На правах рукописи

Кузнецов Петр Анатольевич

АВТОМАТИЗИРОВАННАЯ СИСТЕМА АНАЛИЗА НАДЕЖНОСТИ АСУ ТП ОПАСНЫХ ПРОИЗВОДСТВ

05.13.06 – Автоматизация и управление технологическими процессами и производствами (промышленность)

АВТОРЕФЕРАТ

Диссертации на соискание ученой степени кандидата технических наук

Красноярск - 2019

Работа выполнена в ФГБОУ ВО «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева» (СибГУ им. М.Ф. Решетнева)

Научный руководитель: кандидат технических наук
Лосев Василий Владимирович

Официальные оппоненты:

Дулесов Александр Сергеевич
доктор технических наук, доцент
ФГБОУ ВО «Хакасский государственный университет им. Н.Ф. Катанова», г. Абакан,
профессор кафедры информационных технологий и систем

Царев Роман Юрьевич
кандидат технических наук, доцент
ФГАОУ ВО «Сибирский федеральный университет», г. Красноярск,
доцент кафедры информатики

Ведущая организация: ФГБОУ ВО «Томский государственный университет систем управления и радиоэлектроники»

Защита состоится «20» декабря 2019 г. в __ часов на заседании диссертационного совета Д 212.249.05, созданного на базе Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнева по адресу: 660037 г. Красноярск, проспект имени газеты «Красноярский рабочий», 31.

С диссертацией можно ознакомиться в библиотеке Сибирского государственного университета науки и технологий имени академика М.Ф. Решетнева и на сайте https://www.sibsau.ru

Автореферат разослан «___» _____ 2019 г.

Ученый секретарь
диссертационного совета,
кандидат технических наук, доцент — Панфилов Илья Александрович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В настоящее время происходит быстрое развитие технических систем, в частности, автоматизированных систем управления технологическими процессами (АСУ ТП). Применение АСУ ТП позволяет значительно увеличить производительность технологических процессов и их эффективность. Степень эффективности автоматизированных систем зависит от параметров и показателей АСУ ТП.

Одним из существенных факторов, оказывающих влияние на эффективность управления, является надежность.

Надежность – показатель, включающий в себя множество параметров. Существует целый набор принципов поддержания надежности на должном уровне. Традиционным является подход к анализу надежности в виде анализа безотказности системы. Но на практике надежность АСУ ТП определяют и другие показатели, такие как безопасность. Актуальной является разработка как безопасных, так и безотказных систем, чего требуют современные стандарты безопасности и надежности систем, такие как МЭК 61508/МЭК 61511.

Наиболее активные разработки в области проектирования высоконадежных систем проводятся в Санкт-Петербургском государственном университете, Санкт-Петербургском политехническом университете Петра Великого, Московском государственном техническом университете гражданской авиации и ряде других.

Следует отметить вклад в развитие данного научного направления российских учёных, таких как Соложенцев Е.Д., Рябинин И.А., Сугак Е.В. и зарубежных учёных, таких как Benjamin Lamoureux, Nazih Mechbal, Jeffrey Banks, Felix Redmill.

Для разработки безопасных и безотказных систем необходимо проводить анализ соответствующих надежностных показателей на различных этапах разработки. Следовательно, возникает потребность в создании системы анализа надежности АСУ ТП, учитывающей комплекс надежностных показателей, таких как опасность и ограниченность отказа. Следует установить целевые критерии, увеличение которых будет определять надежность формируемой структуры системы. Также необходимо обеспечить применение в анализе систем учёт различных принципов обеспечения безопасности и безотказности. Учёт таких параметров и принципов является достаточно трудоёмким, следовательно, работу системы следует автоматизировать.

Возникает задача разработки автоматизированной системы анализа надежности АСУ ТП, которая бы позволяла анализировать множество надежностных показателей, строить структуру АСУ ТП с пониженной вероятностью опасных отказов.

Цель работы: повышение параметров надежности АСУ ТП опасных производств на этапе их разработки, внедрения и эксплуатации.

Для достижения поставленной цели в диссертации решаются следующие **задачи:**

– анализ методов повышения надежности на этапах жизненного цикла АСУ ТП;

– разработка методики многоатрибутивной декомпозиции АСУ ТП, обеспечивающей учет важности той или иной функции АСУ ТП при реализации анализа надежности системы;

– разработка алгоритма учета опасностей потенциальных отказов, включающего анализ простых и сложных опасностей, а также опасностей, свойственных функциональному модулю и отдельным его элементам;

– разработка для системы анализа надежности алгоритма ввода в структуру АСУ ТП блокирующих модулей при формировании её структуры;

– разработка имитационной модели для анализа надежности сформированной структуры АСУ ТП;

– разработка программного обеспечения, реализующего предложенную систему анализа надежности;

– применение системы анализа надежности к АСУ ТП.

Область исследования. Работа выполнена в соответствии со следующими пунктами паспорта специальности 05.13.06:

– теоретические основы и прикладные методы анализа и повышения эффективности, надежности и живучести АСУ на этапах их разработки, внедрения и эксплуатации;

– теоретические основы, методы и алгоритмы диагностирования, (определения работоспособности, поиск неисправностей и прогнозирования) АСУТП, АСУП, АСТПП и др.

Методы исследования. Для достижения поставленных целей и решения задач использованы методы теории вероятностей, теории графов, теории вычислительных процессов, теории надежности и метод Монте-Карло.

Новые научные результаты, выносимые на защиту:

1. Разработан новый алгоритм учета опасностей потенциальных отказов, позволяющий, в отличии от существующих, при разработке АСУ ТП разделить отказы на категории, оценить последствия отказов и негативный эффект избыточности, учесть случаи комплексных отказов, обеспечивая более высокий приоритет резервирования модулям с наиболее опасными отказами, таким образом, понижая вероятность наступления опасных отказов.

2. Разработана методика многоатрибутивной декомпозиции АСУ ТП с учетом важности, определяющая отдельные компоненты – модули; функции, выполняемые ими; назначающая важность функции для системы; определяющая типы модулей и явления, происходящие в системе, и, таким образом, позволяющая оценить вероятности пребывания АСУ ТП в различных надежностных состояниях, ограничить последствия отказов и повысить вероятность исправной работы наиболее важных модулей.

3. Предложен алгоритм ввода в структуру АСУ ТП модулей, блокирующих опасности и отказы, впервые включающий типизацию функциональных модулей и ввод блокирующих модулей согласно типам функциональных модулей, что обеспечивает повышение надежности системы при наличии ограничений на избыточность и уменьшение опасностей в случае их возникновения.

4. Разработана имитационная модель на основе многоатрибутивной декомпозиции, использующая сети Петри и которая, в отличии от известных, позволяет, с учётом блокирующих модулей, определять различные конечные состояния системы и вероятности её попадания в них.

Достоверность полученных результатов подтверждается корректным использованием математического аппарата теории вероятностей, вычислительными экспериментами и практическими результатами.

Оценка теоретической значимости результатов работы. Значение для теории состоит в разработке новых алгоритмов учета опасностей, ввода блокирующих модулей и методики многоатрибутивной декомпозиции. Результаты, полученные при выполнении диссертационной работы, создают теоретическую основу для развития алгоритмов анализа показателей надежности АСУ ТП на различных этапах их разработки.

Практическая ценность работы. На основе разработанных алгоритмов и методик создана новая система анализа надежности АСУ ТП, реализующая оригинальный подход, учитывающий и снижающий вероятность опасного отказа в резервированных системах. Результаты диссертационного исследования используются при проектировании новых АСУ ТП на предприятии АО «Красноярский завод синтетического каучука», что подтверждается актом об использовании.

Апробация работы. Модели и алгоритмы, полученные автором данной работы, докладывались на конференциях «Молодые ученые в решении актуальных проблем науки» в 2012, 2013, 2014 гг., г. Красноярск, «Лесной и технический комплексы: проблемы и решения» в 2012, 2013 гг., г. Красноярск, Всероссийской научно-практической конференции творческой молодежи «Актуальные проблемы авиации и космонавтики» в 2015, 2016, 2017, 2018 гг., г. Красноярск, IV Международной молодежной научно-практической конференции «Научные исследования и разработки молодых ученых», Новосибирск, 2015 г., международной научно-практической конференции «Актуальные задачи математического моделирования и информационных технологий», г. Сочи, 2015 г.

Публикации. Основные результаты работы изложены в 18 научных публикациях, в том числе пять статей в ведущих рецензируемых научных изданиях, рекомендуемых ВАК, пять статей, в изданиях, индексируемых в международных базах цитирования Scopus.

Структура работы. Диссертационная работа состоит из введения, четырех глав, основных результатов и выводов, библиографического списка из 133 наименований. Основной текст изложен на 137 страницах.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность работы. Произведена постановка цели и задач исследования. Приводятся основные положения работы.

В первой главе проводится анализ методов и подходов повышения надежности на этапах жизненного цикла АСУ ТП опасных производств.

Описывается метод проектирования высоконадежных систем. Отмечается необходимость дополнения списка анализируемых показателей надежности. Общими свойствами и отличительными особенностями АСУ ТП, как сложных систем являются следующие: наличие множества элементов, многофункциональность элементов и системы, элементы в процессе взаимодействия обмениваются информацией, энергией, материалами и др.

Создание АСУ ТП осуществляется в несколько стадий: формирование требований; разработка концепции; техническое задание; технический проект; рабочий проект; монтаж и наладка; приемо-сдаточные испытания; промышленная эксплуатация.

Качество функционирования технических систем определяется различными показателями. Одним из таких показателей является надёжность. На описанных

стадиях возможно применение различных методов повышения параметров надежности.

На стадии разработки возможно:

1. Введение избыточности (внутриэлементной, структурной, информационной, алгоритмической) системы. Структурная избыточность (фактически – резервирование) позволяет создать надежные автоматизированные системы (АС) из ненадежных элементов.

2. Применение более надежных компонентов. То есть, при разработке АС применяются элементы, которые выполняют требуемые функции в заданных условиях, но при сопоставлении, имеют более высокие показатели надежности.

На стадии эксплуатации возможно:

1. Улучшение условий эксплуатации системы. То есть, в процессе установки системы должна быть правильно выбрана компоновка элементов системы в блоках и обеспечен отвод тепла, выделяющегося при работе.

2. Организация интенсивного профилактического обслуживания системы и отдельных ее элементов.

Одним из важнейших средств обеспечения заданного уровня параметров надежности объекта является резервирование.

На построение резервированной системы отводится определённый объем ресурсов. Требуется определить структуру системы, которая достигает экстремума целевой функции $P(t)$, при наличии ограничений. Ограничивающим степень резервирования фактором является запас ресурсов, выделяемый на построение системы.

Таким образом, имея целевую функцию и ограничения, переходим к формированию оптимального состава резервированной системы. Для решения этой задачи возможно применить базовый метод покоординатного наискорейшего спуска с фиксированным шагом. В случае последовательного соединения элементов системы, наибольшее приращение суммарной безотказности обеспечивает резервирование самого ненадежного модуля. Повышение безотказности системы производится путём итерационного добавления резервного элемента в модуль с наименьшей вероятностью безотказной работы. Для каждого модуля определяется функция выбора направления, также называющаяся функцией приоритета, значение которой в базовом методе будет обратно пропорционально вероятности безотказной работы.

Во второй главе описывается разработанная методика многоатрибутивной декомпозиции АСУ ТП, выявляющая дополнительные показатели надежности и позволяющая определить опасности отказов и необходимость их блокировки. В главе разрабатываются алгоритм учёта опасностей и алгоритм ввода в структуру АСУ ТП блокирующих модулей, включаемые в систему анализа надежности. Данные алгоритмы и методики разработаны с учётом современных достижений теории надежности и стандартов. В многоатрибутивную декомпозицию включается декомпозиция компонентная, функциональная, декомпозиция по атрибуту «тип компонента» и декомпозиция по атрибуту «явление» (возникающее в системе).

Компонентная декомпозиция выявляет отдельные модули системы, которые могут быть резервированы. Декомпозиция на типы модулей выявляет вещества и энергии, используемые модулями системы. Анализ выявленных типов модулей позволяет определить дополнительные способы повышения надежности модулей.

Декомпозиция на явления определяет варианты явлений, происходящих в АСУ ТП при отказах, а также их последствия.

Функциональная декомпозиция важна, так как исследование надежности системы не должно ограничиваться рассмотрением надежности отдельных модулей. Рассмотрение должно охватывать систему целиком. Как правило, одна система АСУ ТП выполняет несколько функций. При анализе надежности системы необходимо определить, какие элементы участвуют в выполнении функций АСУ ТП.

Предлагаемая глубина декомпозиции АСУ ТП ограничивается уровнем функциональных последовательностей. В случае рассмотрения АСУ производственного процесса, в первую очередь, функцией системы управления можно назвать получение какого-либо материального результата, выходного продукта. Другой функцией может быть и контроль над определённым параметром, получение информации. В случае рассмотрения АСУ прочих процессов, варианты функций и их важности могут быть и другими.

Важность последовательностей, выполняющих функции, должна учитываться при выборе приоритетного для резервирования модуля.

Шаги методики многоатрибутивной декомпозиции и назначения важности имеют вид:

1. Выявление компонентов АСУ ТП.
2. Определение типов компонентов.
3. Определение явлений, происходящих в АСУ ТП.
4. Выявление последовательностей компонентов, исправность которых обеспечивает управление технологическими параметрами системы для получения продукта.
5. Выявление последовательностей, исправность которых обеспечивает контроль технологических параметров системы.
6. Назначение важности выявленным функциям, исходя из необходимости их исправности и масштаба последствий, вызываемого прекращением выполнения этих функций.
7. Последовательный перебор модулей и определение, в выполнении какой функции участвует очередной модуль. Если модули окончились – завершение.
8. Если модуль участвует в выполнении функции управления – переход к пункту 10.
9. Если модуль участвует в выполнении только функции контроля – переход к пункту 11.
10. Назначение модулю важности, соответствующей функции управления. Переход к пункту 7.
11. Назначение модулю важности, соответствующей функции контроля. Переход к пункту 7.

Разработанная оригинальная методика многоатрибутивной декомпозиции АСУ ТП позволяет оценить вероятности её пребывания в состоянии полной или частичной исправности путём выявления последовательностей модулей, выполняющих функцию контроля, при возникновении отказа, в которых АСУ ТП становится частично исправной. Данная методика обеспечивает повышение безотказности выбранных функций системы. Также разработанная методика многоатрибутивной декомпозиции определяет явления опасных и безопасных отказов, происходящих в системе. А это, в свою очередь, обеспечивает не только

безотказность, но и безопасность системы. Различие опасностей по их влиянию может быть выражено в виде определённой величины, коэффициента. Следует определить для каждого модуля значение величины, количественно оценивающей опасность, которую несёт отказ, а так же те показатели надежности, при которых модуль можно признать безопасным. Подобные параметры и величины приведены в МЭК 61508/МЭК 61511.

Алгоритм учёта опасностей отказов состоит из следующих этапов:

1. Определение возможных опасных воздействий системы.

2. Определение для каждого модуля величины, количественной оценивающей опасность отказа.

3. Анализ того, возникает ли опасное воздействие при отказе модуля или его резервного элемента. В случае возникновения опасного воздействия при отказе модуля алгоритм переходит к пункту 4. В случае опасного воздействия при отказе элемента – к пункту 5.

4. Определение коэффициента опасности отказа модуля. Переход к пункту 6.

5. Определение коэффициента опасности отказа элемента. Переход к пункту 6.

6. Обнаружение комплексных опасностей – опасностей, возникающих из-за нескольких одновременных отказов.

7. Назначение модулям или элементам коэффициентов приоритета с учётом их доли влияния.

Создание алгоритма учёта опасностей потенциальных отказов позволяет системе разделить опасности на категории по значимости в зависимости от масштабов опасности и причиняемого ими вреда.

Рассмотрение опасных воздействий, возникающих из-за отказов, и в особенности, опасных воздействий, возникающих из-за отказов резервных элементов, приводит к необходимости применения дополнительных мер, иных, чем добавление резервных элементов.

Одним из методов повышения надежности является метод блокирующих модулей (БМ). Применение блокирующих модулей эффективно при наличии негативных последствий избыточности, а, следовательно, наличии ограничения на избыточность. Повышение вероятности безотказной работы системы путем ввода блокирующих модулей достигается путём нейтрализации разрушающих воздействий, направленных на АСУ ТП.

Варианты блокирующих модулей, включаемых в АСУ ТП, зависят от типов функциональных модулей, определённых многоатрибутивной декомпозицией.

С учётом вероятности выхода из строя самого БМ формула надежности будет иметь вид

$$P = (1 – (1 – P_2) \times (1 – P_b)) \times P_c,$$

где P_2 – вероятность того, что отказ функционального модуля не произошёл, P_b – вероятность того, что блокирующий модуль сработал, P_c – вероятность исправности самого блокирующего модуля в штатном режиме. Корректность данной формулы подтверждается проверкой при помощи метода Монте-Карло.

Наряду с модулями, блокирующими отказы, существуют и модули, которые предотвращают воздействие опасности на персонал и инфраструктуру.

Основные шаги включения блокирующих опасности и отказы модулей выглядят следующим образом:

1. Анализ типов компонентов.

2. Назначение блокирующих модулей в соответствии с требованиями стандартов и выявленными при многоатрибутивной декомпозиции типами компонентов.

3. Расходование ресурсов на назначенные блокирующие модули.

4. Увеличение безотказности модулей, которым назначены блокирующие отказ модули.

Алгоритм включения при формировании системы блокирующих модулей позволяет обеспечить уменьшение опасных воздействий и повышение надежности модулей системы.

Таким образом, предложенные модификации метода позволяют не только повысить безотказность системы, но и обеспечить безопасность отказов и ограничить их последствия.

В третьей главе приведенным выше алгоритмам и методикам даётся точное математическое описание, с целью их практического применения.

В качестве исходных данных система использует набор модулей со всеми вариантами их основных и резервных элементов и набор ограничений ресурсов L. Для каждого модуля осуществляется поиск версии с максимальной надежностью. Затем среди всех версий находятся все остальные версии, для которых надежность равна максимальной. Далее среди всех элементов находится версия с наименьшим расходом ресурсов. С учётом рассмотренных параметров надежности делается вывод о необходимости введения показателя, определяющего очередность резервирования модулей. Вводится функция приоритета, вычисляющая данный показатель. Она будет иметь вид

$$Ra_i = (K_{dei} \cdot K_i) / (P_i), \quad (1)$$

где i – номер модуля, чей приоритет вычисляется; K_i – коэффициент приоритета, зависящий от важности и опасности отказа модуля; P_i – вероятность исправной работы модуля; K_{dei} – коэффициент приоритета, зависящий от опасности отказа элемента модуля.

Причём коэффициенты K_i и K_{dei} подчиняются условиям $0 < K_i < 1$, $0 < K_{dei} < 1$.

В дальнейшем эти значения будут считаться показателями целевой вероятности безотказной работы i-го модуля. Данная функция (1) позволяет при формировании структуры АСУ ТП учитывать специфические для них показатели надежности, такие как важность и опасность отказа. Рассмотрим, как вычисляются аргументы введённой функции приоритета.

Для обеспечения учёта важности той или иной функции, на первом шаге определяются последовательности модулей, выполняющие функцию. Каждой последовательности назначаются показатели важности W.

$$W_j = w,$$

где $w = 1$, если последовательность выполняет функцию контроля; $w = 2$, если последовательность выполняет функцию управления объектом.

Каждому модулю должна быть назначена величина Wm_i, определяющая важность этого модуля. В случае если i-ый модуль имеет важность $Wm_i = 1$, соответствующий коэффициент K_i выбирается равным показателю вероятности безотказной работы самого ненадежного модуля системы. Это уменьшит приоритет резервирования менее важных модулей. В случае если важность модуля $Wm_i = 2$ – производится анализ опасности i-го модуля. Согласно требованиям к безопасности системы выбирается интегральный уровень безопасности *SIL* (safety integrity level). Каждому интегральному уровню безопасности соответствует своя

доля опасных отказов *SFF* (safety failure factor). Также при формировании требований выбирается целевая вероятность безотказной работы главной функции *P*.

Исходя из интегрального уровня безопасности, определяется интенсивность опасных отказов и интенсивность безопасных отказов:

$$\lambda = \frac{-\ln(P)}{t}, \lambda = \lambda_s + \lambda_d ,$$

где λ_s – интенсивность безопасных отказов, λ_d – интенсивность опасных отказов, t – срок службы системы.

По λ_s и λ_d находятся целевые вероятности опасных и безопасных отказов всей системы $\lambda_s = \lambda \cdot SFF$, $\lambda_d = \lambda \cdot (1 - SFF)$. По λ_s и λ_d находятся целевые вероятности опасных и безопасных отказов:

$$P_{fdt} = 1 - e^{-\lambda d\, t},\ P_{fst} = 1 - e^{-\lambda st}.$$

Введём понятие целевой вероятности безотказной работы каждого *i*-го модуля P_{sti} и P_{dti}. Причём P_{sti} будет соответствовать безотказной работе безопасного модуля, а P_{dti} – опасного модуля. Данные величины должны быть равны между собой и обеспечивать достижение вероятностей P_{fst} и P_{fdt} соответственно:

$$P_{fst} = 1 - P_{sti}^{\ n},$$

$$P_{fdt} = 1 - P_{dti}^{\ n}.$$

Решая относительно $P_{sti,}$ получим:

$$P_{sti} = \sqrt[n]{1 - P_{fst}} .$$

Решая относительно $P_{dti,}$ получим:

$$P_{dti} = \sqrt[n]{1 - P_{fdt}} .$$

Среди модулей с безопасными отказами не производится градация по опасности, таким образом, коэффициентом для каждого безопасного модуля будет $K_i = P_{sti.}$ Градация по опасности проводится среди модулей с опасными отказами. В зависимости от природы опасного воздействия, выбирается величина *c*, количественно оценивающая опасность. Затем находится отношение этой величины к критическому её значению, умноженное на вероятность опасного отказа.

В случае с аварийно-химическими опасными веществами такой величиной, к примеру, может служить среднесмертельная концентрация:

$$M_i = \frac{C_i}{\text{ССК}_\text{i}} \cdot P_{fdti}, P_{fdti} = 1 - P_{dti},$$

где c_i – концентрация, возникающая в воздухе рабочей зоны при опасном отказе в *i*-ом модуле, $ССК_i$ – среднесмертельная концентрация, P_{fdt} – вероятность отказа.

Данная величина находится для каждого модуля с опасным отказом, а затем определяется среднее её значение. Затем при постоянных *c* и *ССК*, определяется, какой должна быть P_{dtib} для достижения этой средней *M*:

$$P_{fdti} = M_{avg} \cdot \frac{\text{ССК}_\text{i}}{C_i}, \text{P}_\text{dtib} = 1 - \text{P}_\text{fdti} .$$

Достижение всеми модулями равной величины M_{avg} обеспечивает равное распределение ущерба по всем модулям. В случае, если опасный отказ возникает в

модуле то $K_i=P_{dtib}$, $K_{dei}=1$. Если же опасный отказ возникает в элементе, то $K_i=P_{dti}$, $K_{dei}=P_{dtib}$.

Действие алгоритма не ограничивается учётом опасностей. Предложен следующий механизм включения блокирующих модулей. Имеется множество T типов функциональных модулей, выявленных при декомпозиции. Их типизация основывается на используемых ими веществах и энергиях. Каждому типу модуля соответствует свой, блокирующий отказ или опасность, модуль.

$$T_i \leftrightarrow Bf_i, T_i \leftrightarrow Bd_i,$$

где T – множество типов модулей, Bf – множество блокирующих отказ модулей, Bd – множество блокирующих опасность модулей, i – порядковый номер типа БМ.

$$T_i = j \Rightarrow Bf_i = j,$$

где j – номер типа модуля.

Затем для каждого функционального модуля определяется его тип и назначается блокирующий модуль соответствующего типа.

$$M_i \leftrightarrow T_i \leftrightarrow Bf_i, M_i \leftrightarrow T_i \leftrightarrow Bd_i,$$

где i – порядковый номер модуля.

У каждого блокирующего отказ модуля имеется определенный набор характеристик надежности, расход ресурсов на реализацию, и формула, согласно которой снижается вероятность отказа. У каждого блокирующего опасность модуля имеется величина снижения ущерба и расход ресурсов на реализацию.

Рассмотренные действия объединяются в единую автоматизированную систему анализа надежности. Работа системы анализа представляет собой следующую последовательность действий. Вначале итерационного процесса добавления модулей формула приоритета не вычисляется. Первый набор версий модулей, формирующих систему, будет набором основных модулей, который будет образовывать минимально работающую систему. Только после того, как такая система будет создана, начнётся процесс приоритетного резервирования. Это обеспечивает наличие определённой величины вероятности отказа у каждого модуля. Для каждого модуля вычисляется приоритет резервирования и модуль с самым большим приоритетом резервируется.

Используя вероятность безотказной работы каждого модуля и результаты декомпозиции строится имитационная модель надежности АСУ ТП в виде стохастической сети Петри. Вероятности отказа и исправности модулей, возникновения явлений и срабатывания блокировок представляются в виде вероятностей срабатывания перехода. По сформированной сети Петри находится вероятность исправной работы только главной функциональной последовательности АСУ ТП и вероятность исправной работы всех модулей АСУ ТП. Вероятность пребывания сети в определённом состоянии зависит от вероятностей срабатывания переходов (рисунок 1). В позицию P_{41}, обозначающую исправность функции управления, фишка попадёт при попадании фишек в позиции P_{14}, P_{15} и т.д. Фишка попадет позицию P_{14} когда сработает переход T_2 или когда сработает переход T_1, а затем T_4. В позицию P_{15} фишка попадёт после срабатывания перехода T_5. Для остальных позиций вероятности вычисляются аналогично. Таким образом, математически реализуется система анализа, учитывающая различные показатели надежности АСУ ТП и обеспечивающая более точный их учёт.

Для автоматизации вычислений предложенных алгоритмов разработана программа, содержащая в себе процедуры, выполняющие алгоритм учета

опасностей, использующий предложенный способ их анализа, реализующие механизм включения блокирующих модулей и методику декомпозиции с учетом важности функции. Диаграмма последовательностей работы программы приведена на рисунке 2. Блок-схема алгоритма работы автоматизированной системы приведена на рисунке 3.

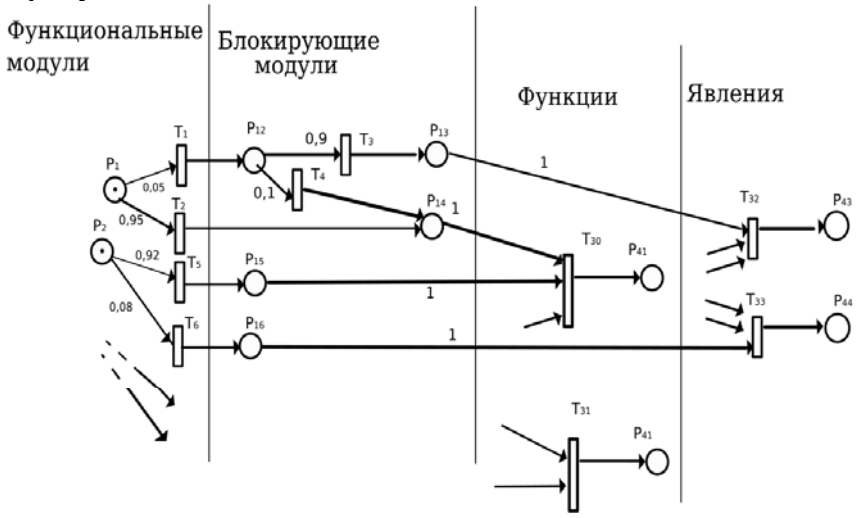

Рисунок 1 – Сеть Петри, моделирующая АСУ ТП с избыточностью

Исходя из важности функций, программа выполняет распределение важности по модулям и находит наиболее важную функциональную последовательность модулей. Программа выполняет анализ опасностей, считанных из файлов, проводя их категоризацию, рассчитывая распределение долей опасностей в случае комплексных опасностей и определяя опасность модулей и элементов.

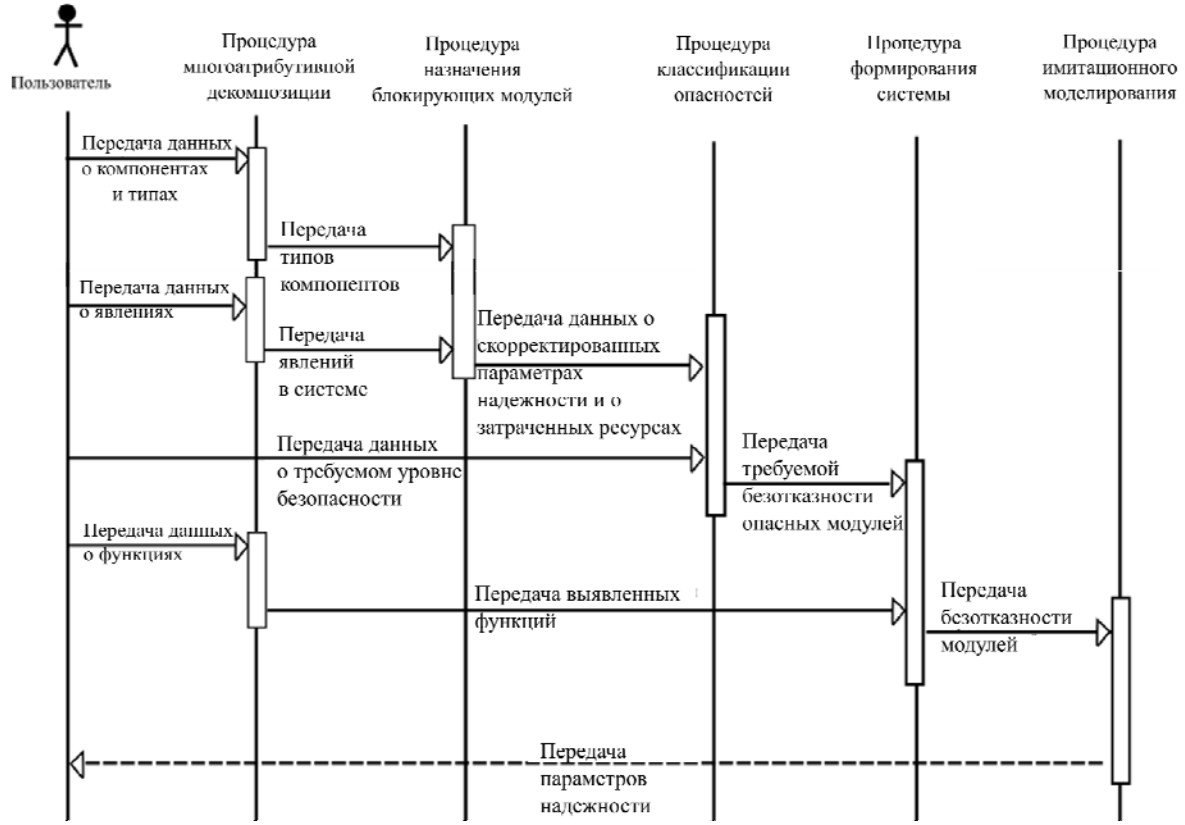

Рисунок 2 – Диаграмма последовательностей работы программы

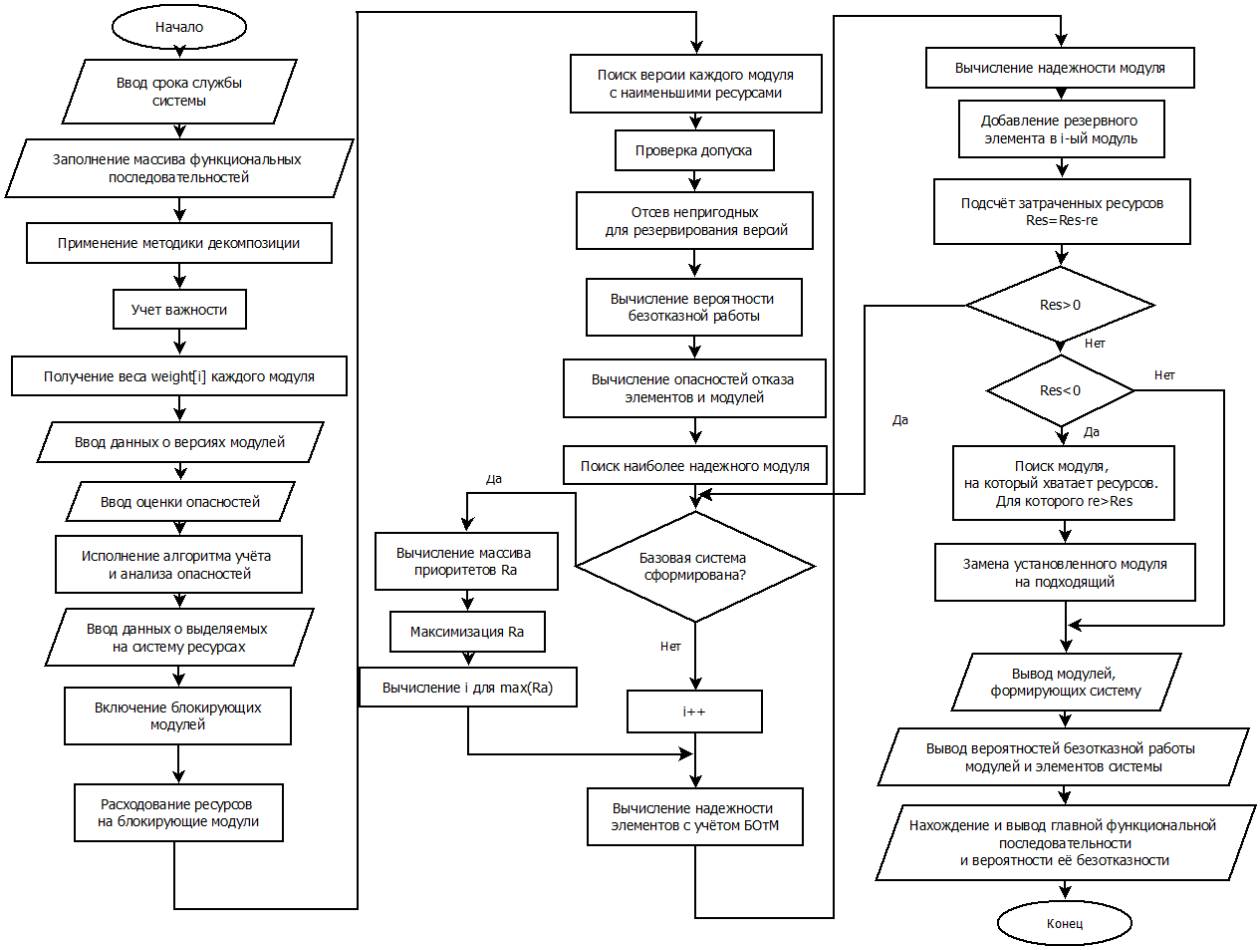

Рисунок 3 - Блок-схема алгоритма работы автоматизированной системы

Исходя из выявленных при декомпозиции типов функциональных модулей, программа включает в систему блокирующие модули. Система выбирает наиболее подходящие резервные элементы среди всех возможных для каждого модуля. Используя полученные данные о важности, безотказности и опасности модулей, система итеративно вычисляет функцию приоритета резервирования модулей, выбирает резервируемый модуль, добавляет в него резервный элемент и вычисляет остаток ресурсов. После формирования структуры АСУ ТП системой вычисляются и выводятся ее итоговые показатели надежности.

Для представления эффективности работы системы необходимо продемонстрировать её работу на примере анализа надежности автоматизированной системы управления технологическим процессом получения поликарбоната и контроля испытания агрегата.

Четвертая глава посвящена практической реализации метода, его применению к реальным АСУ опасных технологических процессов. Рассматривается технологический участок процесса получения поликарбоната и технологический процесс контроля испытаний энергетического агрегата.

На рисунке 4 приведена схема технологического процесса получения поликарбоната. Водный раствор дифенолята натрия непрерывно поступает в реактор каскада реакторов. Сюда же подается метиленхлорид из резервуара и фосген. Синтез поликарбоната на основе дифенолята проводится фосгенированием дифенолята в растворе хлоралканов (обычно метиленхлорида) при нормальных условиях. Дифенолят и фосген являются аварийно химически опасными веществами, следовательно, использование их в технологическом процессе

характеризует его, как опасный. Расход дифенолята натрия стабилизирован. Он измеряется расходомером FE (2-1) и регулируется клапаном (2-2). Расход фосгена также стабилизирован. Измеряется его расход расходомером FE (4-1). Регулируется расход фосгена клапаном (4-2), выполненном в специальном исполнении для регуляции опасных веществ. Уровень метиленхлорида в резервуаре 1 контролируется расходомером LT (1-1).

Для сравнения эффективности известных методов повышения надежности с предлагаемым, приведем показатели надежности, полученные с применением данных методов. При полном дублировании всех модулей АСУ ТП получается система с вероятностью безотказной работы главной функции – 0,89, а всей системы – 0,87. Применение метода наискорейшего спуска без учёта безопасности и блокирования отказов даёт вероятность безотказной работы главной функции 0,916, а всей системы – 0,91.

Применив разработанный метод, получим следующие результаты. При декомпозиции выявляются модули системы, функции управления процессом и контроля параметров. Функциями, выполняемыми системой, будут функция получения реакционной смеси и функции контроля уровня в резервуаре и реакторе. Определяются модули, выполняющие их. Также определяются типы модулей – в частности, выявляется, что расходомеры, датчик температуры, контроллер, шина сбора данных использует электрическую энергию, а следовательно, их необходимо снабдить блокирующим модулем, предотвращающим отказы из-за отклонений параметров электропитания. Явлениями в системе, требующими особого учёта, будут опасные отказы клапанов регулирования расхода фосгена и дифенолята натрия.

Целевая вероятность безотказной работы всей АСУ ТП будет равна 0,99. Для того чтобы считаться достаточно безопасной, она должна будет иметь SIL 3, исходя из чего целевой вероятностью безопасной работы клапанов фосгена и дифенолята будет 0,994 и 0,989 соответственно.

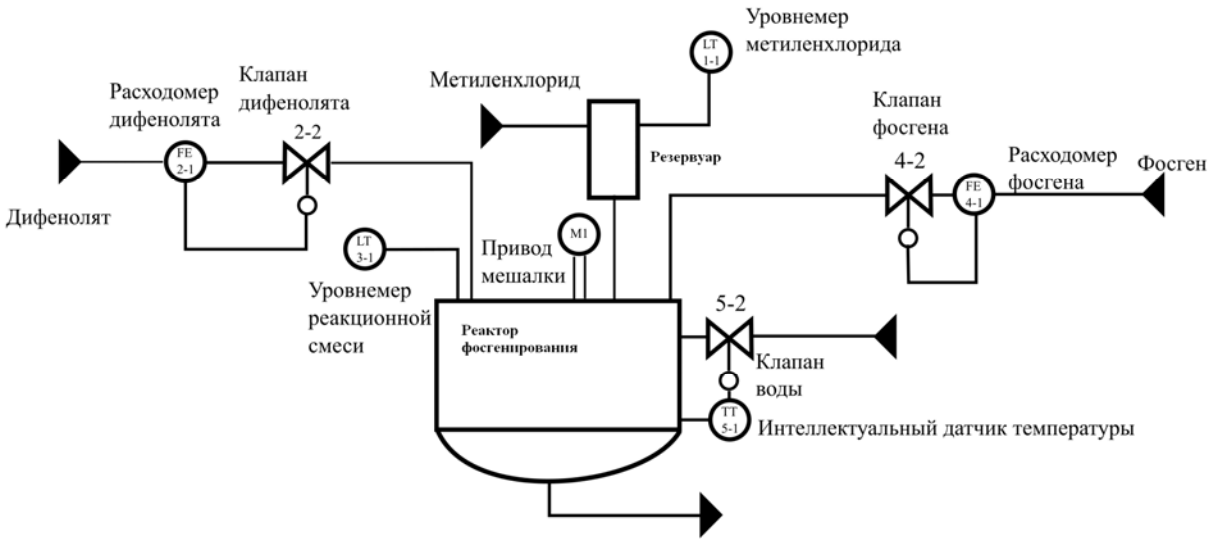

Рисунок 4 – Схема технологического процесса получения поликарбоната

Построение безотказной и безопасной структуры АСУ ТП при помощи автоматизированной системы анализа и повышения надежности осуществляется путём оптимизации структуры резервирования по методу наискорейшего спуска, используя функцию приоритета (1). Система анализа формирует структуру системы с избыточностью, учитывающую опасность и важность модулей.

Для АСУ, построенной с учётом безопасности и блокирования отказов, вероятность безотказной работы главной функции будет 0,94, а для всей системы – 0,96.

На рисунке 5 приведено дерево отказов созданной АСУ ТП с введенными резервными модулями, выделенными пунктиром. Используется аппарат и обозначения математической логики, что позволяет проследить возникновение событий в системе. Таким событиями будет отказ всей системы или главной её функции.

Отказы основного и резервного элементов структуры АСУ ТП процесса получения поликарбоната обозначены с F1 по F20. Через событие T1 обозначен отказ всей АСУ ТП, через событие T2 – отказ функции регулирования АСУ ТП.

Результирующими надёжностными показателями системы, построенной без учёта опасности и важности модулей, будет вероятность исправности главной функции Ps_1 = 0,94. Результирующими надёжностными показателями АСУ, построенной при помощи разрабатываемой системы, учитывающей опасность и важность, будет вероятность исправности главной функции Ps_1 = 0,96. Сравнивая величины вероятности исправности, можно сделать вывод, что применение метода позволяет повысить безотказность главной функции на 7,8%.

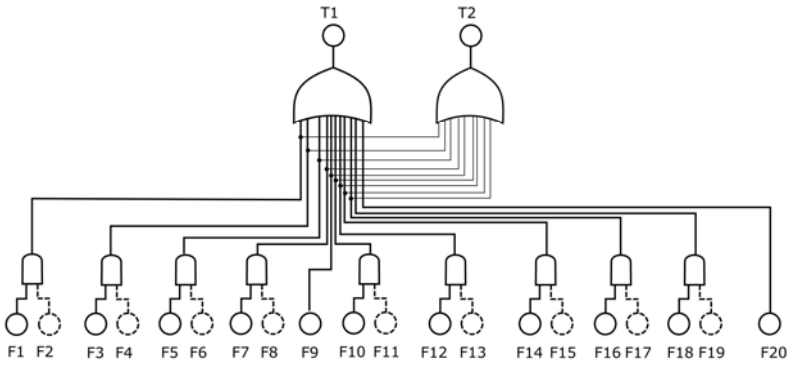

Рисунок 5 – Деревья отказов АСУ ТП

Второй рассматриваемой системой является АСУ технологического процесса испытаний энергетического агрегата, представленная на рисунке 6.

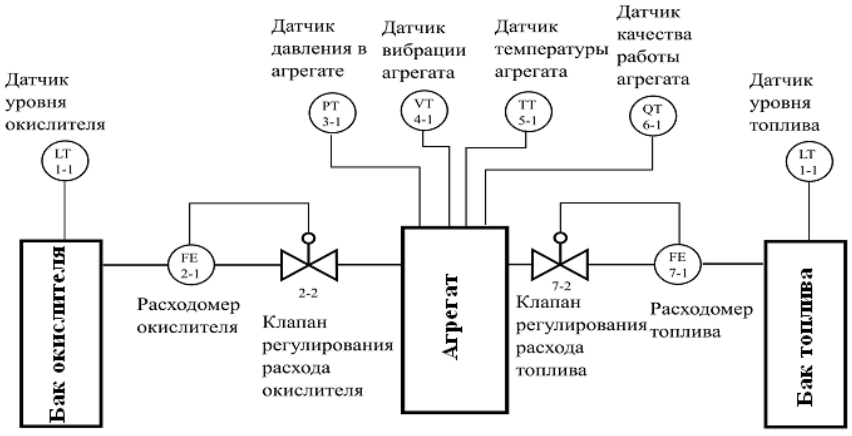

Рисунок 6 – Система технологического процесса испытаний

В своей работе агрегат использует топливную смесь. Подача компонентов топлива регулируется контуром управления, включающим в себя датчики расхода топлива и окислителя $FE_т$ и $FE_о$, клапанами КТ и КО. При дублировании всех элементов системы вероятность одновременной исправности всех элементов системы будет 0,93, а главной функции 0,94. Результирующими показателями надежности системы, построенной без учёта опасности и важности модулей, будет

вероятность исправности всей системы P равная 0,963 и главной функции Ps_1 равная 0,974. В результате работы автоматизированной системы с учётом безопасности и блокирования отказов выделяются функции системы. Ими будет функция сбора информации об испытании и функция контроля параметров самой технологической установки.

Анализируя типы модулей, определено, что расходомеры, датчики температуры, вибрации, давления и качества, а также шина сбора данных и контроллер используют электрическую энергию, и, следовательно, должны быть снабжены блокирующим колебания электропитания модулями.

Обнаруженными явлениями будет опасный отказ клапанов регулирования расхода компонентов топливно-воздушной смеси. Для продолжения анализа выбирается целевая вероятность безотказной работы 0,97%. Показатель доли безопасных отказов SFF выбираем равным 90%, что соответствует третьему уровню интегральной безопасности.

Опасный отказ наступает, когда отказывает клапан регулирования расхода. Следовательно, целевая вероятность отказа отдельного модуля 0,0015, вероятность безотказной работы 0,9985. Причём данной вероятностью безотказной работы должен обладать именно отдельный клапан. Система анализа надежности использует эти данные и предлагает структуру АСУ с вероятностью исправности всей системы P, равной 0,964 и вероятностью исправности главной функции P_{s1} - 0,985. Результаты работы системы анализа надежности в виде дерева отказов построенной структуры АСУ ТП испытания с резервированием приведены на рисунке 7. Отказы основного и резервного элементов структуры АСУ ТП процесса испытания энергетического агрегата обозначены с F1 по F25. Через событие T1 обозначен отказ всей АСУ ТП, через событие T2 – отказ функции регулирования АСУ ТП.

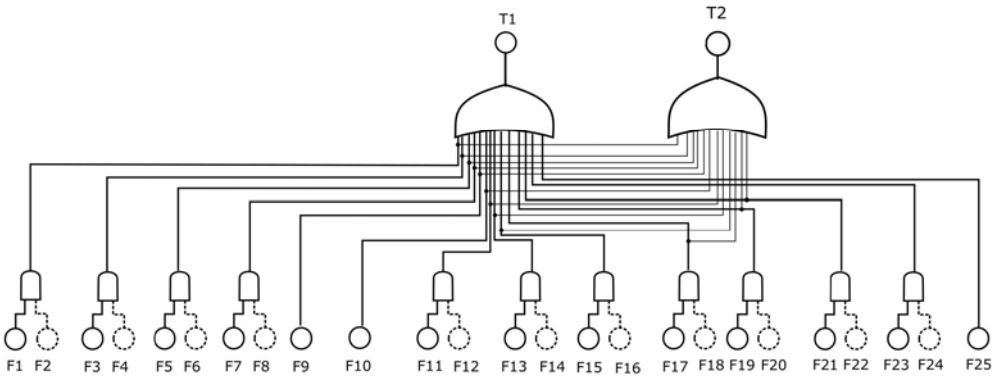

Рисунок 7 – Дерево отказов АСУ ТП испытания

В заключении сформулированы основные результаты и выводы, полученные по результатам разработки автоматизированной системы анализа надежности АСУ ТП, реализующей новый оригинальный подход, учитывающий и снижающий вероятность опасных отказов в резервированных системах.

Основные результаты и выводы работы:

1. Разработан алгоритм учёта опасностей потенциальных отказов, позволяющий системе анализа надежности разделить опасности на категории по значимости в зависимости от масштабов опасности и причиняемого ими вреда. Для алгоритма разработан способ анализа опасностей, позволяющий системе дать оценку негативного эффекта избыточности, учесть случаи комплексных отказов, и,

таким образом, обеспечить приоритет резервирования модулей с наиболее опасными отказами, понижая вероятность наступления наиболее опасных отказов.

2. Для автоматизированной системы разработана оригинальная методика многоатрибутивной декомпозиции АСУ ТП, определяющей компоненты – модули, выполняющие функции, с учетом важности, что позволяет оценить вероятности её пребывания в различных состояниях. В методике обеспечены учёт важности той или иной функции АСУ ТП, позволяющий ограничить последствия отказов, повышая вероятности безотказности наиболее существенных функций, а также определение типов компонентов и явлений, возникающих в АСУ ТП.

3. Предложен и введён в систему анализа надежности механизм добавления блокирующих модулей при формировании структуры АСУ ТП, позволяющий обеспечить уменьшение опасных воздействий и повышение надежности модулей системы

4. На основе многоатрибутивной декомпозиции разработана имитационная модель, использующая сети Петри и позволяющая с учётом блокирующих модулей определять различные конечные состояния системы и вероятности её попадания в них.

5. Разработано программное обеспечение, реализующее систему анализа надёжности с учётом опасностей отказов, важности функций, применением блокирующих опасности и отказы модулей и формирующее безотказную и безопасную структуру АСУ ТП.

6. Проведена апробация системы анализа надежности на примере АСУ ТП процесса получения поликарбоната и АСУ ТП процесса испытаний, по результатам которой получено повышение безотказности главной функции на 7,8% и 4,7% соответственно.

Таким образом, разработанная система позволяет повысить безотказность и безопасность различных АСУ ТП за счёт снижения вероятности опасных отказов.

Сравнивая величины вероятности исправности, можно сделать вывод, что применение системы позволяет повысить безотказность главной функции. Учитывая введение в структуру блокирующих опасности модулей, сделан вывод о том, что опасные отказы блокируются, а определяя вероятность безотказной работы опасных модулей, делается вывод о том, что системой достигается необходимый уровень интегральной безопасности, и следовательно, анализируемая АСУ ТП становится безопасной. Таким образом, цель данного исследования достигнута путем разработанной автоматизированной системы анализа, которая обеспечивает построение надежной структуры АСУ ТП с высокой безотказностью и безопасностью. Проведена проверка работы системы анализа надежности на примере АСУ ТП процесса получения поликарбоната и АСУ ТП процесса испытаний по результатам которой получено повышение безотказности до 7,8% и 4,7% соответственно.

Публикации в изданиях, рекомендованных ВАК РФ:

1. Кузнецов П. А. Модификация метода последовательной оценки и отсеивания вариантов структурно-сложных объектов АСУ / П.А. Кузнецов, Н.А. Бесчастная, К. К. Бахмарева, О.А. Антамошкин, А.Н. Антамошкин // Вестник СибГАУ. 2012. – Вып. 6 (46). С. 97-100.

2. Кузнецов П. А. К вопросу анализа эффективности систем с полным резервированием / П.А. Кузнецов // Вестник СибГАУ. 2015. – Т. 16. № 2. С. 326-331.

3. Кузнецов П.А. К вопросу оценки надежности АСУ с блокирующими модулями защиты / И.В. Ковалев, П.А. Кузнецов, П.В. Зеленков, В.В. Шайдуров, К.К. Бахмарева. Приборы. 2013. – Вып. 6. С. 20-24.

4. Кузнецов, П.А. Зависимые отказы в многофункциональных автоматизированных системах управления // Вестник СибГАУ. 2015. – Т. 16. № 1. С. 86-91.

5. Кузнецов, П.А. К вопросу о состояниях работоспособности структурно-сложных систем автоматического управления / П.А. Кузнецов, Д.И. Ковалев, В.В. Лосев, А.О. Калинин // Вестник СибГАУ. 2015. – Т. 16. № 4. С. 941–945.

В изданиях, входящих в базу SCOPUS

6. Dependent failure in multifunctional automatic control systems / Kuznetsov P.A., Usakov V.I., Kovalev, I. V., Et al // IOP Conference Series: Materials Science and Engineering. 2018. – 450(3).

7. Genetic algorithms of physical modelling with postcrossover survival / Kuznetsov P.A., Karaseva T. S., Kovalev I. V. Et al. // IOP Conference Series: Materials Science and Engineering. 2018. – 450(4).

8. To the question of the organization of a learning environment for developers of cross-platform on-board software for unmanned aerial vehicles/ Kuznetsov P.A., Losev V.V., Saramud M.V. Et al // Turkish Online Journal of Educational Technology. 2017. – С. 700-705.

9. To the question about the states of workability for automatic control systems with complicated structure / Kuznetsov P.A., Kovalev I.V., Losev V.V. Et al // IOP Conference Series: Materials Science and Engineering. 2016. – 122(1).

10. Dangerous failures in multifunctional systems / Kuznetsov P.A., Kovalev I.V., Zelenkov P.V. // IOP Conference Series: Materials Science and Engineering. 2015. – 94(1).

В других изданиях:

11. Кузнецов П.А. Реализация метода Волковича и Михалевича при проектировании системы автоматического регулирования параметра технологического процесса [Электронный ресурс] Режим доступа http://econf.rae.ru/article/6855 (дата обращения: 18.06.2012).

12. Кузнецов П.А. Модификация метода последовательной оценки и отсева вариантов структурно-сложных объектов АСУ / П.А. Кузнецов // Сборник статей по итогам Всероссийской научно-практической конференции «Молодые ученые в решении актуальных проблем науки». В 3 т. 2013. – Т. 2. С. 247-252.

13. Кузнецов П.А. Надежность и безопасность АСУ / П.А. Кузнецов // Сборник статей по материалам Всероссийской научно-практической конференции «Лесной и химический комплексы - проблемы и решения» Красноярск. В 2 т. 2013. – Т. 2. С. 171-174.

14. Кузнецов П.А. Надежность АСУ ТП с учетом её функциональности / П.А. Кузнецов, И.В. Ковалев // X Всероссийская научно-практическая конференция творческой молодежи «Актуальные проблемы авиации и космонавтики». В 2 т. 2014. – Т. 1. С. 316-317.

15. Кузнецов П.А. Опасные отказы в АСУ ТП. / П.А. Кузнецов // Сборник материалов IV Международной молодежной научно-практической конференции

«Научные исследования и разработки молодых ученых», Новосибирск. 2015. – С. 97-101.

16. Кузнецов П.А. Надежность АСУ ТП с учетом её функциональной направленности / П.А. Кузнецов, В.В. Храпунова, С.В. Ефремова, Н.Н. Голоскокова // Материалы Международной научно-практической конференции «Актуальные задачи математического моделирования и информационных технологий», г. Сочи. 2015 – С. 77-80.

17. Кузнецов П.А. Зависимые отказы в многофункциональных АСУ / П.А. Кузнецов // Вестник СибГАУ. 2015 г. Вып. 1 (16). – С. 86-96.

Зарегистрированные программные системы

18. Ковалев И. В., Зеленков П. В., Ковалев Д. И., Кузнецов П. А., Прохорович Г. А. Анализатор надежности АСУ. Свидетельство о государственной регистрации программы для ЭВМ №2015660981 от 14.10.2015.

Кузнецов Петр Анатольевич

Автоматизированная система анализа надежности АСУ ТП опасных производств

Автореферат
Подписано к печати 11.10.19. Формат 60х84/16
Уч. изд. л. 1.0 Тираж 100 экз. Заказ № _____
Отпечатано в отделе копировальной и множительной техники
СибГУ им. М.Ф. Решетнева.
660037, г. Красноярск, пр. им. газ. «Красноярский рабочий», 31