УДК 629.039.58

ИССЛЕДОВАНИЕ МАРКОВСКИХ МОДЕЛЕЙ ИНФОРМАЦИОННО-УПРАВЛЯЮЩЕЙ СИСТЕМЫ НА ОСНОВЕ САМОДИАГНОСТИРУЕМЫХ ПРОГРАММИРУЕМЫХ ПЛАТФОРМ

В.В. СКЛЯР[1], Ю.Л. ПОНОЧОВНЫЙ[2], Е.Н. БУЛЬБА[1], А.О.ИВАСЮК[1]

[1]Научно-производственное предприятие «Радий», Кировоград, Украина
[2]Полтавский национальный технический университет им. Ю. Кондратюка, Украина

У статті розглянуто основні етапи побудови та дослідження марковських моделей функціональної безпеки інформаційно-управляючої системи (ІУС) на основі самодіагностованої програмованої платформи (СДПП). Множину станів моделей отримано на підставі побудови і аналізу дерева відмов, що включає виявлені і невиявлені відмови апаратних каналів ІУС. На підставі запропонованого підходу отримані моделі ІУС в режимі нормальної експлуатації, що враховують різні рівні діагностування. Застосування моделей дозволило визначити межі областей третього рівня повноти безпеки (SIL3) ІУС в двовимірному просторі зміни вхідних параметрів і часу експлуатації системи.

Ключові слова: *інформаційно-управляюча система, функціональна безпека, марковська модель, рівень повноти безпеки.*

В статье рассмотрены основные этапы построения и исследования марковских моделей функциональной безопасности информационно-управляющей системы (ИУС) на основе самодиагностируемой программируемой платформы. Множество состояний моделей получено на основании построения и анализа дерева отказов, включающего обнаруженные и необнаруженные отказы аппаратных каналов ИУС. На основании предложенного подхода получены модели ИУС в режиме нормальной эксплуатации, учитывающие различные уровни диагностирования. Применение моделей позволило определить границы областей третьего уровня полноты безопасности (SIL3) ИУС в двумерном пространстве изменения входных параметров и времени эксплуатации системы.

Ключевые слова: *информационно-управляющая система, функциональная безопасность, марковская модель, уровень полноты безопасности.*

The article describes the main stages of construction and study Markov models of functional safety information-control system (ICS) based on self-checking programmable platform (SCPP). Many states of the model is obtained based on the design and analysis of fault tree that includes detected and undetected hardware failures channel ICS. Based on this approach we obtain the model ICS during normal operation, taking into account the different levels of diagnosis. Application models allowed to define the boundaries of the areas of the third of safety integrity level (SIL3) ICS in two-dimensional space of the input parameters and the operating time of the system.

Key words: *information control system, functional safety, Markov model, safety integrity level.*

Информационно-управляющие системы (ИУС) критических объектов, которые выполняют функции, важные для безопасности критических объектов, оцениваются с позиций функциональной безопасности. Функциональная безопасность зависит от правильного функционирования электрических,

электронных и программируемых электронных (E/E/PE) систем, связанных с безопасностью технологических систем и оборудования для снижения внешнего риска [1]. Принципы анализа функциональной безопасности изложены в [2].

Оценивание функциональной безопасности – это определение показателя уровня риска в области безопасности. Его значение является композицией вероятности опасных ситуаций на производстве и тяжести всех последствий, которые могут возникнуть за время эксплуатации. Особое место занимает оценка функциональной безопасности для систем аварийной защиты реакторных установок.

Модели оценивания функциональной безопасности детально рассмотрены в 6 части стандарта IEC-61508 [3]. В этом документе представлены примеры моделей: блок-схемы надежности, дерева отказов, марковские и мультифазные, сети Петри и Монте-Карло, формальных языков. Также, в данном стандарте отмечено, что приведенные модели являются лишь примерами для построения моделей реальных систем. Так, в работах [4,5] анализируются модели функциональной безопасности систем управления ядерными реакторами и сенсорных систем защиты с учетом их ограничений и условий функционирования. Поэтому в данной работе рассмотрено построение марковских моделей безопасности ИУС САЗ в режиме нормальной эксплуатации и исследовано влияние входных параметров модели на значение показателя функциональной безопасности.

1. Анализ условий функционирования систем аварийной защиты в режиме нормальной эксплуатации

Анализ функциональной безопасности системы аварийной защиты является обязательным при проектировании блока. Система аварийной защиты (САЗ) реактора является одной из наиболее важных систем безопасности и от ее надежности во многом зависит безопасность реакторной установки в целом. САЗ реактора включает в себя электрическую и механическую части.

Механическая часть органа регулирования системы управления защитой (ОР СУЗ) состоит из различного числа приводов с поглощающими стержнями (для современных блоков – 121 ОР СУЗ, на действующих блоках – 61, 89, 103 и др.) а также аппаратуры контроля нейтронного потока (АКНП), системы группового и индивидуального управления (СГИУ), автоматизированных рабочих мест (АРМ), регуляторов ограничения мощности (РОМ) и систем электропитания [6,7].

Отказы в САЗ возникают под воздействием разнообразных факторов. Поскольку каждый фактор в свою очередь зависит от многих причин, то отказы элементов, входящих в состав системы, относятся, как правило, к случайным событиям, а время работы до возникновения отказов – к случайным величинам.

Системы аварийной защиты могут быть реализованы на основе платформ с использованием программируемых логических интегральных схем (ПЛИС). Основное внимание в таких платформах должно быть уделено самодиагностированию для определения опасных и безопасных отказов системы.

Анализ отказов выполняется методами сбора и исследования информации об отказах системы в целом, либо элементов системы. Большинство методов основывается на проведении опросов экспертов, применении численных методов, экспериментальных исследованиях, методах теории вероятности и математической статистики [7].

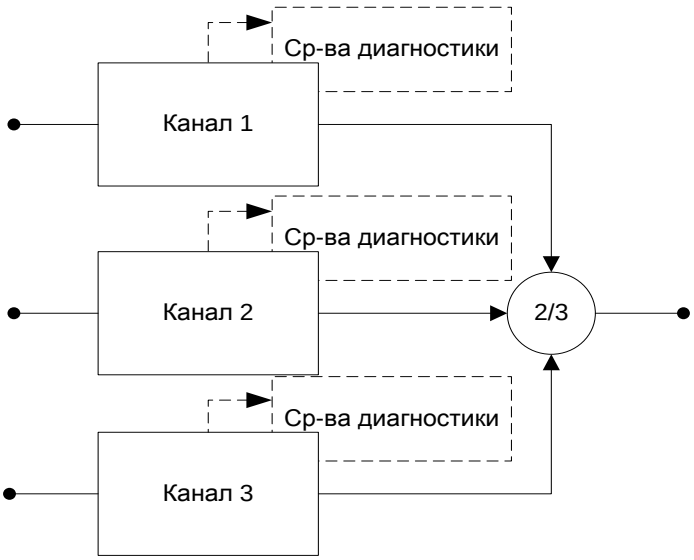


Рис.1. Структурная схема надежности ИУС САЗ в режиме нормальной эксплуатации

Результатом такого анализа может быть построение дерева отказов САЗ, а как следствие, марковской модели состояний системы. Структурная схема надежности, учитывающая мажоритарный контроль представлена на рис.1.

2. Основные допущения марковских моделей информационно-управляющей системы

Рассмотрим работу ИУС, которая является частью САЗ в режиме нормальной эксплуатации. Под нормальной эксплуатацией (normal operation) понимается эксплуатация в установленных эксплуатационных пределах и условиях. ИУС включает три независимых аппаратных канала, каждый из которых диагностируется на наличие опасных отказов системой контроля. Рассматриваемая система функционирует в режиме с низкой частотой запросов к функциям безопасности. Соответственно, для оценки функциональной безопасности необходимо использовать показатель PFD_{avg} – средней вероятности опасного отказа ФБ по запросу.

Система контроля характеризуется параметром DC – охват диагностикой. В отличие от моделей, представленных в [3,5], в рассматриваемой системе контроль выполняется непрерывно (а не периодически) и выявленные отказы устраняются немедленно после обнаружения. Остальные допущения при

построении модели следующие:

– события отказов и восстановлений аппаратных каналов составляют простейшие потоки (стационарные, ординарные и без последействия), с постоянными параметрами λ (интенсивность отказов) и μ (интенсивность восстановления);

– в системе используются идентичные аппаратные каналы с одинаковыми интенсивностями отказов;

– интенсивность отказов мажоритарного органа и системы контроля пренебрежительно мала и в рассматриваемой модели эти системы приняты абсолютно надежными;

– в модели рассматриваются только опасные отказы аппаратных каналов ИУС, интенсивность отказов которых рассчитывается как $\lambda_D = 0.5*\lambda$ [3];

– доля отказов по общей причине пренебрежительно мала, поэтому в данной модели они не рассматриваются [2];

– при диагностировании часть опасных отказов выявляется, соответственно интенсивность обнаруженных опасных отказов $\lambda_{DD} = \lambda_D*DC$, а интенсивность необнаруженных опасных отказов $\lambda_{DU} = \lambda_D*(1–DC)$;

– в предложенной модели не рассматриваются отказы программных средств.

3. Построение множества состояний моделей ИУС САЗ

Каждый аппаратный канал модели может находиться в одном из трех состояний:

- работоспособное;
- проявление опасного отказа, выявленного системой контроля (обнаруженный опасный отказ);
- проявление опасного отказа, невыявленного системой контроля (необнаруженный опасный отказ).

Примечание: так как в данной системе ремонт производится сразу же после

проявления явного отказа, то состояние ремонта не рассматривается, а моделируется возврат в работоспособное состояние с интенсивностью μ.

На рис.6 представлено дерево отказов ИУС, при этом использована графическая нотация (+, –, ×) для отображения соответственных состояний: работоспособного, обнаруженного опасного отказа и необнаруженного опасного отказа.

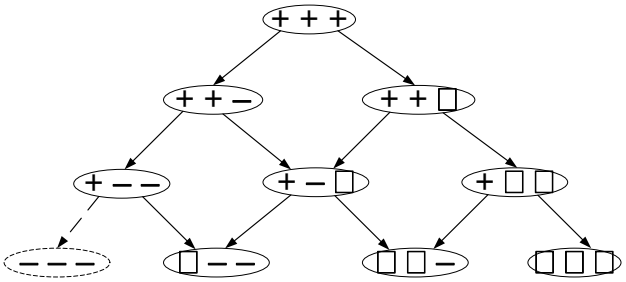


Рис.2. Дерево отказов ИУС

Исходя из спецификации системы, одно из состояний – состояние с тремя обнаруженными опасными каналами, является абстрактным, так как после обнаружения двух опасных отказов система останавливается до выхода из ремонта одного из них.

Размеченный граф (орграф) модели функционирования ИУС в условиях проявления опасных отказов представлен на рис.3. Данный граф построен по классическому подходу, описанному в [3] и содержит поглощающее состояние с необнаруженными опасными отказами S8. В классической модели не предусмотрен выход из состояния необнаруженного опасного отказа без проведения дополнительных мероприятий (например, периодических профилактик с повышенным DC).

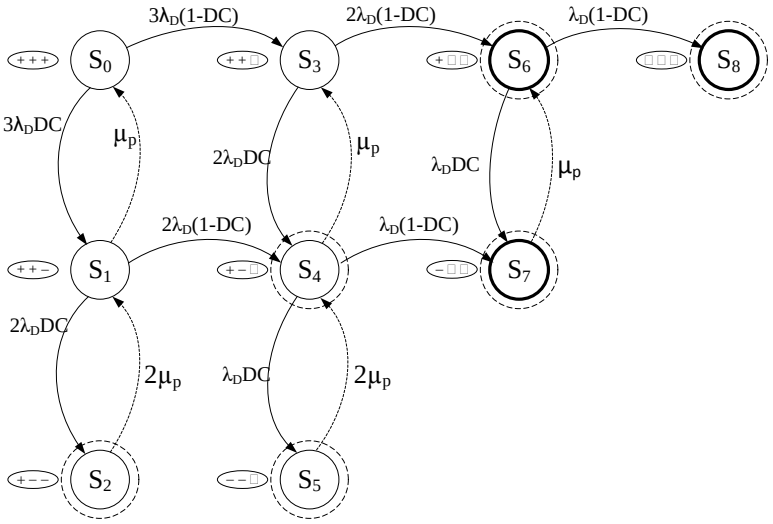


Рис.3. Размеченный граф модели функционирования ИУС САЗ с поглощающими состояниями (МФБ1)

Исходя из логики функционирования системы контроля и мажоритарного органа, содержит:

а) работоспособные состояния: S0 (все каналы исправны), S1 (в одном из каналов проявился и обнаружен опасный отказ) и S3 (в одном из каналов проявился, но не обнаружен опасный отказ);

б) неработоспособные состояния: S2 (в двух каналах проявились и обнаружены опасные отказы), S4 (в одном из каналов проявился и обнаружен опасный отказ, в другом - проявился, но не обнаружен опасный отказ) и S5 (в двух каналах проявились и обнаружены опасные отказы, в третьем проявился, но не обнаружен опасный отказ);

в) состояния с необнаруженными опасными отказами, которые неспособен парировать мажоритарный орган: S6 (в двух каналах проявились, но не обнаружены опасные отказы), S7 (в одном из каналов проявился и обнаружен опасный отказ, в двух каналах проявились, но не обнаружены опасные отказы), S8 (в трех каналах проявились, но не обнаружены опасные отказы).

После обнаружения проявления опасного отказа, неработоспособный канал отключается и восстанавливается с интенсивностью μ_p, это моделируется соответствующими переходами S1→S0, S2→S1, S4→S3, S5→S4, S7→S6. Показатель PFDavg определяется как:

$$PFD_{avg} = 1 - P_0(t) - P_1(t) - P_3(t) \qquad (1)$$

Практика использования рассматриваемых систем [4] показывает, что аппаратный канал с проявившимся необнаруженным опасным дефектом продолжает использоваться. В процессе его использования вероятно проявление других дефектов, которые могут быть выявлены системой контроля. Соответственно, ИУС, после проявления необнаруженного опасного отказа и последующего проявления нового дефекта (обнаруженного опасного отказа) может перейти в состояние ремонта канала.

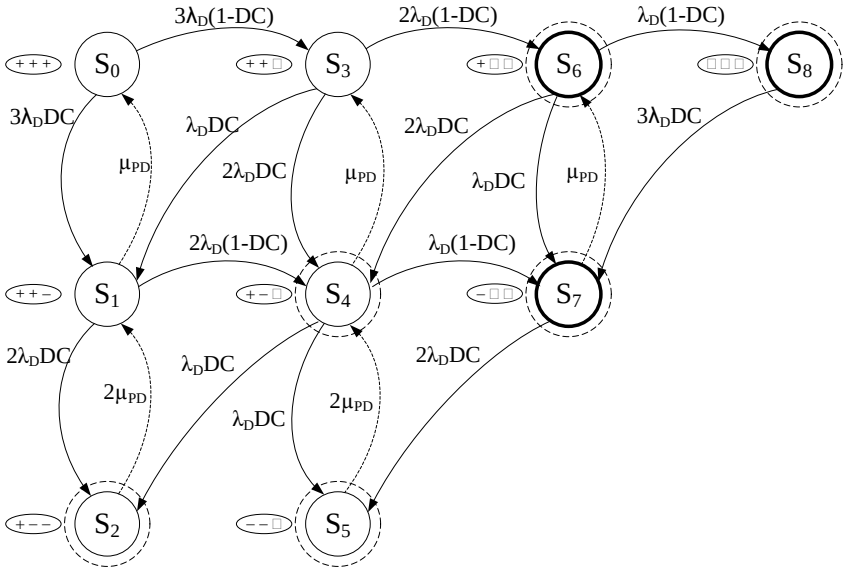


Рис.4. Размеченный граф модели функционирования ИУС САЗ без поглощающих состояний (МФБ2)

При этом, в ходе восстановительных операций проводится полная диагностика канала с устранением всех (обнаруженных и необнаруженных) дефектов.

Также это влияет на длительность восстановления, соответственно $\mu_{PD}=1/(MRT+T_D)<$

$<\mu_P$. Здесь MRT – средняя длительность ремонта одного канала ИУС, T_D – дополнительное время диагностирования невыявленных отказов. Размеченный граф такой модели представлен на рис.4.

Повторное проявление обнаруженных опасных отказов на графе проиллюстрировано переходами S8→S7, S7→S5, S6→S4, S4→S2. Таким

образом, граф на рис.4 не содержит поглощающих состояний.

5. Обоснование входных параметров марковской модели ИУС САЗ

Значения входных параметров были определены исходя из опыта практической эксплуатации рассматриваемого класса систем, а также исходя из рекомендаций, изложенных в [3].

Так как требуется обеспечить значение показателя функциональной безопасности на уровне УПБ3 (SIL3), то есть $PFD_{avg} \in$]1e-4…1e-3], то необходимо провести дополнительные исследования моделей с целью подбора значений входных параметров. Значения входных параметров, относительно которых проводятся исследования, считаются базовыми и представлены в табл.1.

Таблица 1

Базовые значения входных параметров моделей функциональной безопасности ИУС САЗ

Параметр	Базовое значение	Диапазон изменения	Единица измер.
$\lambda_D=0.5*\lambda$	2.5e-5	[0.05 … 5]*1e-5	1/час
$\lambda_{DD}=\lambda_D*DC$	2.25e-5		1/час
$\lambda_{DU}=\lambda_D*(1–DC)$	2.5e-6		1/час
$\mu_P=1/MRT$	1/8		1/час
$\mu_{PD}=1/(MRT+T_D)$	1/(8+4)		1/час
DC	0.9	[0.01…1]	

Также в табл.1 представлены варианты изменения входных параметров λ_{DU} и DC для исследования их влияния на показатель функциональной безопасности.

6. Построение и исследование марковской модели ИУС САЗ

Система дифференциальных уравнений Колмогорова-Чепмена, для графа на рис.3 будет иметь следующий вид:

$$
\begin{cases}
\frac{dP_0}{dt} = -\left[3\lambda_D DC + 3\lambda_D(1-DC)\right]P_0 + \mu_p P_1, \\
\frac{dP_1}{dt} = -\left[2\lambda_D DC + \mu_p + 2\lambda_D(1-DC)\right]P_1 + 3\lambda_D DC P_0 + 2\mu_p P_2, \\
\frac{dP_2}{dt} = -2\mu_p P_2 + 2\lambda_D DC P_1, \\
\frac{dP_3}{dt} = -\left[2\lambda_D(1-DC) + 2\lambda_D DC\right]P_3 + 3\lambda_D(1-DC)P_0 + \mu_p P_6, \\
\frac{dP_4}{dt} = -\left[\lambda_D DC + \lambda_D(1-DC) + \mu_p\right]P_4 + 2\lambda_D DC P_3 + 2\lambda_D(1-DC)P_1 + 2\mu_p P_5, \\
\frac{dP_5}{dt} = -2\mu_p P_5 + \lambda_D DC P_4, \\
\frac{dP_6}{dt} = -\left[\lambda_D(1-DC) + \lambda_D DC\right]P_6 + 2\lambda_D(1-DC)P_3 + \mu_p P_7, \\
\frac{dP_7}{dt} = -\mu_p P_7 + \lambda_D DC P_6 + \lambda_D(1-DC)P_4, \\
\frac{dP_8}{dt} = \lambda_D(1-DC)P_6;
\end{cases}
$$

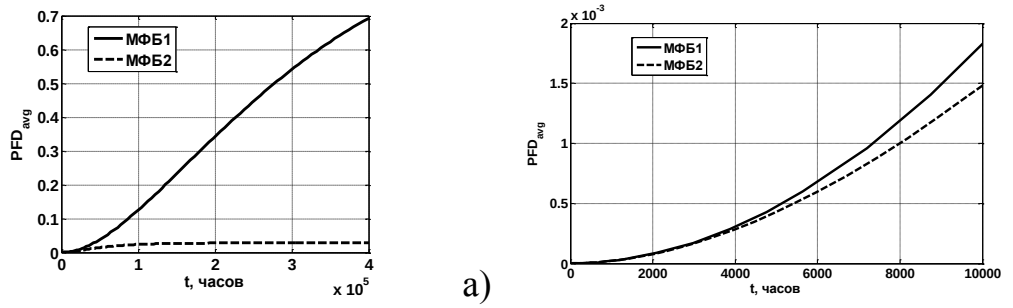
$$
\sum_{i=0}^{8} P_i(t) = 1; \qquad P_0(0) = 1, P_{1..8}(0) = 0. \tag{2}
$$

а для графа на рис.4:

$$
\begin{cases}
\frac{dP_0}{dt} = -3\lambda_D P_0 + \mu_{PD} P_1, \\
\frac{dP_1}{dt} = -\left[2\lambda_D + \mu_{PD}\right]P_1 + 3\lambda_D DC P_0 + 2\mu_{PD} P_2 + \lambda_D DC P_3, \\
\frac{dP_2}{dt} = -2\mu_{PD} P_2 + 2\lambda_D DC P_1 + \lambda_D DC P_4, \\
\frac{dP_3}{dt} = -\left[2\lambda_D + \lambda_D DC\right]P_3 + 3\lambda_D(1-DC)P_0 + \mu_{PD} P_6, \\
\frac{dP_4}{dt} = -\left[\lambda_D(DC+1) + \mu_{PD}\right]P_4 + 2\lambda_D DC(P_3 + P_6) + 2\lambda_D(1-DC)P_1 + 2\mu_{PD} P_5, \\
\frac{dP_5}{dt} = -2\mu_{PD} P_5 + \lambda_D DC P_4 + 2\lambda_D DC P_7, \\
\frac{dP_6}{dt} = -\left[\lambda_D + 2\lambda_D DC\right]P_6 + 2\lambda_D(1-DC)P_3 + \mu_{PD} P_7, \\
\frac{dP_7}{dt} = -\left[\mu_{PD} + 2\lambda_D DC\right]P_7 + \lambda_D DC P_6 + \lambda_D(1-DC)P_4 + 3\lambda_D DC P_8, \\
\frac{dP_8}{dt} = -3\lambda_D DC P_8 + \lambda_D(1-DC)P_6;
\end{cases}
$$

$$
\sum_{i=0}^{8} P_i(t) = 1; \qquad P_0(0) = 1, P_{1..8}(0) = 0. \tag{3}
$$

Решение СДУ Колмогорова было выполнено в системе Matlab с помощью метода ode15s для временного интервала [0…10000] часов. Результаты моделирования представлены на рис.9 для модели ИУС с поглощающими состояниями.



а) б)

Рис.5. Зависимость показателя PFD_{avg} от времени эксплуатации для моделей МФБ1(а) и МФБ2(б)

Из рис.5 хорошо видно, что наличие поглощающих состояний обуславливает непрерывный рост показателя PFD_{avg}. С другой стороны, модель без поглощающих состояний иллюстрирует асимптотическое стремление показателя функциональной безопасности к стационарному значению PFD_{avg} = 0,028 через 16000 часов работы. При этом требования УПБ3 (SIL3) обеспечиваются на временном интервале до 7200 часов эксплуатации (10 месяцев эксплуатации) для модели МФБ1; и на временном интервале до 8000 часов эксплуатации для модели МФБ2.

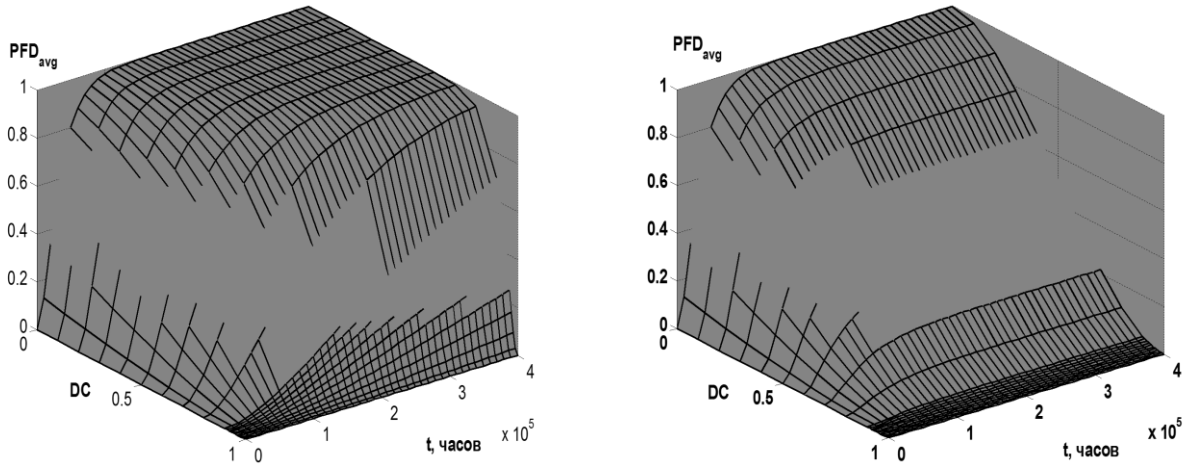


Рис.6. Зависимость поведения функции $PFD_{avg}(t)$ от входного параметра DC (охвата диагностикой) для МФБ1 (а) и МФБ2 (б)

На рис.6 в трехмерном представлении показана зависимость функциональной безопасности $PFD_{avg}(t)$ от значений входного параметра $DC \in [0…1]$. Анализируя графики можно отметить, что при отсутствии диагностики опасных отказов (DC = 0), обе модели показывают идентичное поведение функции $PFD_{avg}(t)$ (графики совпадают). При выявлении всех опасных отказов (DC=1) модели показывают одинаковое поведение функции $PFD_{avg}(t)$: асимптотическое стремление к устоявшемуся значению; при этом графики отличаются в силу разности входных параметров μ_P и μ_{PD} (рис.7).

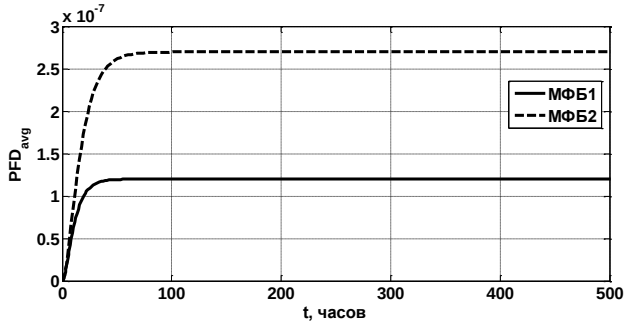
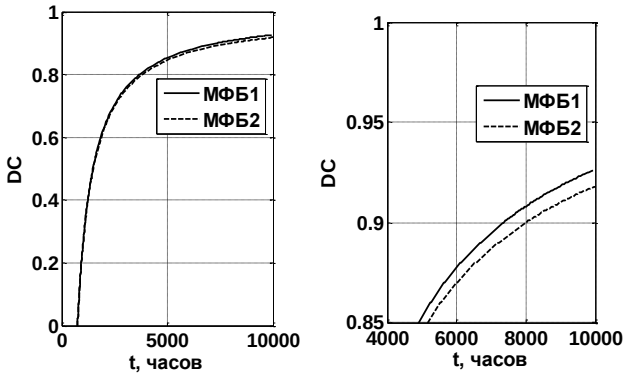


Рис.7. Различие между функциями $PFD_{avg}(t)$ моделей МФБ1 и МФБ2 при DC=1

Динамика изменения показателя функциональной безопасности $PFD_{avg}(t)$ показывает, что в обеих моделях (МФБ1 и МФБ2) значение входного параметра охвата диагностикой DC влияет на длительность временного периода выполнения системой требований УПБ3 (SIL3). Более детально такое влияние иллюстрируют график проекции трехмерной фигуры на плоскость [t,DC] по уровню PFD_{avg}=1e-3 (рис.8). Для лучшей наглядности графики показаны в

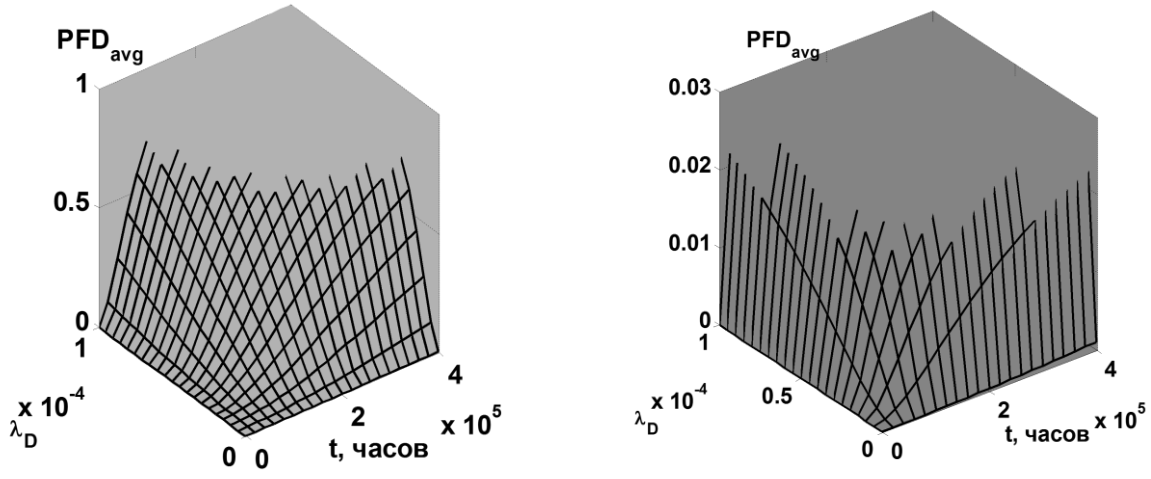
разных масштабах относительно оси DC.



а) б)

Рис.8. Проекции показателя PFD_{avg} на плоскость [t,DC] по уровню PFD_{avg}=1e-3 в масштабе $t \in [0 \ldots 10000]$(а) и $t \in [4000 \ldots 10000]$(б)

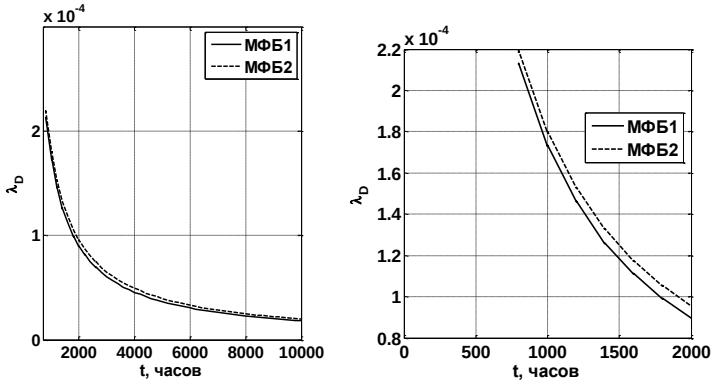
На рис.9 в трехмерном представлении показана зависимость функциональной безопасности $PFD_{avg}(t)$ от значения интенсивности опасных отказов λ_D для моделей МФБ1 и МФБ2. На первый взгляд, модель МФБ2 (без поглощающих состояний) иллюстрирует лучший результат, так как в ней показатель $PFD_{avg}(t)$ стремиться к устоявшемуся значению PFD_{avg} = 0,028 (значение обусловлено стабильной комбинацией параметров DC = 0.9 и μ_{PD} = 0.0833).



а) б)

Рис.9. Зависимость поведения функции $PFD_{avg}(t)$ от входного параметра λ_D для МФБ1 (а) и МФБ2 (б)

Модель МФБ1 иллюстрирует стремление показателя $PFD_{avg}(t)$ к единице. И чем больше интенсивность опасных отказов, тем быстрее функция $PFD_{avg}(t)$ приближается к устоявшемуся значению.



а) б)

Рис.10. Проекции показателя PFDavg на плоскость [t, λ_D] по уровню PFD_{avg}=1e-3 3 в масштабе t∈[0…10000](а) и t∈[4000…2000](б)

Однако, если посмотреть проекцию трехмерных фигур рис.9 на плоскость [t, λ_D] по верхнему срезу требований УПБ-3 (SIL-3), то разница между результатами моделирования МФБ1 и МФБ2 не превышает Δt=100 часов при λ_D =1e-4 (рис.10).

Выводы

Анализ полученных результатов моделирования функциональной безопасности ИУС показал, что:

а) при учете вторичного проявления опасных отказов и выявления их системой контроля для базисных значений входных параметров достигается устоявшееся значение PFD_{avg} = 0,028, что недостаточно для систем безопасности уровня УПБ3 (SIL3);

б) при значении интенсивности опасных отказов = 2.5e-5 (1/час) рассматриваемая система удовлетворяет требованиям УПБ3 (SIL3) в течении первых 8000 часов работы; для продления этого срока до 10000 часов необходимо повысить охват диагностикой до уровня DC=0.92;

в) если невозможно повысить охват диагностикой, то для продления временного периода обеспечения требований УПБ3 (SIL3) до 10000 часов необходимо снизить интенсивность отказов каждого канала до $\lambda = 2*\lambda_D$ = 4e-5 1/час.

Практический интерес представляют разработанные Matlab-программы, которые можно использовать в инженерной практике.

Существенным не достатком разработанных моделей является отсутствие учета влияния программных отказов в каналах ИУС. Учет проявления

программных дефектов и устранения их в ходе ремонтно-восстановительных работ, как описано в [8], является направлением дальнейших исследований и развития разработанных моделей.

БІБЛІОГРАФІЯ

1. IEC 61508-1:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems -Part 1: General requirements [Text]. – impl. 01.05.2010. – Brussels: European Committee for Electrotechnical Standardization, 2010. – 68 p.
2. Скляр, В.В. Элементы методологии анализа функциональной безопасности информационно-управляющих систем [Текст]/ В.В. Скляр // Радіоелектронні і комп'ютерні системи. - 2009. - № 6. - С.75-79.
3. IEC 61508-6:2010. Functional safety of electrical/electronic/programmable electronic safetyrelated systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 [Text]. – impl. 01.05.2010. – Brussels: European Committee for Electrotechnical Standardization, 2010. – 118 p.
4. Бахмач, Е.С. Обеспечение и оценка безопасности информационных и управляющих систем АЭС на базе ПЛИС [Текст]/ Е.С. Бахмач, А.А. Сиора, В.В. Скляр, В.И. Токарев, В.С. Харченко // Радіоелектронні і комп'ютерні системи. - 2007. - № 7. - С.75-82.
5. Langeron, Y. Combination of safety integrity levels (SILs): A study of IEC61508 merging rules [Text]/ Y. Langeron, A. Barros, A. Grall, C. Berenguer // Journal of Loss Prevention in the Process Industries. – 2008. - 21(4) – P.437-449.
6. ГОСТ 26843-86. Реакторы ядерные энергетические. Общие требования к системе управления и защиты[Текст]. – введ. 01.03.1986. – М.: Стандартинформ, 1986. – 112 с.
7. Погосов, А.Ю. Технические средства управления ядерными реакторами с водой под давлением для АЭС: учеб. [Текст] /А.Ю. Погосов - М.: Наука и техника, 2012. - 288 с.
8. Поночовный, Ю.Л., Сиора, А.А., Харченко. В.С. Модели готовности двухканальной информационно-управляющей системы с учетом обновления программных средств [Текст] / Ю.Л. Поночовный, А.А. Сиора, В.С. Харченко // Радіоелектронні і комп’ютерні системи. – 2014. – № 6(70). – С.135-139.

Скляр Владимир Владимирович – доктор технических наук, профессор, директор технический научно-производственного предприятия «Радий», Кировоград, Украина.

Поночовный Юрий Леонидович – кандитат технических наук, старший научній сотрудник, доцент кафедры компьютерной инженерии Полтавского национального технического университета им. Юрия Кондратюка, Полтава, Украина.

Бульба Евгений Николаевич – старший научный сотрудник научно-производственного предприятия «Радий», Кировоград, Украина.

Ивасюк Александр Олегович – заместитель директора технического научно-производственного предприятия «Радий», Кировоград, Украина.