элемент, невыход помехи за указанный уровень гарантирует отсутствие сбоев для наихудшего случая работы элемента.

Отказы логических элементов в статическом состоянии проявляются в виде одной из следующих ситуаций:

нарушение логики работы элемента;

установление элемента в неопределенное состояние $u^0 < u < u^1$.

При кратковременном проявлении ситуаций имеет место перемежающийся отказ (сбой) (см. зоны 2 и 5). При устойчивом проявлении перечисленных ситуаций в статическом состоянии имеет место отказ элемента.

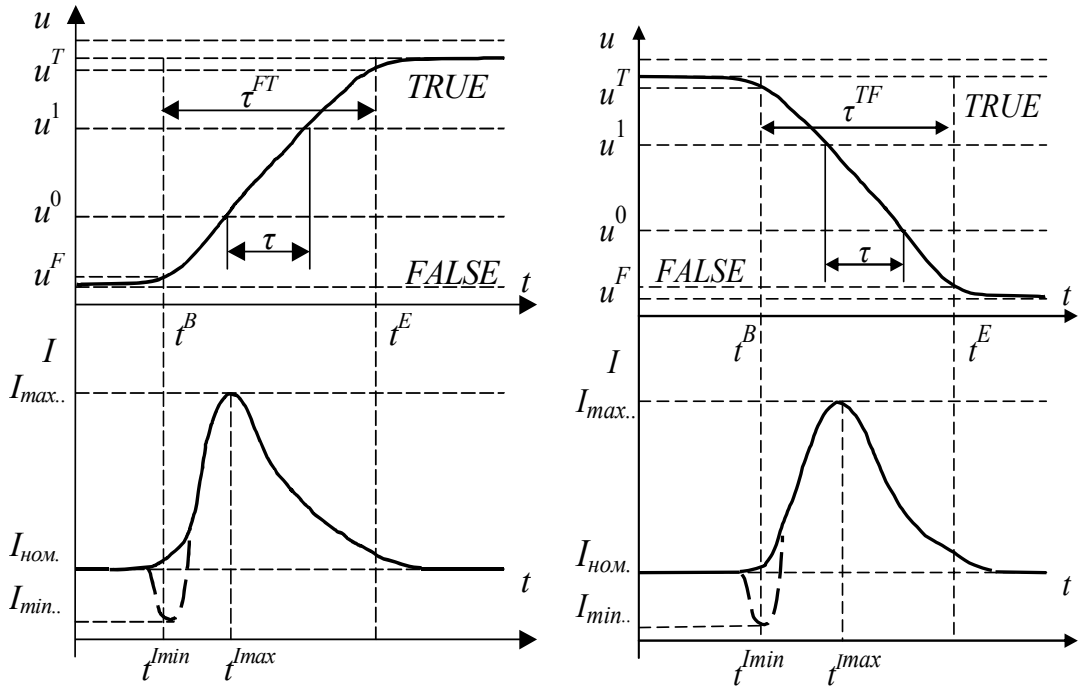
К основным динамическим параметрам элементов относятся (рис. 3):

время $t^{TF} = t^E - t^B$ переключения логического элемента из состояния *TRUE* в состояние *FALSE*;, в течение которого происходит переход выходного напряжения от значения $0{,}1\left(u^T - u^F\right)$ до значения $u^F - 0{,}1\left(u^T - u^F\right)$;

время $t^{FT} = t^E - t^B$ переключения логического элемента из состояния *FALSE* в состояние *TRUE*;, в течение которого происходит переход выходного напряжения от значения $u^F - 0{,}1\left(u^T - u^F\right)$ до значения $0{,}1\left(u^T - u^F\right)$;

время τ^s задержки переключения логического элемента, отсчитываемое от значений $0{,}1\left(u^T - u^F\right)\left(u^F - 0{,}1\left(u^T - u^F\right)\right)$ до значений $0{,}1\left(u^T - u^F\right)\left(u^F - 0{,}1\left(u^T - u^F\right)\right)$.

Кроме того существует ненормируемый параметр τ, время нахождения сигнала в зоне неопределенности, который влияет как на динамический, так и на статический режим работы. Нормальным следует считать переходный процесс, в котором при переключении логического элемента время τ не превышает некоторого предела.



а ***б***

Рис. 3. Переходные процессы в потенциальных элементах: а - при переключении FALSE→TRUE; б - при переключении TRUE→FALSE

В динамическом режиме работы, т.е. при переключениях логических элементов возникает наибольшее количество как устойчивых, так и перемежающихся отказов. Это явление связано со следующими обстоятельствами. В состав реальных логических элементов кроме электрических элементов, проектируемых разработчиком, и выполняющих в изделии заранее запрограммированные функции, входят также т.н. «паразитные» элементы, формируемые в процессе изготовления, но не предусмотренные конструкторской документацией. К элементам подобного рода можно отнести сопротивления и индуктивности проводников, емкости близко расположенных проводников и т.п.

За счет паразитных элементов возможно появление импульсной помехи, во входных цепях триггеров, что иллюстрируется рис. 3, где показано, как за счет паразитного резистора R при срабатывании элемента DD1 возможно возникновение импульса по цепи питания, который переключает RS-триггер DD4-DD5 [9].

Следующий тип отказов возникает при взаимодействии элементов на втором и более высоких уровнях иерархии.

Статические отказы, как правило, возникают при превышении нагрузки на выходе логического элемента его допустимой нагрузочной способности. В этом случае выходной сигнал нагружаемого элемента сдвигается в область $u^0 < u < u^1$, что может привести к сбоям в работе нагружающих элементов. Кроме того, перегрузка приводит к повышенному расходу энергии на гпшожпнили элементе, что может привести его в неработоспособное состояние.

Динамические отказы на этом уровне возникают за счет эффекта «гонок», который иллюстрируется рис. 5.

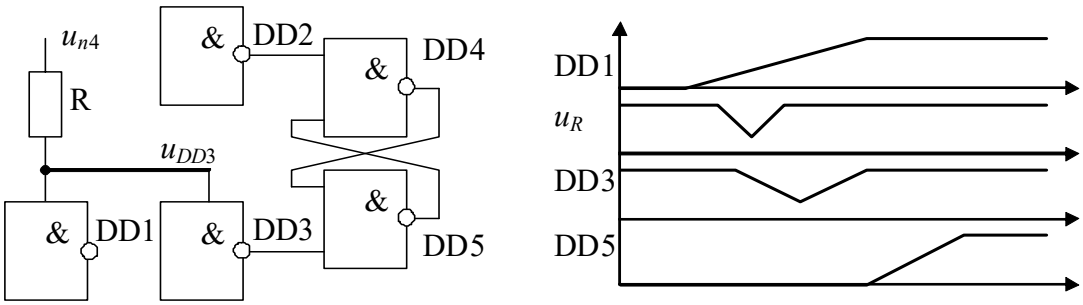


Рис. 4. Формирование импульсной помехи, переключающей RS-триггер

На рис. 5, а производится запись данных с выходов комбинационных логических схем L1, L2, L3 в регистр RG фронтом сигнала C. Переходный процесс в L1, L2, L3 начинается одновременно, но в силу различия задержки переключения во времени, заканчивается в разные моменты [9]. В результате время от окончания переходного процесса до тактирующего фронта сигнала C оказывается равным, соответственно, τ_1, τ_2, τ_3. Каждый из перечисленных интервалов имеет разброс, и с учетом разброса, интервалы могут возникать отказы при записи данных в регистр.

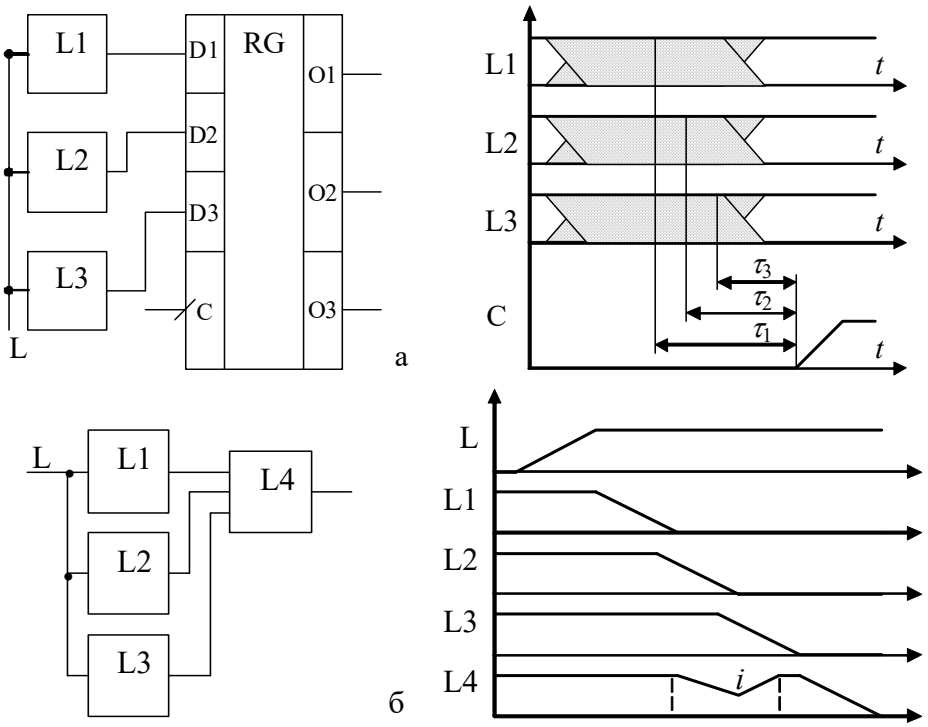


Рис. 5. Эффект "гонок"

В схеме, приведенной на рис. 5 б эффект «гонок» приводит при разбросе формирования сигналов на выходах комбинационных схем одновременном переключении сигнала L на входах комбинационных схем L1, L2, L3 к ложному срабатыванию комбинационной схемы L4.

На уровнях со второго по нулевой ЭЦУС функционирует как конечный автомат, включающий J элементов, каждый из которых при переходе ЭЦУС из текущего состояния в следующее должен сработать безошибочно. Исходя из этой особенности, моделью отказов ЭЦУС может быть сеть Петри-Маркова, представленная на рис. 6 [10]. В сети Петри-Маркова места $a_1, ..., a_j, ..., a_J$ моделируют пребывание соответствующих элементов в работоспособном, или неработоспособном состоянии; место a_{J+1} фиксирует факт бессбойной работы си-

стемы на текущем временном интервале функционирования; место a_{J+2} фиксирует факт отказа системы; переходы z_1, z_2, z_3 являются синхронизирующими. Плотность распределения времени пребывания сети в состояниях $a_1, ..., a_j, ..., a_J$ определяется как $\delta(t-T)$, где T - период следования тактирующих импульсов; $\delta(...)$ - δ-функция Дирака; плотность распределения времени пребывания в месте a_{J+1} определяется как $\delta(t)$; время пребывания в месте a_{J+2} определяется как $f_{J+1}(t)$, т.е. плотность распределения времени , затрачиваемого на восстановление системы.

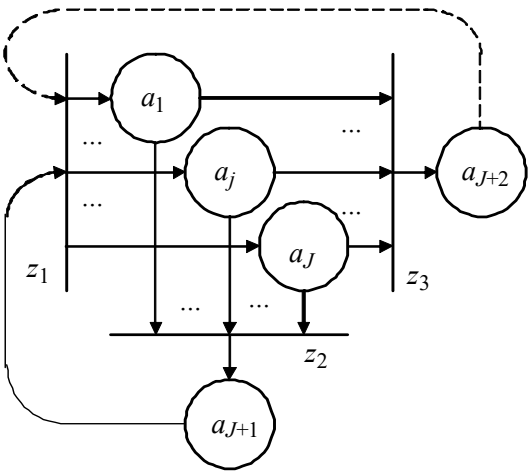


Рис. 6. Петри-Марковская модель отказов ЭЦУС

Вероятности p_j, $1 \le j \le J$ выполнения полушагов из мест a_j в переход z_2 определяются вероятностями отсутствия сбоя *j*-х элементов на момент переключения. Вероятности $1-p_j$, $1 \le j \le J$ выполнения полушагов из мест a_j в переход z_3 определяются вероятностями появления сбоя *j*-х элементов на момент переключения. Логические условия выполнения полушагов (z_2, a_{J+1}) и (z_2, a_{J+2}) являются следующими:

$$\lambda(z_2, a_{J+1}) = \bigwedge_{j=1}^{J} \lambda(a_j, z_2); \quad \lambda(z_2, a_{J+2}) = \bigvee_{j=1}^{J} \lambda(a_j, z_3),$$

где $\lambda(a_j, z_2)$ и $\lambda(a_j, z_3)$ - логические функции выполнения соответствующих полушагов; Λ - групповая конъюнкция; V - групповая дизъюнкция;

$$\lambda(a_j, z_2), \lambda(a_j, z_3) = \begin{cases} 1, \text{if semi} - \text{step is done;} \\ 0, \text{if semi} - \text{step is not done} \end{cases}.$$

По сети Петри-Маркова, приведенной на рис. 6, может быть получена общая зависимость для времени наработки ЭЦУС до отказа:

$$T_O = \frac{T \cdot \prod_{j=1}^{J} p_j}{1 - \prod_{j=1}^{J} p_j}.$$

Вероятности p_j могут быть оценены в результате анализа факторов, воздействующих на каждый элемент ЭЦУС в отдельности. Если эти факторы являются независимыми, то каждая из вероятностей равна произведению вероятностей отсутствия воздействия соответствующих факторов.

Таким образом, для иерархической структуры ЭЦУС, на основании анализа физических процессов, протекающих в элементах системы выявлены основные факторы, вызывающие сбои в работе аппаратных средств. Построена модель, позволяющая рассчитать время наработ-

ки до отказа системы на уровях со второго до верхнего. Дальнейшие исследования в этой области могут быть направлены на определение численных значений различных факторов для различной элементной базы ЭЦУС.

Список литературы

1. Landau I.D., Zito G. Digital Control Systems, Design, Identification and Implementation. Springer, 2006. 484 p.

2. Aström J., Wittenmark B., Computer Controlled Systems: Theory and Design. Tsinghua University Press. Prentice Hall, 2002. 557 p.

3. Sánchez-Silva M., Klutke G.-A. Reliability and Life-Cycle Analysis of Deteriorating Systems. Springer International Publishing. Switzerland. 2016. 355 p.

4. O'Conner P., Kleyner A. Practical Reliability Engineering, Willey and Sons, 2012. 456 p.

5. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем / Отв. ред. В.А. Гуляев. Киев: Наукова думка, 1990. 184 с.

6. Malik S.C., Rathee R. Reliability modelling of a parallel system with maximum operation and repair times. International Journal of Operational Research, Vol. 25, No. 1. 2016. P. 131 - 142.

7. Smith M.D.J., Simpson K.G.: Safety Critical Systems Handbook, Elsevier Ltd., NY. 2011. 270 p.

8. Rousand M. Reliability of Safety-Critical Systems: Theory and Applications, John Wiley & Sons, 2014. 466 p.

9/ Балашов Е.П., Пузанков Д.В. Проектирование информационно-управляющих структур. М: Сов. радио, 1987. 254 с.

10 Ларкин Е.В. К вопросу о расчете временных характеристик сетей Петри-Маркова // Известия Тульского государственного университета. Серия: Вычислительная техника. Автоматика. Управление. Т. 1. Вып. 1. Вычислительная техника. Тула: ТулГУ, 1997. С. 68 - 75.

11. Ларкин Е.В., Сабо Ю.И. Применение сетей Петри-Маркова при моделировании структурных отказов в системе // Известия Тульского государственного университета. Серия: Вычислительная техника. Информационные технологии. Системы управления. Т. 4. Вып. 3. Системы управления. Тула: ТулГУ, 2003. С. 75 - 103.

Привалов Александр Николаевич, д-р техн. наук, профессор, privalov.61@mail.ru, Россия, Тула, Тульский государственный педагогический университет им. Л.Н. Толстого,

Шаров Вадим Арнольдович, аспирант, vs@aqs.ru, Россия, Шуя, Шуйский филиал Ивановского государственного университета

FAILURE PHYSICS OF ELECTRONIC DIGITAL CONTROL SYSTEMS

A.N. Privalov, V.A. Sharov

Electronic digital control systems are investigated. It is noted, that from point of view reliability such systems have hierarchical four-level structure, top level of which is performed with the system itself, and on the lower level electronic elements are situated. It is shown, that when system operation, on the lower level emerging both short-time failures, and failures, which may damage the system as a whole. Failures of lover level are classified on static and dynamic. Static failures are linked with exit of input and output signals out of borders, which divide their ranges onto logic zero zone, uncertain meaning zone and logic unit zone. Dynamic failures essentially are linked with «races» effect. With use of mathematical apparatus of Petri-Markov nets mathematical model of failures emerging on upper hierarchical levels is worked out, from which formula for time of operation till failure is obtained.

Key words: reliability, failure, hierarchical structure, Petri-Markov net.

Privalov Alexander Nikolaevich, doctor of technical sciences, professor, privalov.61@mail.ru, Russia, Tula, Tula State Pedagogical University named after L.N. Tolstoy,

Sharov Vadim Arnoldovich, postgraduate, v.a.d.i.m@bk.ru, Russia, Shuya, Shuya branch of Ivanovo State University