Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева»

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)

ДИССЕРТАЦИЯ

на соискание ученой степени кандидата технических наук

Научный руководитель
кандидат технических наук
Лосев В.В.

Красноярск – 2019

Оглавление

Введение

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 российских учёных, таких, как д.т.н. Соложенцев Е.Д., д.т.н. проф. Рябинин И.А., д.т.н. проф. 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, понижая вероятность опасных отказов в АСУ ТП.

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.

Реализация результатов работы. Диссертационная работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках государственного задания №2.2867.2017/ПЧ.

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 17 научных публикациях, в том числе в ведущих рецензируемых научных изданиях,

рекомендуемых ВАК, – 5 статей.

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

1 Исследование существующих подходов к анализу и повышению параметров надежности технических систем

Автоматизированные системы управления являются важной составной частью промышленного производства.

АСУ ТП – это системы, включающие в себя на каком-то участке своей работы человека и обеспечивающие автоматизированный сбор и обработку информации, а также управление технологическим процессом. В отличие от автоматических систем, автоматизированная система управления предполагает активное участие человека, что обеспечивает необходимую гибкость и адаптивность АСУ ТП.

1.1 Специфика автоматизированных систем

Анализируя упрощенную структурную схему переработки данных в АСУ ТП (рисунок 1.1), можно сделать вывод, что этапы 1, 2, 3, 4, 8, 9 в своем составе могут содержать много операций, которые не требуют творческого участия человека и, следовательно, могут быть выполнены техническими средствами.

Следует говорить не о вытеснении человека из процесса управления технологическим процессом, а о рациональном распределении функций между человеком и техническими средствами, освобождающем человека от решения рутинных задач и возлагающем на него задачи, решение которых требует творчества. Существенными признаками АСУ ТП является наличие больших потоков информации, сложной информационной структуры. Общими свойствами и отличительными особенностями АСУ ТП как сложных систем являются следующие[51,52]:

– наличие множества элементов;

– многофункциональность элементов и системы;

– элементы в процессе взаимодействия обмениваются информацией, энергией, материалами и др.;

– наличие у всей системы общей цели;

– взаимодействие элементов в системе и с внешней средой в большинстве

случаев носит стохастический характер.

Рисунок 1.1 – Структура автоматизированной системы управления

Информационное обеспечение АСУ ТП

Информационное обеспечение АСУ ТП включает:

– исходные данные, используемые в процессе разработки или эксплуатации системы;

– промежуточные данные, хранящиеся в базах данных реального времени, используемые для дальнейшей обработки;

– выходные данные, передаваемые для реализации на исполнительные устройства, отображаемые визуально на панелях операторов, табло и мониторах рабочих станций, передаваемых пользователям в электронном или бумажном виде;

– принятые формы входных и выходных документов (электронных или бумажных);

– принятая система кодирования информации;

– электронные архивы данных.

В состав информационного обеспечения АСУ ТП входят внемашинные (на бумажных носителях) и внутримашинные (на электронных носителях) компоненты. Так, например, к внемашинным компонентам информационного обеспечения АСУ ТП можно отнести технологический регламент, определяющий допустимые пределы изменения технологических параметров, условия аварийных отключений, порядок пуска и останова оборудования и т.п. К внутримашинному информационному обеспечению АСУ ТП относятся входные сигналы, поступающие от датчиков, а также выходные сигналы на исполнительные устройства, архивы нарушений технологического регламента, графики изменений контролируемых параметров, сформированные на экране монитора и т.п.

В зависимости от роли человека в процессе управления все системы можно разделить на два класса:

1. Информационные системы, обеспечивающие сбор и выдачу в удобном виде информации о ходе технологического или производственного процесса. В результате соответствующих расчетов определяют, какие управляющие воздействия следует произвести, чтобы процесс протекал наилучшим образом. Основная роль принадлежит человеку, а машина играет вспомогательную роль, выдавая для него необходимую информацию;

2. Управляющие системы, которые обеспечивают наряду со сбором информации выдачу непосредственно команд исполнителям или исполнительным механизмам. Управляющие системы работают обычно в реальном масштабе времени, то есть в темпе технологических или производственных операций. В управляющих системах важнейшая роль принадлежит машине, а человек контролирует и решает наиболее сложные вопросы, которые по тем или иным причинам не могут решить вычислительные средства системы.

Цель таких систем – получение оператором информации с высокой достоверностью для эффективного принятия решений. Характерной особенностью для информационных систем является работа ЭВМ в разомкнутой

схеме управления [26, 45, 46, 47].

При непосредственном выборе и проектировании программно-технического комплекса часто рассматривается только центральная часть системы – основное оборудование автоматизированных систем. При этом совершенно упускается из виду общая надежность контуров управления и защиты – функций безопасности, – начиная от датчиков и заканчивая исполнительными устройствами.

Стадии жизненного цикла АСУ

Ключевым аспектом современного подхода является концепция жизненного цикла**,** определяющая все этапы существования системы от зарождения идеи до списания. Современные стандарты дают возможность перейти от интуитивных представлений о достаточности той или иной архитектуры к количественным оценкам вероятности отказа и дают соответствующие соотношения, позволяющие определить интегральную безопасность системы. В последние годы появились отечественные нормативные документы по анализу рисков и оценке последствий отказов [27, 28, 50, 60, 126].

Таким образом, появляется формальная основа для предъявления требований к поставщикам оборудования и разработчикам систем, соответствие которым будет обеспечивать приемлемый уровень риска в реальных обстоятельствах [30, 34, 36]. Главные вопросы, на которые необходимо получить ответ, прежде чем приступить к реализации конкретного проекта, состоят в следующем:

1. Как обрести уверенность, что система обеспечит безопасность, то есть действительно выполнит заложенные функции защиты, когда в этом возникнет необходимость?

2. Как должна быть построена система, чтобы исключить возможность ложных, немотивированных остановок процесса по вине оборудования системы [55, 56, 57, 61, 75]?

Жизненный цикл процесса создания автоматизированных систем согласно ГОСТ 34.601-90 [4] включает следующие стадии:

– формирование требований к автоматизированной системе;

– разработка концепции автоматизированной системы;

– техническое задание;

– эскизный проект;

– технический проект;

– рабочая документация;

– ввод в действие;

– сопровождение автоматизированной системы.

Полный перечень документации, разрабатываемой на данных стадиях создания автоматизированной системы, приводится в ГОСТ 34.201-89.

На начальном этапе создания АСУ ТП согласно требованиям [40] необходимо проведение обследования объекта автоматизации. В рамках обследования происходит сбор и анализ данных об организации, производственной структуре и функционировании объекта автоматизации. Источником для получения данных сведений могут послужить устав и регламенты организации, а также общегосударственные законы, постановления и другие нормативно-правовые акты.

Обследование также должно включать анализ автоматизированных систем, уже функционирующих в рамках объекта автоматизации. На данном этапе необходимо также определить степень интеграции создаваемой АСУ ТП с существующими системами. Кроме того, должен быть проведен сбор и анализ сведений о зарубежных и отечественных аналогах, создаваемой АСУ ТП.

Таким образом, возникает необходимость выявить на базе полученных данных основные функциональные и пользовательские требования к АСУ ТП.

1.2 Разработка концепции АСУ ТП

Исходя из результатов проведенных исследований объекта автоматизации, согласно [40] разрабатывается несколько вариантов концепций АСУ ТП, удовлетворяющих требованию пользователей. Концепции АСУ ТП могут быть представлены заказчику в виде отчета о выполненных работах, отдельного

документа «Концепция АСУ ТП» или стать частью аналитического отчета.

Ключевая роль при создании АСУ ТП отводится именно разработке и согласованию технического задания, так как он должен определять требования и порядок разработки, развития и модернизации системы. В соответствии с данным документом должны будут проводиться работы по испытанию и приемке системы в эксплуатацию. Техническое задание может быть разработано как на систему в целом, так и на ее части [13].

Стандартом для разработки данного документа является [51], регламентирующий содержание разделов и стиль изложения в техническом задании (ТЗ).

Полный перечень документации, разрабатываемой на данных этапах создания АС, приводится в [52].

Зачастую создание полного пакета документов эскизного и технического проекта является нецелесообразным. Поэтому минимальный комплект документации согласовывается с заказчиком и фиксируется в техническом задании на создание АСУ ТП.

Именно на этапе построения проекта и выполняется формирование структуры системы, а, следовательно, обеспечение ее надежности путем применения технических средств.

От правильной работы АСУ ТП зачастую зависит не только эффективность управления, но и зачастую здоровье и жизнь персонала [38].

При работе АСУ ТП могут возникать отказы, приводящие к снижению эффективности их работы.

Для повышения эффективности АСУ ТП следует изучить процессы возникновения отказов.

1.3 Свойства, причины и последствия отказов

Выражения для показателей эффективности, учитывающие широкий круг действующих на изделие внутренних и внешних факторов, как правило, весьма сложны. Расчет таких показателей требует переработки большого объема

информации и поэтому проводится при выборе облика будущего изделия, а также при окончательной оценке технического уровня созданного изделия. В процессе разработки, изготовления и эксплуатации изделия используют обычно частные показатели эффективности. Так, главным показателем эффективности функционирования систем управления является точность.

В процессе эксплуатации технических систем возможны различного вида отказы, приводящие к снижению эффективности. Обусловленное этими отказами снижение эффективности характеризуется надежностью. Таким образом, надежность является более частной характеристикой, чем эффективность.

Наиболее универсальным показателем надежности является вероятность безотказной работы изделия при определенных условиях. Для получения численных значений показателя надежности необходимо определить понятие отказа. Понятие отказа допускает большое разнообразие интерпретаций. Для конкретизации этого понятия вводят понятие условной эффективности, то есть эффективности, полученной при отказе того или иного компонента изделия.

По мере накопления отказов компонентов эффективность изделия снижается [56, 61, 131]. Снижение эффективности может происходить постепенно либо скачком. Примером постепенного снижения эффективности может служить увеличение погрешности позиционирования промышленного робота или системы численно-программного управления (ЧПУ) станка при некритических отказах в системе управления. В качестве примера скачкообразного снижения эффективности можно привести изменение характеристики резервированной системы при отказе резервных компонентов.

Изделия, эффективность которых при отказе равна нулю, называются простыми. Постепенное снижение эффективности характерно для сложных изделий. Для определения отказа сложного изделия необходимо задать допустимую границу снижения эффективности. Тогда состояние выхода ее значений за эту границу можно считать отказом. Так, например, может быть задано предельное значение погрешности позиционирования. Изделия, в которых может быть задана допустимая граница эффективности, называют квазипростыми.

Их надежность определяется вероятностью безотказной работы. Однако существует большое число изделий, для которых указать строго границу допустимой области нельзя. Так, например, при поломке робота в производственном модуле подача заготовок может производиться вручную, то есть отказа модуля не происходит. Для отказов по общей причине на разных этапах «жизненного» цикла установки характерны следующие признаки.

На стадии проектирования:

1) функциональные недостатки автоматических защитных систем:

– отсутствие индикации приближения опасности отказа из-за недостаточного знания динамики процессов;

– неадекватность показаний вследствие неправильного диапазона измерения или неточности контрольно-измерительных приборов;

– неадекватность управления, когда действия защитных систем недостаточны для выполнения возложенных на них функций;

2) недостатки схемно-конструкторских решений:

– зависимость элементов от первоначально неопознанных электрических, механических и других зависимостей, включая общий элемент или общую вспомогательную систему;

– общий дефект в разработке отдельных элементов;

– зависимость от других систем;

– общие элементы для систем;

– неодинаковые элементы от неправильной подборки их по точности, надежности, времени работы;

– недостатки в проработке эксплуатационных операций;

– ошибки в чертежах, спецификациях, расчетах, программах и т.д.;

– ошибки, связанные с неправильной трактовкой документации, недостаточной взаимосвязью между разработчиками или отступлением от стандартов.

В процессе изготовления и монтажа:

– недостаточный контроль качества изделий;

– нарушение действующих норм и правил;

– недостаточный объем проверок и испытаний;

– ошибки человека в процессе проведения работ;

– воздействие окружающей среды или другого оборудования.

На стадии эксплуатации:

– ошибки эксплуатационного персонала в процессе обслуживания и испытаний: незавершенный ремонт, несовершенные проверки оборудования, калибровки и испытаний, неполнота регламента;

– ошибки оператора: неправильные действия или пропуск действия согласно установленным инструкциям, непрямая ошибка из-за несовершенства инструкций, недостаточные наблюдения;

– влияние окружающей среды – условий, как входящих в пределы, ограниченные проектом, так и не входящих в эти пределы (температура, давление, вибрация, ускорение, коррозия, загрязнение, радиация, статический разряд), и внезапные внешние и внутренние воздействия (пожар, погодные условия).

Классификация производств

Производства, на которых протекают технологические процессы, управляемые автоматизированными системами, различаются по множеству показателей.

В зависимости от степени сложности технологического процесса все производства подразделяются на два типа – простые и сложные.

К простым относятся производства, вырабатывающие однородную продукцию (например, добыча угля, выработка электроэнергии и тепловой энергии, лесопильное производство и т.п.). Технологический процесс в таких производствах представляет собой единый процесс, в котором незавершенное производство либо отсутствует, либо имеет незначительные и стабильные размеры, которые при исчислении себестоимости продукции обычно во внимание не принимаются.

Наиболее типичными представителями простых производств являются отрасли добывающей промышленности и производства, вырабатывающие

энергию.

К сложным относятся производства, в которых технологический процесс состоит из ряда самостоятельных стадий, переделов, фаз, в процессе которых исходное сырье последовательно превращается в готовый продукт. В этих производствах продукты каждой стадии (фазы, передела) выступают как полуфабрикаты на последующих стадиях обработки.

Как правило, сложные производства характерны для отраслей обрабатывающей промышленности – металлургической, текстильной, химической, стекольной, машиностроительной и т.п.

Множество технологических производств используют вещества и энергии, способные при возникновении аварийной ситуации нанести ущерб персоналу и инфраструктуре. Данные производства определяются Федеральным законом от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов» как опасные.

В соответствии с ним к опасным производственным объектам (далее – ОПО) относятся предприятия или их цеха, участки, площадки, а также иные производственные объекты, на которых получаются, используются, перерабатываются, образуются, хранятся, транспортируются, уничтожаются опасные вещества:

– воспламеняющиеся вещества – газы, которые при нормальном давлении и в смеси с воздухом становятся воспламеняющимися и температура кипения которых при нормальном давлении составляет 20 градусов Цельсия или ниже;

– окисляющие вещества – вещества, поддерживающие горение, вызывающие воспламенение и (или) способствующие воспламенению других веществ в результате окислительно-восстановительной экзотермической реакции;

– горючие вещества – жидкости, газы, способные самовозгораться, а также возгораться от источника зажигания и самостоятельно гореть после его удаления;

– взрывчатые вещества – вещества, которые при определенных видах внешнего воздействия способны на очень быстрое самораспространяющееся химическое превращение с выделением тепла и образованием газов;

– токсичные вещества – вещества, способные при воздействии на живые организмы приводить к их гибели.

Также опасным считается производство, если на нём:

– используется оборудование, работающее под избыточным давлением более 0,07 мегапаскаля;

– используются стационарно установленные грузоподъемные механизмы (за исключением лифтов, подъемных платформ для инвалидов), эскалаторы в метрополитенах, канатные дороги, фуникулеры;

– получаются, транспортируются, используются расплавы черных и цветных металлов, сплавы на основе этих расплавов с применением оборудования, рассчитанного на максимальное количество расплава 500 килограммов и более.

Согласно действующим нормативным актам, в частности, стандарту МЭК 61508/МЭК 61511 следует обеспечивать безопасность указанных производств.

Оценкой безопасности производства является его уровень интегральной безопасности (SIL).

Количественной оценкой происходящих во время выполнения технологического процесса отказов и их последствий будут показатели надежности.

1.4 Надежность и показатели надежности

Каждый сложный объект с течением времени изменяет свое состояние, переходит из одного в другое. Подобный переход сопровождается изменениями качеств. Качество любого изделия – это совокупность его свойств, обуславливающая пригодность для удовлетворения определенных потребностей в соответствии с назначением этого изделия.

Качество функционирования технических систем определяется различными показателями. И одним из таких показателей является надежность – свойство объекта сохранять по времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения. Это сложное свойство,

складывающееся в общем случае из таких составляющих, как безотказность, долговечность, ремонтопригодность и сохраняемость изделия.

Состояние объекта, при котором он соответствует всем требованиям нормативно-технической и конструкторской документации, является исправным состоянием. Работоспособное состояние – это состояние, в котором значения всех технических параметров и качеств, характеризующих способность выполнить заданные функции, соответствует требованиям нормативно-технической и конструкторской документации. Если значение хотя бы одного из этих параметров объекта не соответствует указанным требованиям, то объект находится в неработоспособном состоянии. Переход объекта в неисправное, но работоспособное состояние называют повреждением, а в неработоспособное – отказом. Как и повреждения, так и отказы возникают в результате воздействия на систему многих факторов, таких как время работы системы, нагрузка, накладываемая на нее, условия ее работы и другие [28,102].

Работоспособный объект, в отличие от исправного, должен удовлетворять лишь требованиям документации, выполнение которых обеспечивает нормальное применение объекта по назначению. С понятием «отказ» связана такая важнейшая составляющая надежности, как безотказность – свойство объекта непрерывно сохранять работоспособное состояние в течение какого-либо времени [42]. Продолжительность или объем работы, выполненной объектом, называется наработкой. Наработка может измеряться в единицах времени или объема выполненной работы. Наработка объекта от начала его работы до первого отказа называется наработкой на отказ.

Переход объекта из неработоспособного состояния в работоспособное происходит в результате выполнения операций восстановления или ремонта. Объект, для которого восстановление работоспособного состояния в рассматриваемой ситуации предусмотрено технической документацией, называется восстанавливаемым. В противном случае объект называется невосстанавливаемым.

Ремонтопригодность – свойство объекта, заключающееся в

приспособленности к предупреждению и обнаружению причин возникновения отказов, поддержанию и восстановлению работоспособного состояния путем проведения технического обслуживания и ремонта. Долговечность – свойство объекта сохранять работоспособное состояние до наступления предельного состояния – состояния объекта, при котором его дальнейшее применение по назначению недопустимо.

Одним из важнейших средств обеспечения заданного уровня надежности объекта является резервирование. Резервирование – это применение дополнительных мер для сохранения работоспособного состояния объекта при отказе одного или нескольких его элементов. Применение резервирования является одной из самых распространенных мер повышения надежности оборудования [3, 65, 76, 79].

При использовании понятия надежности в инженерной практике возникает необходимость введения ее количественной оценки, удобной для расчетов, сравнения надежности различных вариантов технических решений. Для этого используются единичные и комплексные показатели надежности – количественные характеристики одного или нескольких свойств.

Такие события, как отказ или восстановление работоспособного состояния объекта, являются случайными событиями. Наработка до отказа объекта, время восстановления – случайные величины.

Последовательности отказов и восстановлений, возникающие в процессе эксплуатации объекта, образуют потоки случайных событий и в качестве показателей надежности используются многие из тех количественных характеристик случайных событий, величин и процессов, которые применяются в теории вероятностей. Однако теория надежности не является подразделом теории вероятностей. Ее инженерный характер заключается прежде всего в повышении надежности. В теории надежности применяются методы теории вероятностей, но они модифицируются для обеспечения как оценки, так и повышения вероятности безотказной работы.

В общем случае это заключается в максимизации и обратном вычислении

формул оценки надежности по свойствам систем.

Наработка до отказа невосстанавливаемого объекта является случайной величиной, для которой исчерпывающей количественной характеристикой является ее функция распределения $F(t)$.

Эта функция обладает следующими свойствами:

$F(t) = 0$ при $t = 0$, так как изучение устройства начинается, когда оно исправно, и отказ за очень малое время маловероятен.

$F(t) \to 1$ при $t \to \infty$, так как любое техническое средство рано или поздно отказывает, и значит, при неограниченном увеличении времени вероятность отказа стремится к единице.

$F(t)$ как всякая функция распределения является неубывающей функцией [27, 81, 83].

Также можно ввести понятие «вероятность отказа», определив его как вероятность того, что объект откажет в течение заданного времени, будучи работоспособным в начальный момент времени.

Для вероятности отказа $Q(t)$ в интервале от 0 до t справедливо выражение

$$Q(t) = F(t) \tag{1.1}$$

Вероятность безотказной работы определяется выражением

$$P(t) = 1 - F(t) \tag{1.2}$$

Показателем надежности невосстанавливаемых объектов является также интенсивность отказов – условная плотность вероятности возникновения отказа невосстанавливаемого объекта, определяемая для рассматриваемого момента времени при условии, что до этого момента отказ не возник. Интенсивность отказов $\lambda(t)$ определяется как отношение плотности распределения $F(t)$ к вероятности безотказной работы.

Плотность распределения определяется как производная от $F(t)$ по времени. Зависимость интенсивности отказов от времени показывает характер работы технических систем по времени.

Период работы устройства подразделяется на три участка. На первом интенсивность отказов высока, этот участок называют участком приработки, на

нем выявляются производственные дефекты. На втором интенсивность отказов постоянна, этот участок называется участком нормальной эксплуатации. На третьем интенсивность отказов растет из-за усиления процессов старения и износа.

Для определения надежности объекта на участке нормальной эксплуатации достаточно указать одно число λ, и в связи с этим интенсивность отказов используется в качестве основного показателя надежности элементов.

Для оценки надежности восстанавливаемых объектов применяются как единичные показатели, характеризующие только безотказность или только ремонтопригодность, так и комплексные показатели, которые являются обобщенной оценкой обоих этих свойств.

Время восстановления работоспособного состояния $t_в$, как правило, является случайной величиной. Поэтому вероятностными характеристиками $t_в$ являются функция распределения времени восстановления $f(t_в)$ и плотность распределения времени восстановления $f_в(t)$.

В качестве показателей ремонтопригодности используются вероятность восстановления работоспособного состояния – вероятность того, что время восстановления работоспособности объекта не превысит заданного, и среднее время восстановления работоспособного состояния – математическое ожидание времени восстановления.

По аналогии с интенсивностью отказов для восстанавливаемых объектов можно ввести понятие «интенсивность восстановлений» – условная плотность распределения времени восстановления до момента t при условии, что до этого момента восстановление объекта не произошло.

При $\lambda\ (t)$ = const получаем экспоненциальное распределение времени восстановления [83].

В качестве показателей безотказности применяются: средняя наработка на отказ – отношение наработки восстанавливаемого объекта к математическому ожиданию числа его отказов в течение этой наработки, и параметр потока отказов – отношение среднего числа отказов восстанавливаемого объекта за произвольно

малую его наработку к значению этой наработки [46].

Наиболее универсальной характеристикой сложной технической системы (СТС) принято считать эффективность, понимая под этим степень приспособленности системы к выполнению заданных ей функций [40-46]. Эффективность СТС зависит от ряда показателей или параметров. Основные из них: стоимость разработки, изготовления и эксплуатации изделия, качество функционирования, мощность потребляемой энергии, масса, габариты, условия нормального функционирования и др.

Кроме этого, эффективность изделия зависит от его структуры, характера связей между элементами, вида управляющих алгоритмов и ряда других закономерностей функционирования, не поддающихся описанию при помощи указанных параметров. Так, эффективность промышленного робота характеризуется грузоподъемностью, мощностью привода, развиваемыми скоростью и ускорением, точностью позиционирования, объемом памяти управляющего устройства, числом степеней свободы, числом технологических переделов, которые может осуществлять данный робот, стоимостью. Эффективность автоматизированной производственной системы характеризуется стоимостью всех видов оборудования, надежностью технических средств, быстродействием технических средств, численностью обслуживающего персонала, числом управляющих программ, производительностью, коэффициентом загрузки технологического оборудования, гибкостью, рентабельностью, живучестью, длительностью производственного цикла. Эффективность средств вычислительной техники характеризуется объемом памяти – оперативной и запоминающего устройства, качеством визуального отображения, числом каналов связи, стоимостью.

Методы повышения надежности

Приведённые выше показатели надежности следует повышать для повышения общей эффективности работы АСУ ТП.

На стадиях жизненного цикла АСУ ТП возможно применение различных методов повышения показателей надежности.

На этапе разработки возможно:

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

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

На этапе эксплуатации возможно:

1. Улучшение условий эксплуатации системы. Т.е. 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.

Рассматривая данные методы подробней, можно выделить принципы, обеспечивающие повышение показателей надежности.

1. Принцип безопасных отказов, предусматривающий:

– разработку таких систем, чтобы отказы по общей причине носили безопасный характер;

– безопасные размыкания цепей, короткие замыкания и отказы заземления в кабельных системах;

– специальную разработку переключений и ручных отключений;

– возможность нахождения резервных элементов в «горячем резерве»;

– выявление потенциально опасных отказов по общей причине, приводящих к другому безопасному уровню эксплуатации;

– контроль калибровки, исключающей возможность отказов по общей причине;

2. Принцип защиты и разделения оборудования, включая:

– физическую защиту избыточных элементов от внешних и внутренних воздействий;

– исключение общих элементов в резервированных системах;

– применение разделения оборудования станции, кабелей, блочных щитов управления;

– разделение линий или схем, предотвращающих короткое замыкание и позволяющих проведение ремонта и контроля оператором;

– обеспечение отдельных кабельных линий и помещения для оборудования при его функциональном разнообразии;

– применение физического барьера там, где разделение не проходит компоновки;

– обеспечение достаточного количества средств пожаротушения для избыточных систем;

– защиту узлов, стыков, оборудования, кабелей и т.д. от таких воздействий, как течь пара или воды, нагревание, механическое воздействие, атмосферная коррозия и т.д.;

– защиту избыточных каналов от влияния электрических и магнитных полей.

3. Принцип упрощения. При этом:

– комплекты оборудования должны выдерживать большие нагрузки по сравнению с предельными значениями;

– при отборе оборудования необходимо рассматривать нагрузки, вызванные переходными процессами.

4. Принцип резервирования модулей системы [4, 56, 90].

Избыточность

Наиболее распространенным способом повышения надежности в данный момент является резервирование модулей и систем. Данный метод является универсальным, применимым к большому числу разновидностей систем. Методы построения систем с применением принципа резервирования описаны во множестве работ.

Резервирование может быть общим, когда резервируется система в целом, и раздельным (поэлементным), когда резервируются отдельные элементы

системы. В случае, когда в системе много однотипных элементов (например, модулей ввода сигналов термопар), число резервных элементов может быть в несколько раз меньше, чем резервируемых. Кратность резерва – отношение числа резервных элементов к числу резервируемых, которое выражается несокращаемой дробью. В частности, в соответствии с [42], кратность резерва 3:2 нельзя представлять как 1,5, и иногда используемый термин «полуторное резервирование» не соответствует стандарту. При сокращении дроби исчезает важная информация об общем количестве элементов в системе. Дублированием называют резервирование с кратностью резерва один к одному.

Постоянное резервирование (к нему относится мажоритарное резервирование и метод голосования) – резервирование с нагруженным резервом, при котором все N элементов в резервированной системе выполняют одну и ту функцию и являются равноправными, а выбор одного из N сигналов на их выходе выполняется схемой «голосования», без переключений. Постоянное резервирование позволяет получить системы с самым высоким коэффициентом готовности.

Применение метода резервирования осуществляется следующим образом.

Будем рассматривать систему, которая состоит из отдельных функциональных модулей. Отказ любого функционального модуля приводит к отказу всей системы в целом. Каждый модуль составлен из основного и резервных элементов. Возможные резервные элементы функциональных модулей подразделяются на типы, различающиеся показателями надежности и затратами ресурсов на их реализацию [89].

На построение резервированной системы отводится определенный набор ресурсов.

Требуется определить структуру системы, которая достигнет экстремум целевой функции $P(t)$ и обеспечивает успешное решение всех задач, поставленных перед системой, с вероятностями не ниже заданных ограничений, при этом затраты не должны превосходить заданной границы.

Целевая функция *P(t)* выражается как произведение вероятностей безотказной работы всех ее модулей.

$$P(t) = \prod_{i=1}^{n} P_i(t) \tag{1.3}$$

где *P(t)* – вероятность безотказной работы системы;

$P_i(t)$ – вероятность безотказной работы *i*-го модуля.

Ограничивающим степень резервирования фактором является запас ресурсов, выделяемый на построение системы:

$$L_i \geq \sum_{j=1}^{n} R_{i,j}, \tag{1.4}$$

где L_i – запас *i*-го ресурса, выделяемый на построение системы;

$R_{i,j}$ – количество *i*-го ресурса, израсходованного на *j*-й модуль;

i – порядковый номер типов ресурса;

j – порядковый номер модуля;

n – количество модулей [96].

Таким образом, имея целевую функцию и ограничения, мы сталкиваемся с задачей формирования оптимального состава резервированной системы.

Метод наискорейшего спуска

Методом решения задачи поиска оптимальной резервированной структуры АСУ ТП может являться метод покоординатного наискорейшего спуска с фиксированным шагом.

Метод наискорейшего спуска - это итерационный численный метод (первого порядка) решения оптимизационных задач, который позволяет определить экстремум (минимум или максимум) целевой функции.

В соответствии с рассматриваемым методом экстремум (максимум или минимум) целевой функции определяют в направлении наиболее быстрого возрастания (убывания) функции, т.е. в направлении градиента (антиградиента) функции. Градиентом функции в точке называется вектор, проекциями которого на координатные оси являются частные производные функции по координатам. Градиент в базовой точке строго ортогонален к поверхности, а его направление

показывает направление наискорейшего возрастания функции, а противоположное направление (антиградиент), соответственно, показывает направление наискорейшего убывания функции.

Метод наискорейшего спуска является дальнейшим развитием метода градиентного спуска. В случае последовательного соединения элементов системы наибольшее приращение суммарной безотказности обеспечивает резервирование самого ненадежного модуля [84, 90-92].

Повышение безотказности системы производится путем итерационного добавления резервного элемента в модуль с наименьшей вероятностью безотказной работы.

$$Ra_i = \frac{1}{P_i(t)} \tag{1.5}$$

Затем находится номер модуля, для которого эта функция максимальна, и в этот модуль добавляется резервный элемент. Далее происходит следующая итерация.

Общая надежность системы при повышении надежности отдельных элементов стремится к надежности тех элементов, чью надежность мы не повышаем. Элементы с меньшей надежностью становятся «узкими местами», лимитирующими надежность системы сверху [62, 97-99].

Применение данного метода позволяет эффективно повышать надежность системы.

В рассмотренном примере максимизируется вероятность безотказной работы. Данный показатель является важным, но не единственным показателем надежности. Специфические особенности автоматизированных систем должны учитываться в анализе их надежности. Следовательно, необходимо учесть анализируемые параметры и систематизировать их учет.

Выводы

1. Автоматизированные системы являются сложными техническими системами, в процессе работы которых могут возникать отказы, имеющие

последствия для работы производства, а также персонала и инфраструктуры. Вероятность отказов определяется показателями надежности системы.

2. Для повышения надежности применяются различные математические методы. Одним из таких методов является метод наискорейшего спуска. Целевой функцией данного метода могут являться различные величины, в том числе, традиционно, – вероятность безотказной работы каждого модуля.

3. Метод наискорейшего спуска, рассматривающий только вероятность безотказной работы, позволяет создавать структуру автоматизированной системы с избыточностью, что повышает ее безотказность. Но данный метод является недостаточно эффективным, он не учитывает множество особенностей автоматизированных систем управления.

4. Отказы, происходящие в системе, могут нести опасные последствия. Следует учитывать данные особенности при анализе надежности.

5. Существует возможность модифицировать метод наискорейшего спуска и сформировать на его основе систему анализа надежности.

2. Концептуальное описание системы

Для обеспечения еще большего повышения надежностных показателей очередность добавления резервных элементов в модули следует формировать с учетом дополнительных параметров.

Исследование надежности системы не должно ограничиваться рассмотрением надежности отдельных модулей. Рассмотрение должно охватывать систему целиком.

2.1 Введение многоатрибутивной декомпозиции.

Для обеспечения требуемого уровня надежности следует использовать методику многоатрибутивной декомпозиции, то есть, декомпозиции по различным атрибутам.

В многоатрибутивную декомпозицию включается декомпозиция компонентная, функциональная, декомпозиция по атрибуту «тип компонента» и декомпозиция по атрибуту «явление» (возникающее в системе). Функциональная декомпозиция важна, так как исследование надежности системы не должно ограничиваться рассмотрением надежности отдельных модулей. Рассмотрение должно охватывать систему целиком.

Надежность работы системы определяется сочетанием надежностей работы отдельных ее элементов. Возникает вопрос о характере этого сочетания. Как правило, одна система АСУ ТП выполняет несколько функций. Наряду с функцией контроля параметров объекта АСУ ТП может выполнять и иные функции. Для определения надежности системы необходимо определять, какие элементы участвуют в выполнении каких функций [130, 64].

Необходимо определять последовательности элементов, выполняющие ту или иную функциональную задачу. Данная процедура разделения имеющейся системы на подсистемы и компоненты называется декомпозицией.

Компонентная декомпозиция

Декомпозиция как процесс расчленения позволяет рассматривать любую исследуемую систему как сложную, состоящую из отдельных взаимосвязанных

подсистем, которые, в свою очередь, также могут быть расчленены на части. При декомпозиции каждое расчленение образует свой уровень (рисунок 2.1).

Исходная система располагается на нулевом уровне. После ее расчленения получаются подсистемы первого уровня. Расчленение этих подсистем или некоторых из них приводит к появлению подсистем второго уровня и т. д.

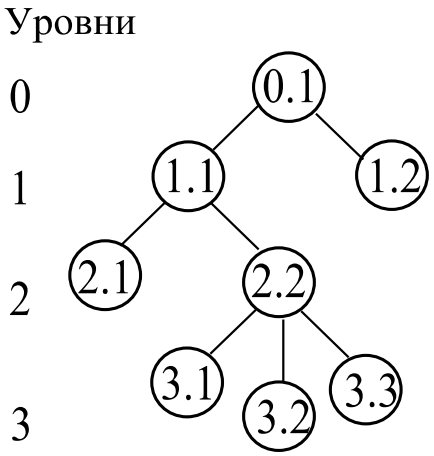


Рисунок 2.1 – Пример иерархической структуры

Упрощенное графическое представление декомпозированной системы называется ее иерархической структурой.

Иерархическая структура может быть изображена в виде ветвящейся схемы наподобие представленной на рисунке 2.1. Здесь на нулевом уровне располагается исходная система C_1, на следующих уровнях – ее подсистемы (число уровней и количество подсистем, показанных на рисунке, выбрано произвольно). С целью получения более полного представления о системе и ее связях в структуру включают надсистему и составляющие ее части (системы нулевого уровня, например, вторая система C_2) [56, 106].

Общий подход к решению проблем может быть представлен как цикл.

При этом в процессе функционирования реальной системы выявляется проблема практики как несоответствие существующего положения дел требуемому. Для решения проблемы проводится системное исследование (декомпозиция, анализ и синтез) системы, снимающее проблему. В ходе синтеза осуществляется оценка анализируемой и синтезируемой систем. Реализация синтезированной системы в виде предлагаемой физической системы позволяет

провести оценку степени снятия проблемы практики и принять решение на функционирование модернизированной (новой) реальной системы.

При таком представлении становится очевидным еще один аспект определения системы: система есть средство решения проблем.

Основные задачи системного анализа могут быть представлены в виде трехуровневого дерева функций (рисунок 2.2) [40].

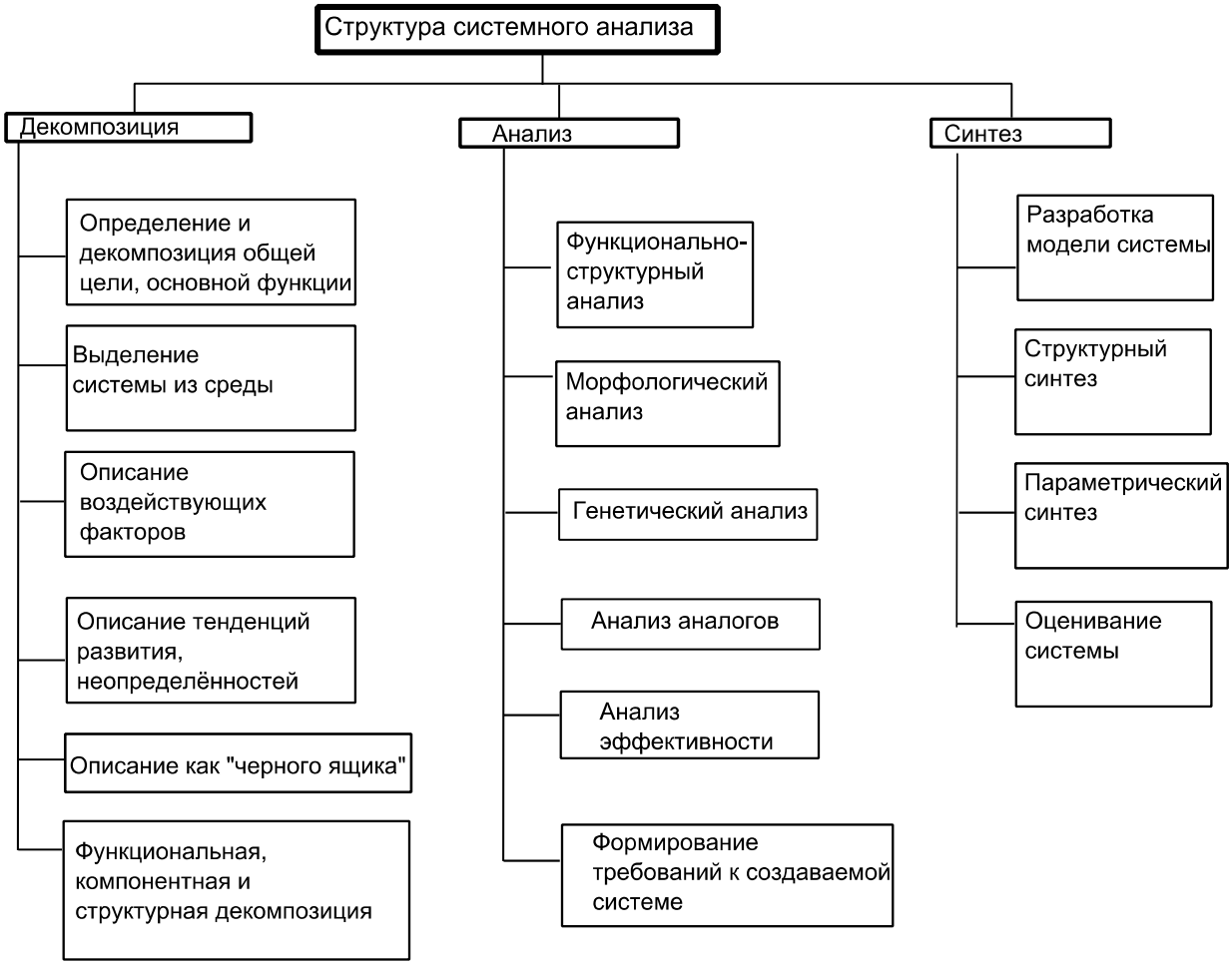


Рисунок 2.2 – Основные задачи системного анализа

На этапе декомпозиции, обеспечивающем общее представление системы, осуществляются определение и декомпозиция общей цели исследования и основной функции системы как ограничение траектории в пространстве состояний системы или в области допустимых ситуаций. Наиболее часто декомпозиция проводится путем построения дерева целей и дерева функций.

Глубина декомпозиции ограничивается. Декомпозиция должна прекращаться, если необходимо изменить уровень абстракции – представить элемент как подсистему. Если при декомпозиции выясняется, что модель начинает

описывать внутренний алгоритм функционирования элемента вместо закона его функционирования в виде «черного ящика», то в этом случае произошло изменение уровня абстракции. Это означает выход за пределы цели исследования системы и, следовательно, вызывает прекращение декомпозиции.

Декомпозиция по компонентам выделяет отдельные составные части АСУ ТП - её модули.

В общем случае компонент не является принципиально неделимым. Таким образом, возникает задача постановки предела декомпозиции.

Декомпозиция ограничивается путём установления признака выделения. Признак выделения отдельных компонентов - сильная связь между их деталями по одному из типов отношений (связей), существующих в системе (информационных, логических, иерархических, энергетических и т.п.). Силу связи, например, по информации можно оценить коэффициентом информационной взаимосвязи $\kappa = N/No$, где N – количество взаимоиспользуемых информационных массивов, $N0$ - общее количество информационных массивов. Для описания всей системы должна быть построена составная модель, объединяющая все отдельные модели. Рекомендуется использовать разложение на подсистемы, только когда такое разделение на основные части системы не изменяется. Нестабильность границ подсистем быстро обесценит как отдельные модели, так и их объединение.

То есть, границы отдельных компонентов будут задаваться связями между их частями.

Функциональная декомпозиция

Функциональная декомпозиция базируется на анализе функций системы. При этом ставится вопрос, что делает система, независимо от того, как она работает. Основанием разбиения на функциональные подсистемы служит общность функций, выполняемых группами элементов [80, 87].

В базовом методе предполагается декомпозиция до уровня единичных резервируемых функциональных модулей.

Предлагаемая глубина декомпозиции АСУ ТП ограничивается уровнем функциональных последовательностей. Данные последовательности представляют собой множества модулей, чья работоспособность необходима для выполнения определенной функции системы.

И каждая такая последовательность, обеспечивая выполнение своей части общей функции системы, вносит свою долю W_n в общий конечный продукт W.

$$W = W_1 + W_2 + \ldots + W_n \qquad (2.1)$$

Таким образом, исследование возможных состояний последовательностей показывает, насколько полно выполняется функция системы.

Для обеспечения выполнения выявленных функций применяются методы повышения надежности. Показателем, определяющим способность технического устройства, сооружения, средства или системы выполнять основные свои функции, несмотря на полученные повреждения, является живучесть. Это свойство системы, состоящее в ее способности противостоять крупным возмущениям за пределами, установленными для их штатного функционирования, не допуская последующего каскадного развития аварийных и катастрофических ситуаций. Живучая система при возникновении отказа в определенной последовательности элементов продолжает выполнять соответствующую функцию [13, 16, 80]. Сохранение функциональных возможностей системы обеспечивается широкой разветвленностью ее первичной сети, организацией обходных направлений и резервных каналов связи, использованием резервных средств. Как следует из названия данного показателя, живучесть играет большую роль при большей интенсивности воздействий, вызывающих отказы.

К каждой отдельной последовательности функции относятся элементы, при неисправности которых ее выполнение нарушается. При этом совершенно не обязательно, чтобы эти элементы располагались последовательно в структуре передачи информации.

В первую очередь функцией системы управления технологического процесса можно назвать получение какого-либо материального результата, выходного продукта, но также функцией АСУ ТП может быть и контроль над

определённым параметром, получение информации. Следовательно, количество выполняемых АСУ ТП функций определяется суммой количества выходов и количества элементов, выполняющих контроль параметров.

С точки зрения последствий отказа более важной является функция управления технологическим процессом. Функция контроля процесса является менее важной.

С учетом этого изменяется подход к определению надежностных показателей системы в целом.

Возможные состояния системы

Состояние всей системы выражается путем вычисления логической формулы системы, аргументами которой будут состояния отдельных элементов, входящих в функциональные последовательности.

Возможными состояниями системы привычно называются работоспособное и неработоспособное. Такой дуальный подход позволяет применять к расчету фактического состояния обыкновенную булевскую логику. Но такой набор состояний не является всеобъемлющим. Возможно предложить расширенное представление о состояниях элементов/системы.

Для оперирования разнообразными состояниями, конечно, нужно применять особую систему вычислений, хотя она во многом будет основана на привычной булевской логике. Отличием предлагаемой системы будет большее число возможных значений переменных состояния.

Для иллюстрации универсальности данного подхода рассмотрим несколько состояний V_1, V_2, V_3, в которых может пребывать как система, так и отдельные ее модули.

V_1 – неработоспособное состояние. В данном состоянии элемент полностью не выполняет свою функцию, и все его параметры не соответствуют требуемым.

V_2 – неисправное состояние изделия, при котором оно не соответствует хотя бы одному из требований нормативной технической и (или) конструкторской документации.

V_3 – состояние исправное. В нем объект соответствует всем требованиям нормативно-технической и конструкторской документации [65,80,96,110].

В зависимости от исправности той или иной функции определяется экономический эффект, приносимый системой.

Согласно этим определениям, система, не выполняющая какую-либо одну свою функцию, будет неисправна. Неисправная система находится в пограничном состоянии, которое может позволить выполнить ее цель.

Опишем последовательности выполнения системой функций, как приведено выше.

Для выполнения любым произвольно взятым устройством функции сбора информации о параметрах объекта необходимо, чтоб были исправны все устройства, управляющие объектом.

Количество последовательностей, выполняющих функции, должно учитываться при выборе приоритетного для резервирования модуля.

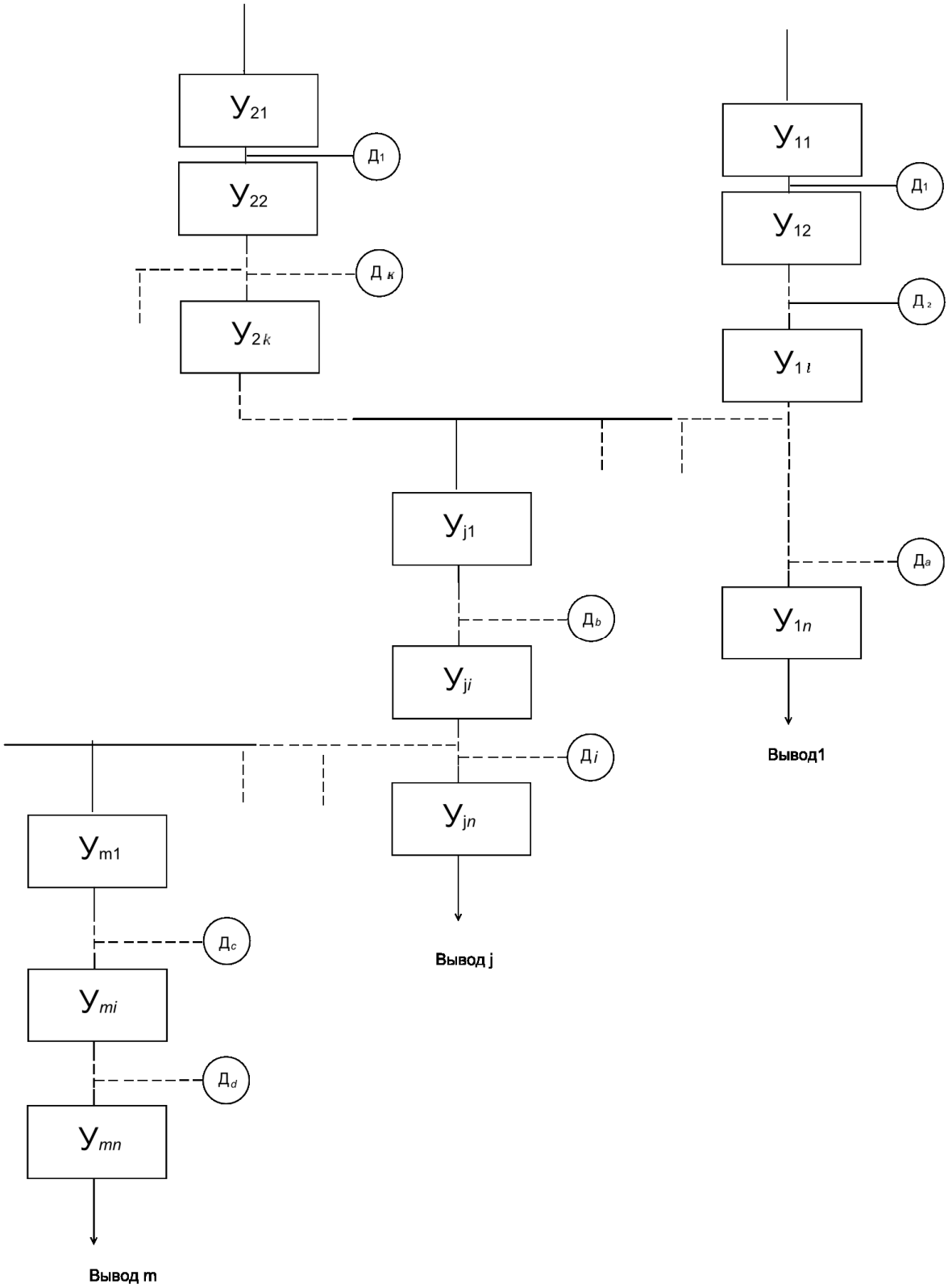


Рисунок 2.3 – Общий вид древовидной структуры

В случае представленного на рисунке 2.3 устройства сбора информации $Д_i$ вероятность того, что им будет выполняться его функция, равна произведению

вероятностей безотказной работы всех элементов, лежащих выше по процессу, учитывая все соединения материальных потоков.

Для приведенного элемента формула будет выглядеть как

$$P = \prod_{s=1}^{l} Д_{1s} \cdot \prod_{s=1}^{k} Д_{2s} \cdot \dots \cdot \prod_{s=1}^{i} Д_{js} \tag{2.2}$$

Аналогично, в случае устройства $У_{ji}$

$$P = \prod_{s=1}^{l} У_{1s} \cdot \prod_{s=1}^{k} У_{2s} \cdot \dots \cdot \prod_{s=1}^{i} У_{js} \tag{2.3}$$

Количество последовательностей, выполняющих функции, должно учитываться при выборе приоритетного для резервирования модуля.

Важность последовательностей, выполняющих функции, должна учитываться при выборе приоритетного для резервирования модуля. Этот учет может быть осуществлен путем введения коэффициента W, отражающего важность каждой функции.

Декомпозиция по типам модулей

Типизация модулей АСУ ТП осуществляется исходя из их свойств [59].

В общем виде чаще всего распределенные АСУ ТП имеют трехуровневую структуру.

На верхнем уровне с участием оперативного персонала решаются задачи диспетчеризации процесса, оптимизации режимов, подсчета технико-экономических показателей производства, визуализации и архивирования процесса, диагностики и коррекции программного обеспечения системы. Верхний уровень АСУ ТП реализуется на базе серверов, операторских (рабочих) и инженерных станций.

На среднем уровне — задачи автоматического управления и регулирования, пуска и останова оборудования, логико-командного управления, аварийных отключений и защит. Средний уровень реализуется на основе ПЛК (программируемых логических контроллеров).

Нижний (полевой) уровень АСУ ТП обеспечивает сбор данных о параметрах технологического процесса и состояния оборудования, реализует

управляющие воздействия. Основными техническими средствами нижнего уровня являются датчики и исполнительные устройства, станции распределенного ввода/вывода, пускатели, концевые выключатели, преобразователи частоты.

Входные сигналы от датчиков и управляющие воздействия на исполнительные механизмы могут подаваться непосредственно на ПЛК (поступать от ПЛК). Однако если ТОУ имеет значительную территориальную протяженность, это потребует длинных кабельных линий от каждого устройства к ПЛК. Такое техническое решение может оказаться не рациональным по двум причинам:

– высокая стоимость кабельной продукции;

– возрастание уровня электромагнитных помех с ростом длины линий.

Более рациональным в такой ситуации является использование станций распределенной периферии, располагающихся в непосредственной близости к датчикам и исполнительным механизмам. Такие станции содержат необходимые модули ввода и вывода, а также интерфейсные модули для подключения к ПЛК через цифровую полевую шину (например, с использованием протокола Profibus DP, или Modbus RTU).

Ввод-вывод сигналов от ПЛК осуществляется через сигнальные модули (модули ввода/вывода), использующие для передачи информации ту или иную модулированную физическую величину.

От типа модуля, от конкретной его природы зависят возможные причины его отказа и его последствия.

Декомпозиция по явлениям

Идентификация опасностей в процессе производственной деятельности – это процесс обнаружения, выявления и распознавания опасных и вредных производственных факторов и установления их количественных, временных, пространственных и других характеристик, необходимых и достаточных для разработки профилактических мероприятий (предупреждающих и корректирующих действий), обеспечивающих безопасность труда.

В процессе идентификации составляется номенклатура опасности и вредности рабочей среды и трудового процесса, проводится ранжирование негативных факторов, выявляются вероятность, частота и условия их проявления, причины, пространственная локализация, возможный ущерб здоровью людей и окружающей среде и другие параметры, необходимые для выработки защитных мер.

Для идентификации опасных и вредных производственных факторов можно применять следующие методы: «Что будет, если...?», проверочный лист, анализ опасности и работоспособности, анализ вида и последствий отказов, анализ «дерева отказов», анализ «дерева событий» и др. Источниками информации для выявления опасностей и вредностей являются [31,32]:

– нормативные правовые акты и нормативные технические документы, справочная и научная техническая литература, локальные нормативные акты и др.;

– протоколы, акты, справки и другие документы органов государственного контроля (надзора);

– результаты производственного контроля за соблюдением требований промышленной, экологической безопасности и санитарно-эпидемиологических требований;

– результаты специальной оценки условий труда;

– результаты санитарно-эпидемиологической опенки выпускаемой продукции;

– предписания специалистов по охране труда, представления уполномоченных лиц по охране труда, предложения комитета (комиссии) по охране труда;

– результаты наблюдения за технологическим процессом, производственной средой, рабочими местами, работой подрядных организаций, внешними факторами (дорогами, организацией питания, климатическими условиями и т.д.);

– результаты анализа анкет, бланков, опросных листов и т.д.;

– опыт практической деятельности;

– результаты многоступенчатого контроля за условиями и охраной труда.

Шаги методики многоатрибутивной декомпозиции и назначения важности имеют вид:

– Выявление компонентов АСУ ТП.

– Определение типов компонентов.

– Определение явлений, происходящих в АСУ ТП.

– Выявление последовательностей компонентов, исправность которых обеспечивает управление технологическими параметрами системы для получения продукта.

– Выявление последовательностей, исправность которых обеспечивает контроль технологических параметров системы.

– Назначение важности *W* выявленным функциям, исходя из необходимости их исправности и масштаба последствий, вызываемого прекращением выполнения этих функций.

– Последовательный перебор модулей и определение, в выполнении какой функции участвует очередной модуль. Если модули окночились – завершение.

– Если модуль участвует в выполнении функции управления – переход к пункту 10.

– Если модуль участвует в выполнении только функции контроля – переход к пункту 11.

– Назначение модулю важности, соответствующей функции управления. Переход к пункту 7.

– Назначение модулю важности, соответствующей функции контроля. Переход к пункту 7.

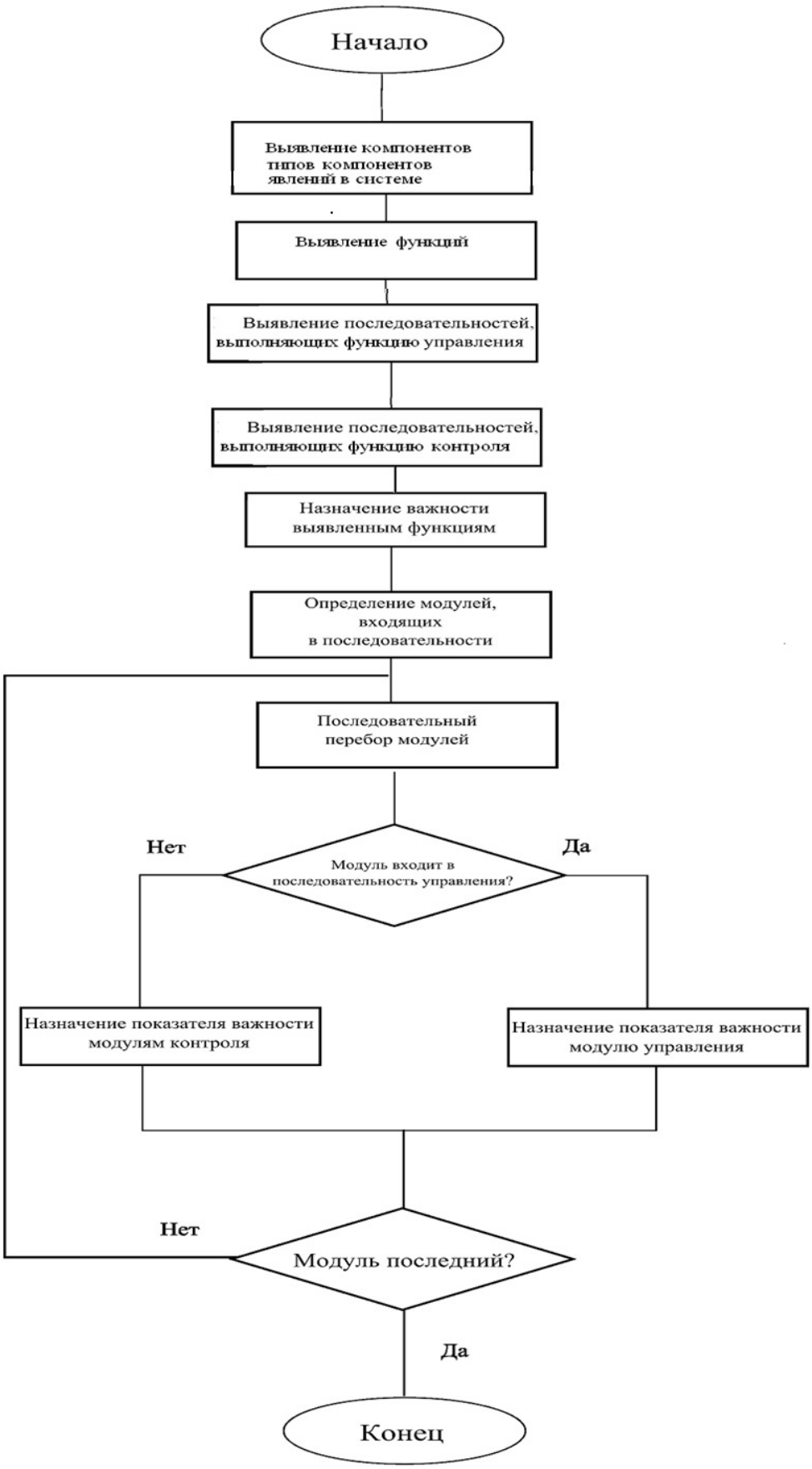


Рисунок 2.4 – Структурная схема методики декомпозиции АСУ ТП

Разработанная оригинальная методика декомпозиции АСУ ТП на функциональные последовательности с учетом важности позволяет оценить вероятности ее пребывания в различных состояниях.

Учет показателей важности модулей системы позволяет, во-первых, модифицировать порядок резервирования модулей, обеспечив более высокую надежность важных функций, а во-вторых, получить более точную оценку вероятности безотказной работы, выводя данные о безотказности не только всей системы, но и отдельно главной функции.

Данная методика обеспечивает повышение безотказности выбранных функций системы, но наряду с данным показателем при формировании системы следует учитывать и иные параметры, в частности, опасность отказов.

2.2 Учет опасных отказов

Современная теория надежности делает упор на повышение вероятности безотказной работы отдельных элементов и увеличение числа резервных элементов. Теория надежности углубляется в изучение и раскрытие принципа резервирования.

Но в случае функционирования реальных систем повышение надежности является не главным направлением улучшения качества работы системы.

Даже при сколь угодно большом повышении надежности мы не можем исключить выход системы из строя, так как этот процесс является вероятностным. При любом значении вероятности безотказной работы сохраняется вероятность обратного – вероятность отказа. Как известно, любое маловероятное событие при неограниченном количестве испытаний произойдет. А отказ в современных сложных системах АСУ ТП может иметь весьма серьезные последствия [65,81,86,128].

Каждая автоматизированная система является многофункциональной системой, функции которой обладают различной значимостью и, следовательно, различными требованиями к надежности. В состав каждой АСУ ТП входит набор различных элементов, выполняющих различные функции. Причем один элемент

может выполнять несколько функций и, наоборот, одна функция может выполняться несколькими элементами. Во многих системах возможно возникновение исключительных, аварийных ситуаций. На вероятность возникновения таких ситуаций влияет состав системы, ее обеспечение и персонал [20, 34, 48, 73]. Но некоторыми исследователями предлагается изменение рассмотрения надежности систем, отход от безотказности в пользу живучести и безопасности.

Безотказностью называется свойство системы сохранять работоспособность в течение определенного времени при нормальных условиях. Живучесть – способность технического устройства, сооружения, средства или системы выполнять основные свои функции, несмотря на полученные повреждения.

Безопасностью же называется способность системы не переходить в опасное состояние, при котором возникает ущерб «большого масштаба». Состоянием, вызывающим такой ущерб, может быть пожар, затопление, утечка вредных химических веществ, расплавление или заморозка оборудования.

Как видно, с эксплуатационной точки зрения безопасность системы гораздо важнее общей надежности. Но ее обеспечение требует иного подхода.

В соответствии с подходом безопасности систем, повышая надежность элементов, вводя структурную и временную избыточность, применяя взаимозаменяемость, восстанавливаемость и иные меры повышения надежности сложной системы, отказоустойчивость мы обеспечиваем. Но именно для сложных систем характерной является возможность весьма сложных, многократных комбинаций отказов, каждая из которых невероятно мала, а в сумме таких невероятных состояний накапливается достаточно, чтоб система попала в опасное состояние.

Опасным состоянием называется состояние, в котором возникает ущерб «большого масштаба» [35, 48, 58].

В проблеме безопасности на первый план выходят не учитываемые в теории надежности компоненты – среда, в которой функционирует система, защитные сооружения, неблагоприятные внешние воздействия, умышленные или

безответственные действия людей. Четкое знание условий возникновения этих неблагоприятных условий позволяет, с одной стороны, принять заблаговременно соответствующие меры защиты, а с другой – разработать безопасный алгоритм управления системой [110].

Опасность – возможность возникновения обстоятельств, при которых материя, поле, энергия, информация или их сочетание могут таким образом повлиять на сложную систему, что приведет к ухудшению или невозможности ее функционирования и развития [90,112,121,122].

Ущерб – потери некоторого субъекта или группы субъектов, части или всех своих ценностей [40].

Опасная ситуация – ситуация, в которой человек подвергается опасности.

Риск – сочетание вероятности появления угрозы и серьезности этой угрозы.

Безопасность – свобода от неприемлемого риска [67, 78, 101].

Надежность системы не связана напрямую с безопасностью, ненадежные системы являются безопасными, если каждый отдельный отказ всегда переводит систему в безопасное состояние.

Даже максимально низкая вероятность критического отказа – отказа системы или ее элемента, тяжесть последствий которого в пределах данного анализа признана недопустимой и требует принятия специальных мер по снижению вероятности данного отказа и/или возможного ущерба, связанного с его возникновением [48,102,66], не исключает возможности его наступления.

То есть в теории безопасности, по сути, родственной надежности, рассматриваются именно опасные и безопасные состояния систем и элементов.

Требования к безопасности

Сложность структуры и алгоритмов функционирования современных систем приводит к тому, что использование математического аппарата теории надежности становится совершенно необходимым уже на этапе задания требований по надежности, предъявляемых к системе в целом и к отдельным составным частям системы.

Задание обоснованных требований по надежности, предъявляемых к системе в целом, представляет собой весьма сложную задачу. При распределении же требований по надежности между отдельными частями системы особых трудностей не возникает.

Иногда при параметрических расчетах получается, что один из вариантов системы оказывается наиболее целесообразным для одних значений параметров, а другой – для других. Такая информация очень важна, так как показывает границы применимости вариантов [108-111].

Рассмотрим особенности применения данного подхода к рассмотрению безопасности АСУ ТП. Их причиной является одновременно и теоретическая универсальность автоматизированной системы управления, и строгая конкретность и привязанность к конкретному объекту испытаний в случае практического применения системы.

Источником ущерба может являться как объект испытания, так и сама АСУ ТП. Это приводит к необходимости рассмотрения в качестве потенциально становящихся опасными параметров как системы (датчиков, контроллеров, индикаторов), так и самого оборудования. Возникающий ущерб, невеликий на данном уровне рассмотрения, имеет свойство накапливаться. Низкий ущерб, приносимый рассматриваемой системой, складывается с подобными ущербами, наносимыми прочими системами суперсистемы, в которую она входит, и оказывается весьма значительным.

Оценку безопасности системы в первую очередь необходимо начинать с рассмотрения ее функций. Именно выполнение функций и является целью создания АСУ ТП. А из знаний конкретных функций системы, знания того, что она делает и какие процессы в ней происходят, можно вывести ее физические принципы действия, которые чаще всего и являются источником опасности. Как уже было сказано, АСУ ТП несет и собственные опасности. Для их анализа необходимо спуститься на один уровень абстракции ниже. При таком рассмотрении функции выполнять будет не система, а отдельные элементы. Вместо АСУ ТП у нас будет набор элементов, преобразующих физические

величины, передающих и изменяющих электрические сигналы, отображающих показания, управляющих техническим оборудованиям.

Таким образом, вырисовывается своеобразный квартет: функция, элемент, опасность, защита.

Некую функцию исполняет какой-то элемент, несущий какую-то опасность, которую можно нейтрализовать механизмом защиты.

В процессе выполнения функции системой в ее элементах возникают события. Некоторые из этих событий напрямую наносят ущерб оборудованию и персоналу. А еще один набор событий могут иметь наносящие ущерб события своим следствием.

Категоризация опасностей

Для лучшего рассмотрения цепочек подобных событий строятся схемы структуры событий (рисунок 2.5).

Устройства и мероприятия, обеспечивающие устранение опасности, защиту от нее, таким образом, будут своеобразными обработчиками событий. Такими устройствами будут системы пожаротушения, планы и схемы процессов пожаротушения, наборы изолирующей спецодежды и инструментов, адсорбирующие и абсорбирующие вредные вещества материалы и прочие подобные объекты.

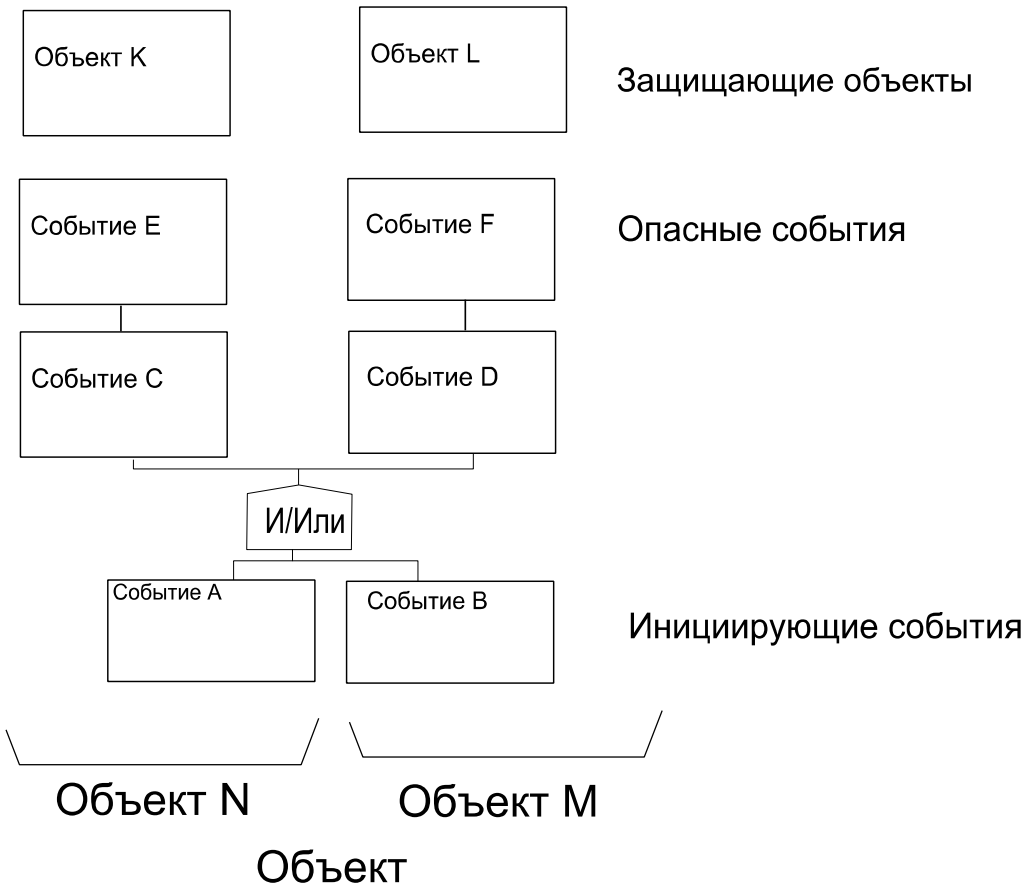


Рисунок 2.5 – Схема структуры событий

Различие опасностей по их влиянию может быть выражено в виде определенной величины, коэффициента [128, 130]. Следует определить для каждого модуля значение величины *C*, количественно оценивающей опасность, которую несет отказ, причем необходимо учитывать разделение по модулям опасности, вызываемой взаимным воздействием двух или более отказов.

Данный коэффициент поможет оценить относительную важность повышения вероятности безотказной работы каждого элемента.

Возникновение опасных событий вызывает ущерб для предприятия, экономической среды, в которой функционирует АСУ ТП. Он физически может иметь различный характер, но для анализа следует выразить его через единую величину.

Оценка приемлемости является чрезвычайно важным вопросом проектирования систем. Необходимо учитывать не только, насколько качественно работает система, но и насколько экономически оправдана та или иная ее конфигурация.

Возникающие опасности различаются по характеру возникновения. Существуют опасности, которые возникают, когда полностью прекращается выполнение функции тем или иным модулем. Предотвращаются данные опасности путем повышения безотказности модуля, к примеру, резервированием. Но также есть опасности, которые возникают, когда происходит отказ лишь элемента. Примером источника таких опасностей могут быть параллельно и одновременно работающие рабочие и резервные реле или магнитные пускатели. В таком случае для предотвращения опасности необходимо применять методы предотвращения отказа элементов или поглощения опасных воздействий.

В зависимости от происхождения опасности от отказа модуля или элемента величина C переводится в величину C_m для опасности, возникающей при отказе модуля, или C_e для опасности, возникающей при отказе элемента.

Алгоритм учета опасностей отказов состоит из следующих этапов:

– определение возможных опасных воздействий системы;

– определение для каждого модуля величины, количественно – оценивающей опасность отказа;

– анализ того, возникает ли опасное воздействие при отказе модуля или его резервного элемента;

– обнаружение комплексных опасностей – опасностей, возникающих из-за нескольких одновременных отказов;

– вычисление для модулей или элементов коэффициентов приоритета с учетом их долей в комплексных опасностях.

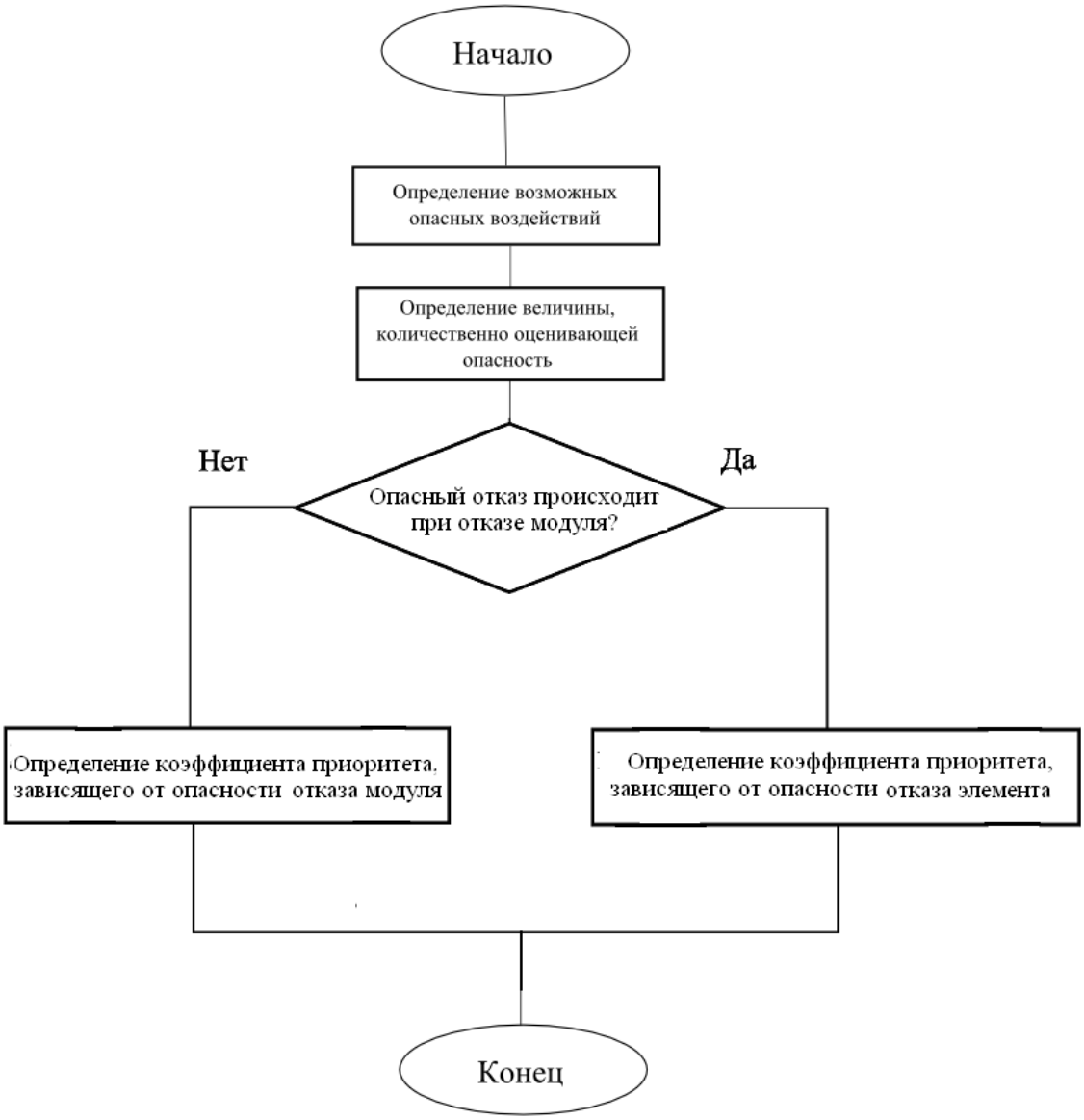


Рисунок 2.5 – Блок схема алгоритма учёта опасностей

Создание алгоритма учета 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, иных, чем добавление резервных элементов, находящихся под нагрузкой, мер.

2.3 Применение блокирующих модулей

Для максимального повышения эффективности анализа и повышения надежности следует учитывать и другие направления повышения вероятности выполнения системой всех функций.

Для более качественного рассмотрения надежности системы следует подходить к этому вопросу комплексно. Наряду с резервированием можно применять и частные методы повышения надежности, специфичные для АСУ ТП.

Одним из таких методов является метод блокирующих модулей (БМ). Ими достигается повышение вероятности безотказной работы системы путем ввода элементов, блокирующих разрушающие внешние воздействия, по отношению к системе обеспечивающих ее работу устройств. Эти отказы и блокируют модули, из-за чего они и получили свое название [74].

Блокирующие отказы модули

Как известно, автоматизированные системы в качестве энергии используют электричество. И зачастую происходят различные отклонения величины напряжения в электрических сетях, в том числе и питающих АСУ ТП. И данные отклонения могут привести к временному или постоянному выходу системы из строя.

Для защиты автоматизированной системы от колебаний напряжения применяются различные технические средства, к примеру, источники бесперебойного питания (ИБП), поддерживающие напряжение на уровне, который необходим для работы модуля.

Подобные средства в общем случае выполняют функцию поддержания напряжения на уровне, который необходим для работы системы. Такими средствами, к примеру, являются стабилизаторы, сглаживающие колебания напряжения, источники бесперебойного питания, обеспечивающее подачу напряжения системе во время отсутствия его в основной питающей сети.

В общем случае функция устройств защиты заключается в том, чтобы срабатывать в определенной ситуации. Вне зависимости от принципа работы

функция устройств защиты заключается в том, чтобы срабатывать в случае необходимости.

В качестве иллюстрирующего примера рассмотрим в качестве устройства защиты ИБП.

Источник бесперебойного питания – устройство, позволяющее обеспечить работу системы при условии нарушения работы основной электрической сети.

ГОСТ 13109-97 определяет следующие нормы в электропитающей сети: напряжение 220 В ± 10 %; частота 50 Гц ± 1 Гц; коэффициент нелинейных искажений формы напряжения менее 8 % длительно и менее 12 % кратковременно.

Реализация основной функции достигается работой устройства от аккумуляторов, установленных в корпусе ИБП, под управлением электрической схемы, поэтому в состав любого ИБП, кроме схемы управления, входит зарядное устройство, которое обеспечивает зарядку аккумуляторных батарей при наличии напряжения в сети, обеспечивая тем самым постоянную готовность к работе ИБП в автономном режиме. Для увеличения автономного режима работы можно оснастить ИБП дополнительной (внешней) батареей.

Режим байпас (англ. Bypass, «обход») – питание нагрузки отфильтрованным напряжением электросети в обход основной схемы ИБП.

«Бустер» (англ. booster) – ступенчатый автоматический регулятор напряжения (англ. Automatic Voltage Regulation, AVR), имеющий автотрансформатор в своей основе. Используется в ИБП, которые работают по интерактивной схеме.

Вышеизложенная информация показывает наличие довольно сложной структуры ИБП, что означает, что он будет обладать собственной надежностью.

Рассмотрим формулу повышения надежности модуля, блокирующего отказы. В соответствии с теорией вероятности это описывается следующим образом.

Полная совокупность событий, присущая данным устройствам, описывается следующими величинами:

$$P = P_1 + P_2 = 1, \quad (2.4)$$

где P – вероятность выхода из строя модуля,

P_1 – вероятность того, что напряжение на выходе исчезло,

P_2 – вероятность того, что напряжение на выходе сети не исчезло.

Причем событие, описываемое P_1, подразделяется на подсобытия,

P_a – вероятность того, что устройство сработало,

P_b – вероятность того, что устройство не сработало.

И одновременно с этим существует определенная вероятность выхода из строя самого ИБП P_c, прекращения передачи им напряжения.

Вероятность того, что модуль не вышел из строя, будет

$$P_2 = 1 - P_1 \quad (2.5)$$

$$P_2 = 1 - (1 - P_2) \quad (2.6)$$

Запишем вероятность выхода из строя как

$$P_1 = 1 - P_2 \quad (2.7)$$

Но если выходы из строя будут блокироваться, то модуль выйдет из строя, когда не будет работать ни он, ни блокирующий модуль.

$$P_1 = (1 - P_2) \times (1 - P_b) \quad (2.8)$$

Следовательно,

$$P_2 = 1 - (1 - P_2) \times (1 - P_b) \quad (2.9)$$

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

$$P = (1 - (1 - P_2) \times (1 - P_b)) \times P_c \quad (2.10)$$

где P_2 – вероятность того, что отказ функционального модуля не произошел,

P_b – вероятность того, что блокирующий модуль не сработал,

P_c – вероятность выхода из строя самого блокирующего модуля.

Имитационное моделирование блокирования

Для того чтобы проверить формулы для вычисления надежностей подобных систем, проведём вычислительный эксперимент, имитирующий работу модуля, воспользовавшись методом Монте-Карло.

Выбор подобного метода обуславливается его универсальностью и гарантированной точностью, так как он позволяет рассчитывать надежность систем исходя из фактических событий в системе [10,17,18,53].

Основная идея метода Монте-Карло при статистическом моделировании надежности элементов заключается в многократном расчете определяющего параметра или параметров по известным зависимостям, описывающим процесс потери работоспособности, причем для случайных аргументов, входящих в формулы, выбираются их наиболее вероятные значения в соответствии с известными законами распределения. Каждое статистическое испытание заключается в выявлении одной из реализаций случайного процесса, а их совокупность позволяет оценить ход этого процесса и его основные параметры.

В общем случае можно считать, что значение определяющего параметра X определяется набором случайных величин Z_t (i = l, 2, ..., n), законы распределения которых известны (или дискретные значения которых заданы своими вероятностями):

$$X = X(Z_1, Z_2, ..., Z_n) \qquad (2.11)$$

Так как аргументы функции (n) являются случайными величинами, то и параметр X является случайной величиной. Поэтому для анализа надежности по параметру X необходимо проанализировать его распределение и для оценки вероятности безотказной работы определить долю, которую составляют допустимые режимы (в общем случае $X_{min} \le X \le X_{max}$).

На первом этапе реализации метода Монте-Карло в зависимости от необходимой точности определения характеристик надежности выбирается необходимое число реализаций N. Затем из заданного диапазона изменения каждого из аргументов Z_t по известным законам распределения $f(Z_i)$ случайным образом (с использованием таблиц или генератора случайных чисел) выбирается по N значений каждого из аргументов:

$$Z_1 \in \{\zeta_{11}, \zeta_{12}, ..., \zeta_{1\varphi}, ..., \zeta_{1N}\},$$

$$Z_2 \in \{\zeta_{21}, \zeta_{22}, ..., \zeta_{2\varphi}, ..., \zeta_{2N}\},$$

...,

$$Z_\iota \in \{\zeta_{\iota 1}, \zeta_{\iota 2}, ..., \zeta_{\iota\varphi}, ..., \zeta_{\iota N}\},$$

$$Z_\nu \in \{\zeta_{\nu 1}, \zeta_{\nu 2}, ..., \zeta_{\nu\varphi}, ..., \zeta_{\nu N}\}.$$

После этого из полученных значений аргументов Z_i случайным образом выбираются N наборов значений (в каждом наборе по одному значению каждого аргумента Z). Для каждого из наборов значений по формуле (2.11) рассчитывается определяющий параметр X.

Определяющим параметром рассматриваемой системы будет исправность.

Она выражается функциями, использующими логические зависимости.

Исправность каждого элемента выражается значением P_i – вероятности безотказной работы, а состояние – традиционно логической переменной S_i, принимающей значение 1 в случае исправности элемента и 0 в случае его неисправности.

Определяет же наступление состояния случайное событие, выражающееся числом R_i, принимающим случайное значение из интервала (0…1).

Следовательно, для определения состояния видится возможным применить следующие выражения:

$$S_i = 1, \text{ при } R_i < P_i \quad (2.12)$$

$$S_i = 0, \text{ при } R_i < P_i, \quad (2.13)$$

где - 1 обозначает рабочее состояние, а 0 – нерабочее.

При проведении эксперимента сначала назначим (сгенерируем) набор случайных событий, происходящие с рассматриваемом БМ – событие выхода из строя блокируемого модуля (R_1), событие срабатывания блокировки БМ (R_a) и событие исправности передачи БМ (R_c).

Потом, назначая соответствующие вероятности (таблица 2.1), определяем состояния и находим логические зависимости между ними.

Таблица 2.1 – Показатели надежности модулей

Надежность передачи	Надежность блокировки	Надежность модуля
0,9	0,9	0,8

Функциональный модуль будет исправным, если он исправен сам по себе или неисправен, но исправна блокирующая функция БМ, а также исправен сам БМ.

$$(S_1 \vee \overline{S_1} \wedge S_a) \wedge S_c \tag{2.14}$$

Эксперимент будет состоять в последовательной генерации событий и получении итоговых состояний функционального модуля, используя выражения (2.12), (2.13), (2.14).

Данный эксперимент повторяется несколько раз, затем подсчитывается, в скольких случаях функциональный модуль по итогам работы БМ оказался в исправном состоянии.

Отношение количества результатов эксперимента, в которых функциональный модуль с БМ оказался исправным ко всем итогам показывает вероятность исправности функционального модуля с БМ.

Выполняя определенное множество вычислений каждого состояния, подставляя в (2.14), суммируя результаты каждого вычисления, принимая истинное значение за единицу, а ложное – за ноль, а затем деля получившийся результат на «длину» множества, получим значение вероятности «заблокированного» отказа, вычисленное по методу Монте-Карло.

При выполнении вычислений над (2.14) и исходными данными из таблицы 2.1 оно будет равно $P_2 \approx 0{,}885$.

А при подстановке в (2.10) результатом вычисления будет $P_2 = 0{,}882$.

Схожесть результата формулы (2.10) с результатом принимаемой за верную (2.14) доказывает верность (2.10).

Блокирующие опасность модули

Наряду с модулями, блокирующими отказы, существуют и модули, которые предотвращают наступление опасности.

В категорию блокирующих опасность модулей включается множество средств защиты.

Применение данных средств в последовательности проектирования системы описывается на стадии рассмотрения безопасности жизнедеятельности. Данная стадия тесно связана с учетом надежности, таким образом, блокирующие опасность модули являются пограничным понятием теории надежности и безопасности жизнедеятельности. Они включены в метод для повышения эффективности проектирования в целом путем автоматизации процесса проектирования.

Средства защиты делятся на средства коллективной защиты и средства индивидуальной защиты.

Средства индивидуальной защиты (СИЗ) – средства, используемые работником для предотвращения или уменьшения воздействия вредных и опасных производственных факторов, а также для защиты от загрязнения [23,25,34]. Применяются в тех случаях, когда безопасность работ не может быть обеспечена конструкцией оборудования, организацией производственных процессов, архитектурно-планировочными решениями и средствами коллективной защиты.

Средства коллективной защиты (СКЗ) – средства, используемые для предотвращения или уменьшения воздействия на работников вредных и опасных производственных факторов, а также для защиты от загрязнения [37-39].

В зависимости от назначения средства защиты подразделяют на классы:

– средства нормализации воздушной среды производственных помещений и рабочих мест,

– средства нормализации освещения производственных помещений и рабочих мест,

– средства защиты от повышенного уровня ионизирующих излучений

– средства защиты от повышенного уровня электромагнитных излучений,

– средства защиты от повышенного уровня шума,

– средства защиты от воздействия химических факторов,

– средства защиты от воздействия биологических факторов [43,61].

Одними из самых важных источников опасности являются опасности, связанные с воздействиями аварийных химически опасных веществ (АХОВ) [49, 83].

Для данных веществ разработана структура средств блокирования их воздействия, что позволяет как ликвидировать их до воздействия на персонал, так и химически или физически нейтрализовать их опасность [90,115,106,125].

Алгоритм включения блокирующих опасности и отказы модулей:

– определение используемых модулями веществ и энергий;

– назначение блокирующих модулей в соответствии с требованиями стандартов и физическими характеристиками веществ и энергий;

– расходование ресурсов на назначенные блокирующие модули;

– уменьшение опасности отказов модулей, которым назначены блокирующие опасность модули;

– увеличение безотказности модулей, которым назначены блокирующие отказ модули.

Средства индивидуальной и коллективной защиты являются обязательным элементом безопасности [29,30]. И в созданной системе включение расходов ресурсов на данные средства введено обязательным этапом.

Вышеприведенная методика позволяет улучшить качество работы системы, обеспечивая более точный учет безотказности, расширение списка рассматриваемых параметров надежности и более полное использование технических средств.

Выводы

1. Предложенная методика декомпозиции АСУ ТП на функциональные последовательности с учетом важности позволяет оценить вероятность пребывания системы в различных состояниях и повысить вероятность безотказной работы наиболее важной для цели АСУ ТП функции.

2. Алгоритм учета системой опасностей позволяет при построении системы целенаправленно понижать вероятность опасного отказа.

3. Механизм включения системой на этапе разработки блокирующих модулей при формировании структуры АСУ ТП позволяет обеспечить уменьшение опасных воздействий и повышение надежности модулей системы.

4. Предложенные модификации позволяют при анализе надежности учесть специфические для АСУ ТП надежностные показатели. Они позволяют разделить опасности на категории по значимости, дать оценку негативного эффекта избыточности из-за опасных отказов в модулях и учесть случаи комплексных отказов.

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

6. Таким образом, предложенные модификации позволяют не только повысить безотказность системы, но и обеспечить безопасность отказов и ограниченность их последствий.

3. Математическое описание системы

3.1 Выбор версий и расчет приоритета резервирования

В качестве исходных данных система использует массив *M*, состоящий из *K* строк (3.1), и восьми столбцов, по количеству типов данных о версиях модуля.

$$K = \sum_{i=1}^{n} v_i \quad , \tag{3.1}$$

где v_i – количество версий *i*-го модуля,

n – количество модулей.

В каждой строке массива записывается определенная версия очередного модуля. Номер модуля, к которой принадлежит каждая *i*-я версия каждого модуля, записан в элементе {*j*,1}, где *j* – сквозной номер версии по порядку. В элементе {*j*,2} записан порядковый номер версии в модуле. Элементы {*j*,3…*j*,5} отведены под ресурсы, необходимые для включения версии в структуру системы. В {*j*,6} указана надежность, в {*j*,7} – среднее время между отказами.

Необходимость указания среднего времени между отказами следует из практической распространенности указания данной величины в технической документации на оборудование.

Используя данную величину и принимаемое в расчете время эксплуатации системы, вычисляется надежность каждой версии элемента, которая используется в дальнейшем расчете надежности всей системы.

Выбор версий

Надежность элемента, полагая, что распределение отказов экспоненциально, вычисляется по формуле:

$$P(t) = e^{-\lambda t} \quad , \tag{3.2}$$

где *t* – срок службы системы

λ – интенсивность отказов:

$$\lambda = \frac{1}{T} \quad , \tag{3.3}$$

где T – среднее время наработки на отказ.

Различные типы резервирования применяются из-за различных технических особенностей оборудования.

При постоянном способе соединения все элементы – и основные элементы, и резервные – подключены к общей нагрузке в течение всего времени работы устройства. При полупостоянном соединении соединенными с общей нагрузкой остаются только исправные элементы, а отказавший элемент отключается от нее. При полузамещении в начале работы соединяют с общей нагрузкой лишь исправные основные элементы, а при отказе одного из них подключается резервный элемент, но отказавший элемент не отключается. При замещении в начале работы к общей нагрузке подключены также только исправные основные элементы; если же один из них отказал, то к нагрузке подключается резервный элемент, а отказавший основной элемент отключается.

Устройства сбора данных могут работать параллельно и одновременно, их работа не оказывает существенного влияния на параметры контролируемого процесса. Таким образом, к ним возможно применить горячее резервирование.

Устройства управления, такие как клапаны, характеризуются конкретными величинами изменения технологических параметров, и их резервные экземпляры не могут изменять параметр одновременно с основным. Но их технологические параметры предусматривают возможность параллельной физической установки и переключения от неисправного элемента к исправному. Резервирование холодное.

Существует и категория устройств, резервирование которых физически затруднительно и не предполагается строением оборудования. Таким образом, устройства из данной категории не резервируются алгоритмом, только учитываются в итоговом подсчете надежности системы.

Вторым источником исходных данных является массив ограничений ресурсов L.

Главным ограничением в модели проекта является ограничение по одному ресурсу – по стоимости.

В данной системе сохраняется принцип предварительного отсева версий модулей, не пригодных к резервированию по расходу ресурсов.

Система выполняет отсев версий, которые невозможно использовать как резервные, согласно условию:

$$L_i - Rs_{ij} > R_{ijk} \qquad (3.4)$$

где L_i – запас i-го ресурса, выделяемый на построение системы,

Rs_{ij} – наименьший i-й ресурс j-го модуля,

R_{ijk} – количество i-го ресурса, расходуемого на реализацию j-го модуля k-й версии.

Реализуется этот принцип следующим алгоритмом.

В i-й элемент массива V заносится число версий каждого i-го модуля, а в i-й элемент массива F – номер каждой первой версии каждого модуля по порядку.

В массив R записываются каждый расход ресурсов на каждую версию каждого модуля. Затем по каждому ресурсу происходит минимизация, таким образом, для каждого j-го модуля находя наименьший расход i-го ресурса Rs_{ij}.

Вычисляется разность между ограничением i-го ресурса L_i и наименьшим расходом i-го ресурса на j-й модуль Rs_{ij}, и данная разность сравнивается с каждым i-м ресурсом k-й версии j-го модуля.

Если неравенство (3.4) не выполняется, то строка давшей невыполнение версии из массива M исключается путем обнуления, с использованием данных о номерах строк из массивов B и F.

Дальнейшим действием будет нахождение наиболее надежной версии каждого модуля.

Особенностью данного поиска является то, что в качестве принимаемого для включения в систему должен быть выбран наиболее подходящий модуль. И критерием выбора служит не только надежность, но и расход ресурсов.

Для каждого модуля осуществляется поиск версии с максимальной надежностью. Максимальная надежность среди всех версий i-го модуля записывается в массив Mo в позицию $\{i,e\}$. Сквозные порядковые номера

наиболее надежной версии *i*-го модуля записываются в массив *No* в позицию {*i,e*}. Величина *e* изначально равна 1.

Затем среди всех версий находятся все остальные версии, для которых надежность равна максимальной:

$$M\{6,n\} = Mo\{i,e\} => e+1,\ No\{i,e\} = n, \tag{3.5}$$

где *n* – очередная версия модуля, *n* увеличивается на 1 на каждом шаге сравнения. Далее среди всех элементов *No* находится версия с наименьшим расходом ресурсов:

$$Nm_i = Min(M\{3,\ No\{i,e\}\} \cdot a + M\{4,\ No\{i,e\}\} \cdot b + \\ + M\{5,\ No\{i,e\}\} \cdot c)\ e = 1 \ldots e_{max}, \tag{3.6}$$

где *a*, *b*, *c* – балансирующие коэффициенты, обеспечивающие равнозначность ресурсов:

$a = 1$

$b = L_1/L_2$

$c = L_1/L_3$

Расчет приоритета резервирования

В соответствии с описанной идеей приоритизации и с учетом рассмотренных иных надежностных параметров, помимо безотказности, делается вывод о необходимости введения показателя, определяющего очередность резервирования модулей. Необходимо создать функцию, вычисляющую данный показатель, – функцию приоритета.

В первую очередь аргументом функции приоритета будет надежность модуля.

Чем более надежен модуль – тем менее нужна ему повышенная степень резервирования, точнее – тем больше нужна повышенная степень резервирования другим, последовательно надежностно-связанным с ним модулям.

Значит, показатель очередности будет обратно пропорционален текущей надежности модуля.

Опасность также будет являться аргументом функции приоритета. И особенностью учета опасности в расчете приоритета будет двойственная ее

природа. Опасность, которую фактически несет выходящий из строя модуль, уменьшается с увеличением степени резервирования. А опасность, которую несет выходящий из строя элемент, с увеличением степени резервирования увеличивается.

Показатель очередности будет прямо пропорционален опасности модуля и обратно пропорционален опасности элемента.

Итоговая функция приоритета будет иметь вид

$$Ra_i = (K_i) / (K_{dei} \cdot P_i), \quad (3.7)$$

K_i – коэффициент приоритета, зависящий от важности и опасности отказа модуля,

P_i – вероятность безотказной работы модуля,

K_{dei} – коэффициент приоритета, зависящий от опасности отказа элемента модуля.

Причем коэффициенты K_i и K_{dei} подчиняются условиям $0 < K_i < 1$, $0 < K_{dei} < 1$, а вероятность отказа считается с учетом избыточности и резервирования. В дальнейшем эти значения будут считаться показателями целевой вероятности безотказной работы i-го модуля.

Данная функция позволяет при формировании системы учитывать специфические для АСУ ТП параметры надежности, такие как важность и опасность отказа. Рассмотрим, как вычисляются аргументы данной функции.

3.2 Многоатрибутивная декомпозиция АСУ

Оригинальная методика декомпозиции системы на функциональные последовательности реализуется следующим образом.

Декомпозиция в разработанном методе выполняется в два этапа. Первый этап – разбиение функциональной схемы автоматизации на функциональные последовательности. Данное разбиение выполняется до начала выполнения алгоритма, результатом ее будет множество последовательностей модулей S

$$S_i = [1 \ldots M_i] \quad (3.8)$$

где i – номер очередной последовательности.

Разбиение выполняется оператором метода. Это происходит из-за трудоемкости автоматизации анализа функциональных схем. Конечными функциями АСУ ТП являются контроль параметров объекта и управление им или контроль сопутствующих систем. Определение того, какие модули должны быть исправными для выполнения той или иной функции, обеспечивается профессиональными знаниями оператора.

Согласно современной концепции автоматизации, каждый информационный поток проходит через центральный процессор контроллера. Непосредственный сбор и передача к объекту информации осуществляются дискретными или аналоговыми модулями ввода-вывода.

Остальные операции выполняются модулями, специфичными для данного конкретного типа сбора данных или управления: первичными и вторичными преобразователями, реле, пускателями, клапанами, приводами и т.п.

Алгоритмом выполняется перевод последовательностей в вид, пригодный для обработки на дальнейших этапах вычисления.

До ввода последовательностей в алгоритм они предварительно обрабатываются в связи с различностью понятий «функциональная последовательность» и «надежностная последовательность».

В то время как в функциональной последовательности в силу ее физической природы не предусматривается изменение порядка элементов, надежностная последовательность обладает свойством транзитивности ветвей. Транзитивность ветвей следует из транзитивности произведения.

Последовательности, имеющие различные структуры, можно привести к одному виду (рисунок 3.1).

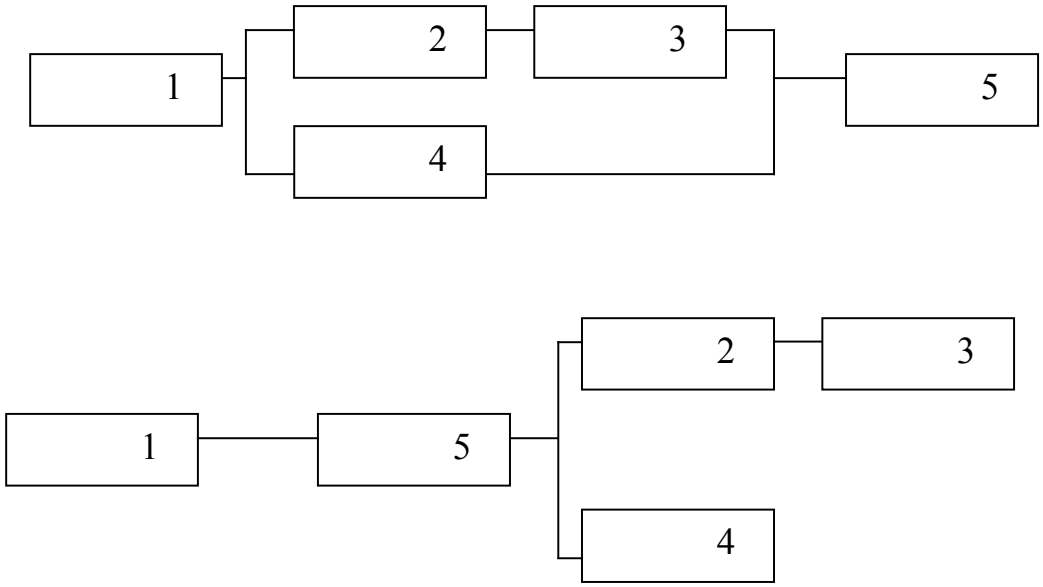


Рисунок 3.1 – Преобразование системы к древовидной структуре

Целью данных преобразований является унификация последовательностей и обеспечение удобства их ввода в алгоритм.

Набор последовательностей, выполняющих функцию, записывается в массив *B*.

Структура ветвления системы кодируется массивом *S*.

В элементе $S\{1,j\}$ приведено множество *N* – множество модулей, после которых возникает развилка, образующая *j*-ю последовательность:

$$S^1_j = [N1, \ldots, Ni] \tag{3.9}$$

В $S\{2,j\}$ – множество количества модулей *A* в побочной ветви *j*-й последовательности.

Таким образом, каждая последовательность B_k формируется как множество элементов:

$$B_j=[1,\ldots N_i, N_k, \ldots, N_k + A_i], \tag{3.10}$$

где N_i – модуль, записанный *i*-м в S^1,

N_k – модуль, следующий за последним модулем B_{i-1} последовательности.

Надежность же каждой ветви определяется, как

$$Ps_i = \prod_{j=1}^{N_j} P_{1+j} * \prod_{j=N_k}^{N_k+A_i} P_{N_k+j}, \quad (3.11)$$

где Ps_i – надежность последовательности,

P_n – надежность n-го модуля.

Учет важности той или иной функции обеспечивается следующим.

На первом шаге определяются последовательности модулей, выполняющие ту или иную функцию. Каждой последовательности назначаются показатели важности $W_j = w$, где $w = 1$, если последовательность выполняет функцию контроля сопутствующих систем, $w = 2$, если последовательность выполняет функцию контроля объекта или управления им.

Каждому модулю должна быть назначена величина W_i, определяющая важность этого модуля. Величина W_i для i-го модуля в этом случае выбирается как наибольшее значение W среди всех последовательностей, в которые входит i-й модуль. Это позволяет обеспечить равномерность учета важности модулей, несмотря на их положение в последовательности.

В случае если i-й модуль имеет важность $W = 1$, соответствующий коэффициент K_i выбирается равным показателю вероятности безотказной работы самого ненадежного модуля системы. Это уменьшит приоритет резервирования менее важных модулей.

В $S\{3,j\}$ записана важность j-й последовательности:

$$S^3{}_j = [W1, \ldots, Wj] \quad (3.12)$$

Данная величина должна быть назначена каждому модулю.

Как следует из (3.12), один и тот же модуль может входить в несколько последовательностей одновременно. Величина W_i для i-го модуля в этом случае выбирается как наибольшее значение W среди всех последовательностей, в которые входит i-й модуль. Это позволяет обеспечить равномерность существенности между модулями, несмотря на их положение в последовательности.

Разработанной методикой обеспечивается учет важности той или иной функции АСУ ТП. Это позволяет при построении системы ограничить

последствия отказов, повышая вероятности безотказности наиболее существенных функций.

3.3 Определение целевой вероятности опасных отказов

В случае если важность модуля $W = 2$, производится анализ опасности i-го модуля.

Разработанный новый алгоритм учета опасностей имеет следующий вид.

Выбирается отношение интенсивности безопасных отказов к интенсивности всех отказов. Это соотношение, вводимое стандартом МЭК 61508/61511 как SFF, выбирается, исходя из нужного для системы интегрального уровня безопасности, определяемого при формировании требований к АСУ ТП. Также при формировании требований выбирается целевая вероятность безотказной работы главной функции P.

Исходя из данных параметров, определяется интенсивность опасных отказов и интенсивность безопасных отказов:

$$\lambda = \frac{-\ln(P)}{t}, \lambda = \lambda_s + \lambda_d \qquad (3.13)$$

где λ_s – интенсивность безопасных отказов,

λ_d – интенсивность опасных отказов:

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

$$P_{fdt} = 1 - e^{-\lambda d t}, P_{fst} = 1 - e^{-\lambda st} \qquad (3.14)$$

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.

Найдем целевые вероятности безотказной работы каждого модуля с безопасными отказами:

$$P_{fst} = 1 - \prod_{i=1}^{n} P_{sti} \tag{3.15}$$

$$P_{fst} = 1 - P_{dti}{}^{n} \tag{3.16}$$

Решая относительно $P_{sti,}$ получим

$$P_{sti} = \sqrt[n]{1 - P_{fst}} \tag{3.17}$$

И с опасными отказами:

$$P_{fdt} = 1 - \prod_{i=1}^{n} P_{dti} \tag{3.18}$$

Решая относительно $P_{dti,}$ получим

$$P_{dti} = \sqrt[n]{1 - P_{fdt}} \tag{3.19}$$

Среди модулей с безопасными отказами не производится градация по опасности, таким образом, коэффициентом для каждого безопасного модуля будет $K_i = P_{sti}$. Ущерб от опасных отказов вычисляется для каждого модуля с опасным отказом с учетом следующих предположений:

– во-первых, к возникновению ущерба может привести отказ как одного модуля, так и нескольких, причем в таком случае, в случае сложных отказов, величина ущерба делится между модулями пропорционально;

– во-вторых, ущерб может быть вызван как из-за опасного отказа в модуле, так и в основном или одном из резервных модулей, поэтому необходим алгоритм их разделения.

Градация по опасности проводится среди модулей с опасными отказами. В зависимости от природы опасного воздействия выбирается величина *Cm* или *Ce*, количественно оценивающая опасность.

Формируется массив *C*, который заполняется следующим образом

$$\{M1_m \ldots Mi_m \ldots Mn_m,\ C_m, x_m\}, \tag{3.20}$$

где *M1…Mn* – номер модуля, отказ которого приведет к ущербу,

C – величина, количественно оценивающая опасность,

x – обозначение, где возникает опасность – в модуле или в элементе.

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

Затем находится отношение десятичного логарифма этой величины к десятичному логарифму критического ее значения, умноженное на вероятность опасного отказа:

$$M_i = \frac{C_i}{\text{ССК}_\text{i}} \cdot P_{fdti}, P_{fdti} = 1 - P_{dti} \tag{3.21}$$

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 ее значение. Затем при постоянных c и ССК определяется, какой должна быть P_f для достижения этой средней M:

$$P_{fdti} = M_{avg} \cdot \frac{\text{ССК}_\text{i}}{C_i}, \text{P}_\text{dtib} = 1 - \text{P}_\text{fdti} \tag{3.22}$$

$$P_{dti} = 1 - P_{fdti} \tag{3.23}$$

Достижение всеми модулями равной величины M_{avg} обеспечивает равное распределение ущерба по всем модулям. Для опасных модулей величины K_i и K_{dei} будут равны получившейся величине P_{dti} в зависимости от того, возникает ли опасное воздействие в результате отказа модуля или его элемента.

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 $K_i=P_{dti}$, $K_{dei}=P_{dtib}$.

Наряду с этим величина P_{dti} является критическим показателем безотказности элемента или модуля. Если вероятность безотказной работы больше, чем P_{dti} – модуль признаётся допустимо опасным.

Данный алгоритм анализа опасностей позволяет разделить опасности на категории. Разработанный способ анализа опасностей позволяет 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.

Определение значения опасностей является первым шагом в их обработке. Действие системы не ограничивается учетом опасностей. Имеются методы непосредственного снижения действительной опасности. Поле, энергия или материя, вредящие персоналу или оборудованию, могут быть нейтрализованы, заблокированы [113, 116].

3.4 Реализация блокирования опасностей и отказов

В рассматриваемом методе для повышения надежностных характеристик применяется резервирование.

Повышение надежности и безопасности АСУ ТП должно быть многонаправленным, диверсифицированным. Применение других методов позволяет сгладить недостатки принципа резервирования.

Для избежания чрезмерной избыточности, приводящей к увеличению вероятности нанесения ущерба одним из резервных элементов, применяется повышение надежности иным, чем резервирование, путем – путем применения блокирующих отказ модулей.

Снижение фактического ущерба может быть выполнено не только при помощи уменьшения вероятности опасного отказа, но и снижения возникшего опасного воздействия.

Блокирующие опасности и отказы модули для функциональных модулей выбираются автоматически в соответствии с используемыми данными функциональными модулями веществами и энергиями. Причем данный выбор выполняется до начала комплектования системы резервными модулями, так как это обеспечивает максимальное использование всех возможностей повышения надежности. Обязательность включения также проистекает из максимизации надежности.

Предложен следующий механизм включения блокирующих модулей.

Имеется множество T типов функциональных модулей. Их типизация основывается на используемых ими веществах и энергиях. Каждому типу функционального модуля соответствует свой блокирующий отказ или опасность модуль:

$$T_i \leftrightarrow Bf_i, T_i \leftrightarrow Bd_i; \tag{3.24}$$

где T – множество типов модулей,

Bf – множество блокирующих отказ модулей,

Bd – множество блокирующих опасность модулей,

i – порядковый номер типа БМ.

$$T_i = j \Rightarrow Bf_i = j, \tag{3.25}$$

где j – номер типа модуля.

Затем каждому функциональному модулю ставится в соответствие определенный тип функционального модуля, а следовательно, и тип блокирующего модуля:

$$M_i \leftrightarrow T_i \leftrightarrow Bf_i, M_i \leftrightarrow T_i \leftrightarrow Bd_i \tag{3.26}$$

У каждого блокирующего отказ модуля имеется определенный набор характеристик надежности, расход ресурсов на реализацию, и формула, согласно которой снижается вероятность отказа:

$$Bf_i = j \Rightarrow PBf_{ik} = n_{jk} \tag{3.27}$$

$$Bf_i = j \Rightarrow RBf_{ik} = r_{jk} \tag{3.28}$$

$$Bf_i = j \Rightarrow Pbj(Pj, PBf_{j1} \ldots PBf_{jk}) \tag{3.29}$$

У каждого блокирующего опасность модуля имеется величина снижения ущерба и расход ресурсов на реализацию:

$$Bd_i = j \Rightarrow HBd_i = h_j \tag{3.30}$$

$$Bd_i = j \Rightarrow RBd_{ik} = r_{jk} \tag{3.31}$$

Далее просматриваются все множества Bf и Bd.

Для каждого *j*-го модуля каждая величина объема выделенных на систему ресурсов L_{ik} снижается на величину RBf_{jk} и RBd_{jk}.

Данные операции показывают вычисление результата включения блокирующих модулей.

Механизм включения системой блокирующих модулей на этапе разработки позволяет обеспечить более точный учет трат ресурсов на повышение надежности системы, рассматривая траты на их реализацию, обеспечить уменьшение опасности и повышение надежности модулей системы [70,71].

3.5 Имитационное моделирование системы

Сети Петри как формальная основа

В настоящее время не существует абстрактной теории, которая позволяла бы интегрировать различные аспекты этой дисциплины. Рассмотрим, может ли теория сетей претендовать на роль данной дисциплины.

Схематическое представление структуры автоматизированной системы, которая является базовой для автоматизации (например, каскадное устройство или структура управления состоянием), а также графическое абстрактное представление причинно-обусловленной связи, напоминает структуру сети. Эти знания не новы, но с точки зрения поведения динамической системы может быть рассмотрена математическая теория обращения к сети основанной Петри. И здесь мотивом для разработки теории была задача «однородно и точно описать как можно больше явлений, возникающих при передаче и преобразовании информации», как писал Петри в своей фундаментальной работе [35].

Технические системы структурно аналогичны сетям. Это наблюдение справедливо, например, для электрических сетей с концентрированными компонентами, для сетевых сетей тепловых и механических систем, для которых имеется много известных примеров. Сети символизируют структуры поведения наземного и воздушного движения, а также поставок газа, воды и электричества. Сети распознаются как модели обработки данных с использованием компьютерных структур и архитектуры. В таких различных областях, как системы

биохимических процессов или системы обработки данных в реальном времени, моделирование с помощью сетей является полезным средством как для структуры, так и для эффективных связей.

В своей простейшей форме сети математически и графически описываются структурами, элементами и поведением.

Структурный принцип

Система состоит из набора частей, взаимодействующих друг с другом и периферийными устройствами системы. Части системы определяются количественно. Значение количества системы представляет состояние системы. Чтобы провести четкое различие между системой и периферийными устройствами, система должна быть независимой.

Система (сеть N) состоит из набора частей (позиция S, переход T), взаимодействующих друг с другом (отношение потока F). Части системы (позиции) описываются количествами (маркировками). Значения (маркировка) величин системы представляют ее состояние (случай, ситуацию, состояние).

Это может быть математически представлено следующим образом:

$$N = \{S, T; F, M,\}; S = \{S_1, S_2,...\}; T = \{T_1,T_2,...\}; F = \{SxT\ \ TxS\} \quad (3.32)$$

Отношение потока можно графически описать направленными дугами между позициями и переходами или между переходами и позициями. В сети маркировка представляет фактическое состояние системы. Маркировка обозначена черными метками, которые покрывают отмеченные позиции. Следовательно, сеть описывается как двудольный граф.

Принцип декомпозиции

Система состоит из набора частей, которые в дальнейшем можно подразделить на части, взаимодействующие друг с другом. Подразделы также представляют определенную сложность, то есть общие системные аспекты.

Части (позиции, переходы) можно подразделить на сети.

$$N = \{S, T; F, M,\}; S\ N_S = \{S_S, T_S; F_S, M_S\};T\ N_T = \{S_T, T_T; F_T, M_T\} \quad (3.33)$$

Система состоит из набора частей. Их взаимодействие друг с другом и результирующие изменения четко определены. В причинно-следственной связи

более поздние состояния могут быть только следствием прежних. Причинность понимается как логика операций. Изменения (маркировка) в этих частях четко определены. Изменения состояния в сети работают следующим образом: метки указанных позиций (S) перемещаются в позиции, еще не отмеченные проходящими переключенными переходами. В этой причинной связи более поздние состояния могут быть только следствием прежних. Это означает, что все позиции, ведущие к переходу, помечены, и все позиции, ведущие к переходу, свободны.

Переход работает следующим образом: отмеченные позиции передают свои метки в следующие немаркированные позиции.

$$M() = M(-1) + C\ T_F\ (-1) \qquad (3.34)$$

Операционная логика соответствует последовательности переключения и маркировки сети (график достижимости).

Система состоит из набора частей. Их структура или состояние зависит от изменений во времени. Временность - это временная последовательность операций и изменений.

Временная последовательность операций может быть получена путем использования временных сетей. Во временных сетях взвешенные по времени, то есть дуги с задержкой (Z_{PRE}), могут нести временное поведение. Здесь маркировка остается на своей позиции до тех пор, пока не пройдет соответствующее время и не переключится следующий переход.

$$N = \{S, T; M\ (0), Z_{PRE}\}, Z_{PRE}\ ((s, t)) \qquad (3.35)$$

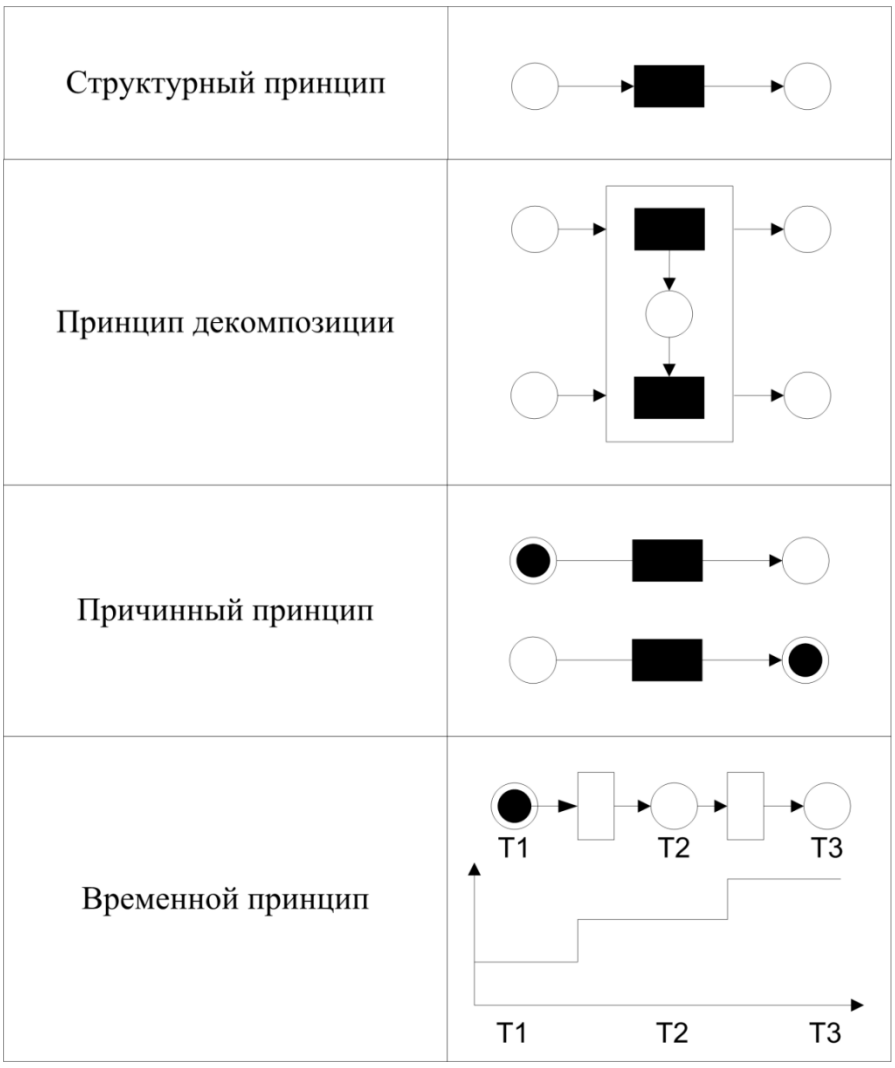


Рисунок 3.2 - Принципы Сети Петри

Применение сетей в технологии автоматизации требует практического математического моделирования и особенно интерпретируемости компонентов, структур и поведения систем автоматизации.

Таблица 3.1 противопоставляет формальным элементам теории сетей и их соответствующим реализациям в технологии автоматизации; следуя принципу декомпозиции, эти реализации представляют разные степени детализации на разных уровнях контроля. Таким образом, структурное сходство между теорией сетей и технологиями автоматизации доказано

Таблица 3.1– Противопоставление формальным элементам теории сетей и их соответствующим реализациям в технологии автоматизации

	Система управления	Контролируемая система					
Элементы сетей Петри	Разработка	Управляющей компьютер	Программное обеспечение	Надежность	Система производства	Система химического производства	Преобразование энергии
Позиции	Фаза Документы Программы Требования	Память Регистр Экран Плоттер Шина Неисправность	Память Переменные Семафоры Состояние программы Операнд	Неисправные состояния	Запас Буфер Машина Состояние Инструменты	Танк Трубопровод Материалы Исполнительный механизм / Измерение Реактор	Отвал Мощность Состояние Трубы Линии
Переходы	Спецификация Строительство Моделирование Анализ Введение в эксплуатацию	Процессор АЦП ЦАП Переходы	Задача Процедура Инструкция	Отказ Восстановление Введение в эксплуатацию	Монтаж Обработка Преобразование Формирование	Реактор Насос Компрессор Смеситель Размалыватель	Турбина Генератор Пароперегреватель Насос Трансформатор
Отношение Вес дуги	Логически Временной Материал	Логически Временной Материал Энергия	Логически Временной	Логически Временной			
Метки	Фактическое состояние развития Архивированные результаты	Данные, Параметр, Значение, Прерывание Неисправность	Данные, Значение Состояния-исключения	Исправное состояния Рабочее состояния	Фаза активных инструментов	Материальное состояние Состояние электропитания	

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.

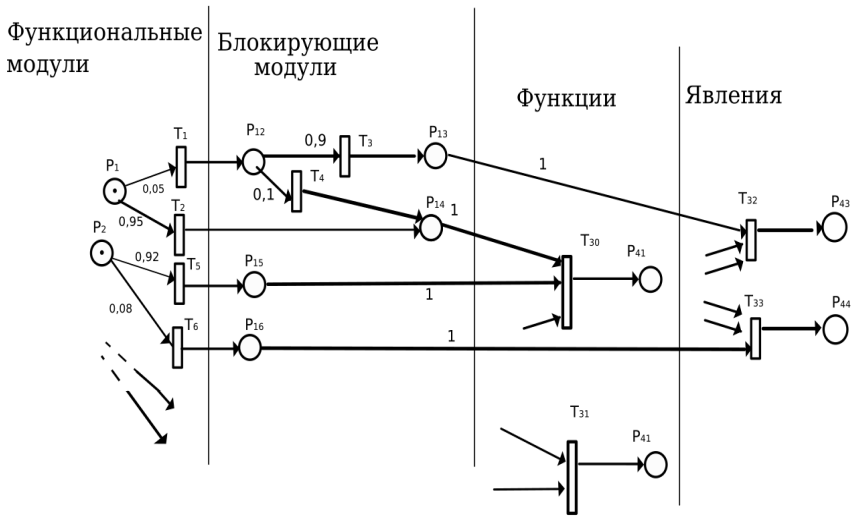


Рисунок 3.3 – Сеть Петри, моделирующая АСУ ТП с избыточностью

По описанным выше алгоритмам, методикам и механизмам находятся параметры, необходимые для вычисления функции приоритета. Покажем теперь полный процесс построения надежной структуры системой

3.6 Последовательность выполнения алгоритма

Работа системы представляет собой следующую последовательность действий.

Алгоритм разделен на насколько логических модулей, ряд которых в качестве исходных данных использует результат работы других модулей, а ряд может выполняться без предварительных вычислений. Именно с последних и должна начинаться работа с алгоритмом.

Первым шагом в выполнении алгоритма будет анализ и декомпозиция исходной системы. Исходными данными для декомпозиции является только структурная схема технологического процесса, что позволяет выполнить эту процедуру до выполнения остальных этапов.

Этап декомпозиции рассматривает структуру системы в масштабе модулей и позволяет получить общее представление о порядке повышения надежности, а также сведения о важности модулей, что является исходными данными для других процедур.

Началом будет перевод функциональной схемы процесса в схему структуры надежности (рисунки 3.3, 3.5).

Получившуюся схему структуры надежности нужно перевести в формат таблицы последовательностей.

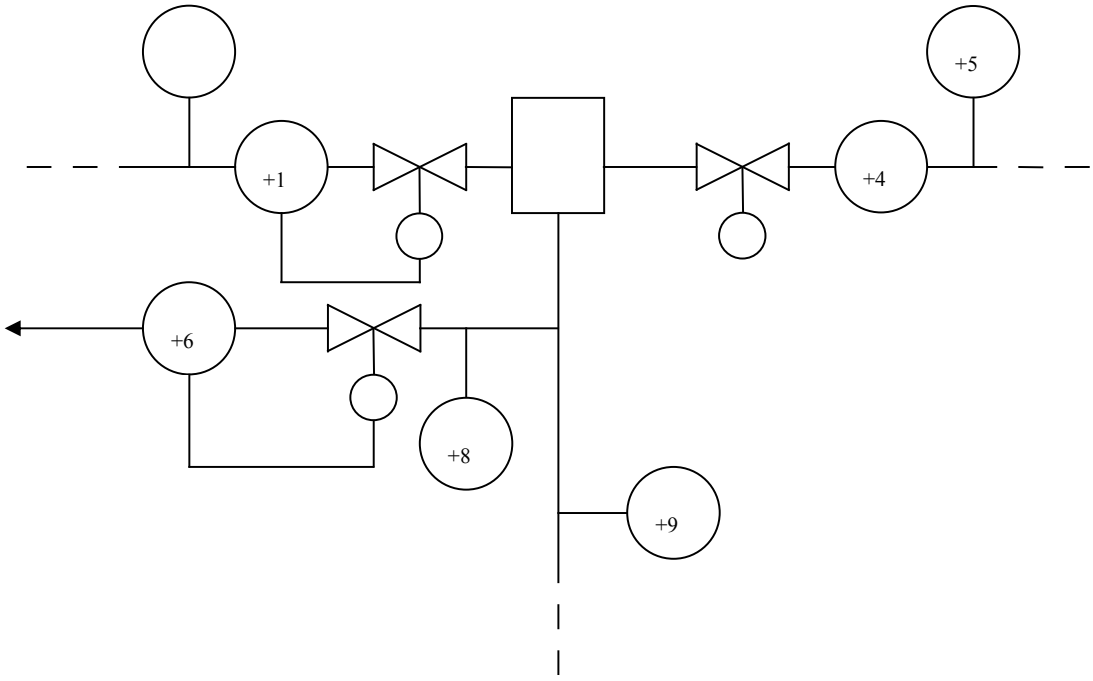


Рисунок 3.4 – Общий вид условной функциональной схемы процесса

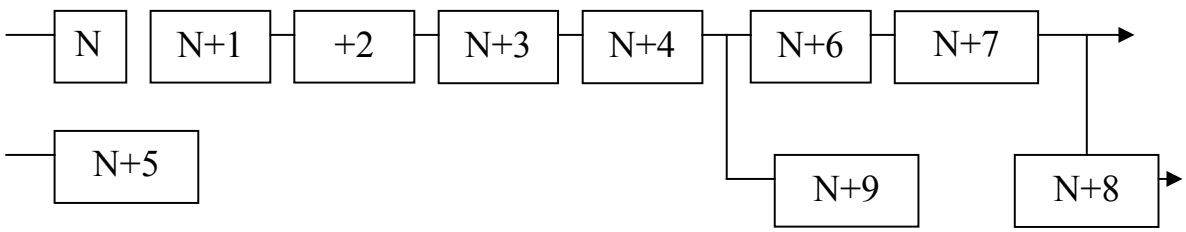


Рисунок 3.5 – Схема структуры надежности процесса

Результатом выполнения алгоритма будет множество последовательностей и множество весов элементов. Данное множество будет использовано при формировании резервированной системы. Но до начала ее формирования необходимо вычислить другие показатели.

Одним из таких показателей будет являться количественная оценка опасности отказа модулей, которая определяется при анализе схемы автоматизированного процесса испытания, вещества и среды.

Исходными данными для вычисления ущерба будет набор отказов, вызывающих ущерб. Он формируется исходя из структурной схемы отказов (рисунок 3.6).

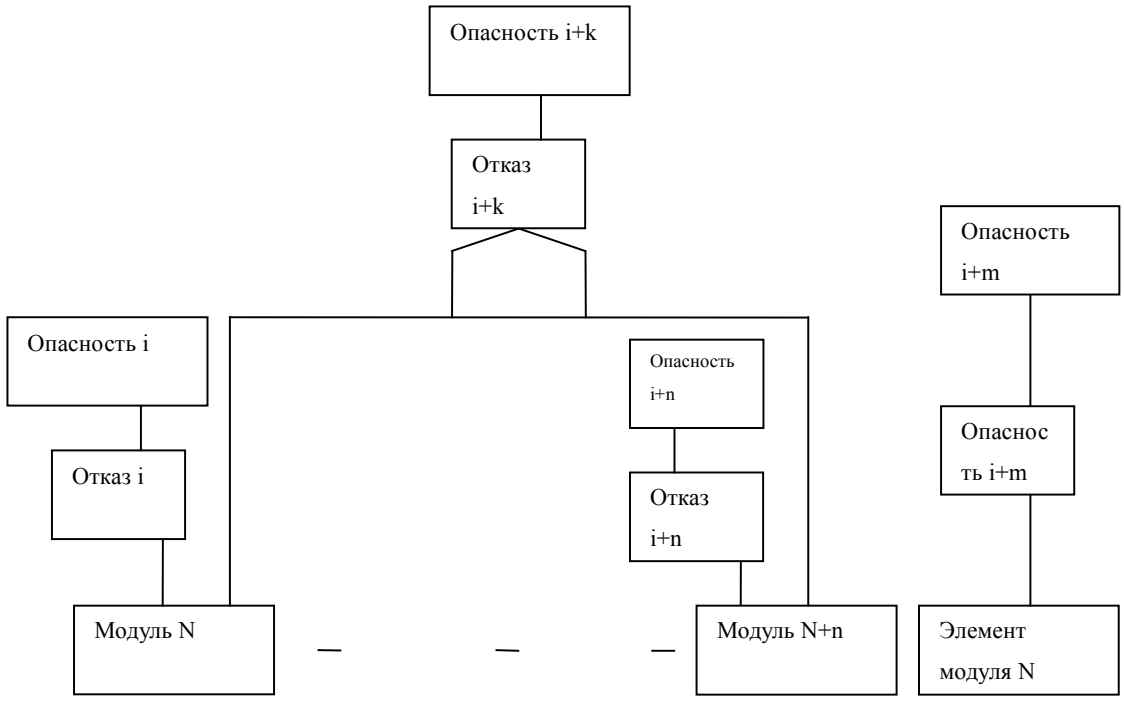


Рисунок 3.6 – Структурная схема отказов

Каждая оценка опасности переводится в численное выражение и записывается в массив *C*.

Дальнейшим действием будет назначение блокирующих опасности и отказы модулей. Исходными данными для этого этапа будут технологические свойства модулей, используемые ими энергии и вещества.

Для каждого модуля из массива типов модулей *T* выбирается один определенный тип. После выбора *j*-го типа *i*-го модуля алгоритмом

выполняется уменьшение k-го ограничения ресурсов L_k на величину $RBf_{j,k}$ или $RBd_{j,k}$ и уменьшение ущерба, вызываемого i-м модулем на HBd_i.

Далее заполняется массив M. Заполнение его производится исходя из функциональной схемы, определяющей типы и количество модулей, и технологических параметров процесса, показывающих, какими параметрами должны обладать элементы модулей.

Исходя из набора параметров элементов, для каждого модуля из ассортимента, представленного фирмами-производителями, выбираются версии модулей, подходящие под параметры.

Данные о расходах ресурсов на реализацию той или иной версии также получаются у производителей, а также поставщиков. Как уже было сказано, надежность вычисляется исходя из среднего времени между отказами (MTBF) и срока службы системы, определяемым на предыдущих этапах проектирования системы.

В начале 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, и начнется процесс приоритетного резервирования. Это обеспечивает наличие определенной величины вероятности отказа у каждого модуля.

После вычисления каждого аргумента функции приоритета получившийся массив Ra максимизируется:

$$Ra2 = \mathrm{Max}(Ra_i) \tag{3.36}$$

Затем находится, каким по счету в массиве Ra было значение $Ra2$. Эта величина o и будет номером модуля, в который добавляется очередной резервный элемент при каждой итерации.

$$Ra_i = Ra2 \Rightarrow o = i \tag{3.37}$$

Затем, если o-й модуль является нерезервируемым, находится ближайший резервируемый модуль.

Надежность *o*-го модуля, хранящаяся в Nm_o, модифицируется по формулам согласно назначенным данному модулю блокирующим опасность модулям:

$$P_o = P_{Bf_o}(P_o, n_{o1} \ldots n_{ok}) \tag{3.38}$$

Затем, исходя из типа резервирования, вычисляется новая надежность модуля:

$$M\{7, F\{o\}\} = \text{"г"} \Rightarrow Pm_o = 1 - (1 - Pm_o) * (1 - P_o) \tag{3.39}$$

$$M\{7, F\{o\}\} = \text{"х"} \ \lambda = 1 \Rightarrow Pm_o = P_o \tag{3.40}$$

$$M\{7, F\{o\}\} = \text{"х"} \ \lambda = 2 \Rightarrow Pm_o = P_o + \left(\frac{t \cdot P_o}{T}\right) \tag{3.41}$$

$$M\{7, F\{o\}\} = \text{"х"} \ \lambda = 3 \Rightarrow Pm_o = P_o + \left(\frac{t \cdot P_o}{T}\right) + \left(\frac{t}{T}\right)^2 \cdot \frac{P_o}{2} \tag{3.42}$$

Итоговая система с избыточностью изображается в виде двумерного массива *S*.

После вычисления надежности в систему заносится выбранная версия *o*-го модуля:

$$j = j + 1, S_{oj} = Nm_o, \tag{3.43}$$

где *j* – порядок резервирования *o*-го модуля.

Затем ресурсы, требуемые для этого модуля, вычитаются из пределов:

$$L_i = L_i - \text{M}\{i, Nm_o\} \tag{3.44}$$

Если $L_i = 0$, формирование системы завершается.

Если же $L_i < 0$, то восстанавливается расход ресурсов и находится такая версия модуля *o*, для которой

$$L_i > \text{M}\{i,k\}, k = [V_o \ldots F_o] \tag{3.45}$$

Она также заносится в S_{oj} , и вновь находится надежность *o*-го модуля. Затем также завершается формирование системы.

Результатом выполнения алгоритма будет структура сформированной системы и набор показателей.

Структура сформированной системы будет представлять собой массив сквозных номеров версий Sy_{ij}, где i – порядковый номер модуля, j – степень резервирования:

$$Sy_{ij} = No_i \tag{3.46}$$

Далее будет выводиться вероятность исправности всех модулей системы:

$$P_f = \prod_{i=1}^{n} Pm_i, \tag{3.47}$$

где P_f – вероятность исправности системы,

n – количество модулей в системе,

Pm_i – надежность i-го модуля.

Затем находится вероятность исправности только главной функциональной последовательности.

Таким образом, математически реализуется система анализа, учитывающая различные параметры надежности АСУ ТП и обеспечивающая более точный их учет.

Вычисления с использованием данных алгоритмов, механизмов и методик объемны, в связи с чем возникает необходимость их автоматизации.

3.7 Программная реализация системы

Вышеприведенный алгоритм является достаточно трудоемким для ручного вычисления. Для облегчения построения надежной системы следует автоматизировать его выполнение – создать программу, реализующую разработанную систему анализа. Данная программа будет реализовывать все приведенные методики и алгоритмы. Программа содержит в себе процедуры, выполняющие алгоритм учета опасностей, использующий предложенный способ их анализа, реализующие механизм включения блокирующих модулей и методику декомпозиции с учетом важности функции.

В качестве способа ввода параметров, необходимых для расчета, применяются таблицы.

Таблицами ввода параметров будет таблица версий модулей, соответствующая массиву M, таблица ограничений ресурсов (массив L),

таблица опасности (массив *D*), таблица функциональных последовательностей (массив *S*) и перечень типов модулей.

Данные для таблицы резервных элементов, таблицы последовательностей и таблицы безопасности хранятся во внешних файлах, предварительно заполняемых исходя из технических свойств системы. И первым шагом в выполнении программы будет чтение информации из них.

Таблицы ограничений и функциональных последовательностей заполняются пользователем исходя из имеющихся у него данных.

Данные о безотказности системы представлены в файлах в виде значений среднего времени между отказами. Следовательно, для вычисления вероятности безотказной работы необходимо вводить срок службы системы, для чего существует соответствующее поле. Далее пользователю следует заполнить перечни типов функциональных модулей, вынесенные на отдельную форму.

После заполнения всех элементов ввода информации пользователь запускает программу на выполнение.

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.

Исходя из введенных пользователем сведений о типах 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 системой вычисляются и выводятся ее итоговые показатели надежности.

Блочная схема автоматизированной системы представлена на рисунке 3.5. Структурная схема автоматизированной системы – на рисунке 3.6.

Таким образом программно реализуется автоматизированная система анализа 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.


Начало
Ввод срока службы системы
Заполнение массива функциональных последовательностей
Применение методики декомпозиции
Учёт важности
Получение веса weight[i] каждого модуля
Ввод данных о мультиверсиях модулей
Ввод оценки опасности
Исполнение алгоритма анализа и учёта опасностей
Ввод данных об выделяемых на систему ресурсах
Включение блокирующих модулей
Расходование ресурсов на блокирующие модули
Поиск версии каждого модуля с наименьшими ресурсами
Проверка допуска
Отсев непригодных для резервирования версий
Нахождение вероятности безотказной работы
Вычисление опасности отказа модулей и элементов
Поиск наинадежного модуля
1

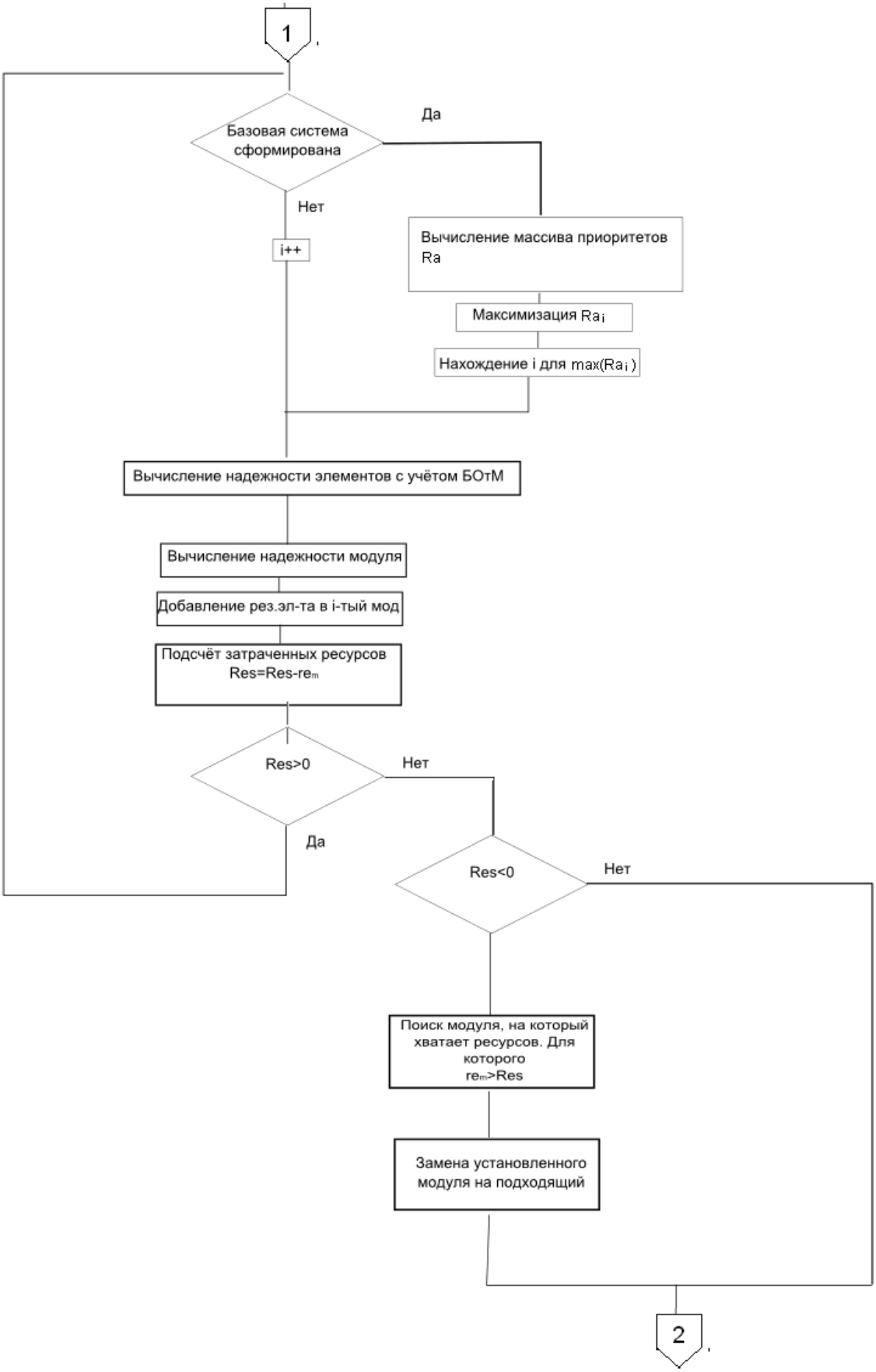

1
Базовая система сформирована
Да
Нет
i++
Вычисление массива приоритетов Ra
Максимизация Rai
Нахождение i для max(Rai)
Вычисление надежности элементов с учётом БОтМ
Вычисление надежности модуля
Добавление рез.эл-та в i-тый мод
Подсчёт затраченных ресурсов Res=Res-rem
Res>0
Нет
Да
Res<0
Нет
Поиск модуля, на который хватает ресурсов. Для которого rem>Res
Замена установленного модуля на подходящий
2

Рисунок 3.7 – Блочная схема автоматизированной системы

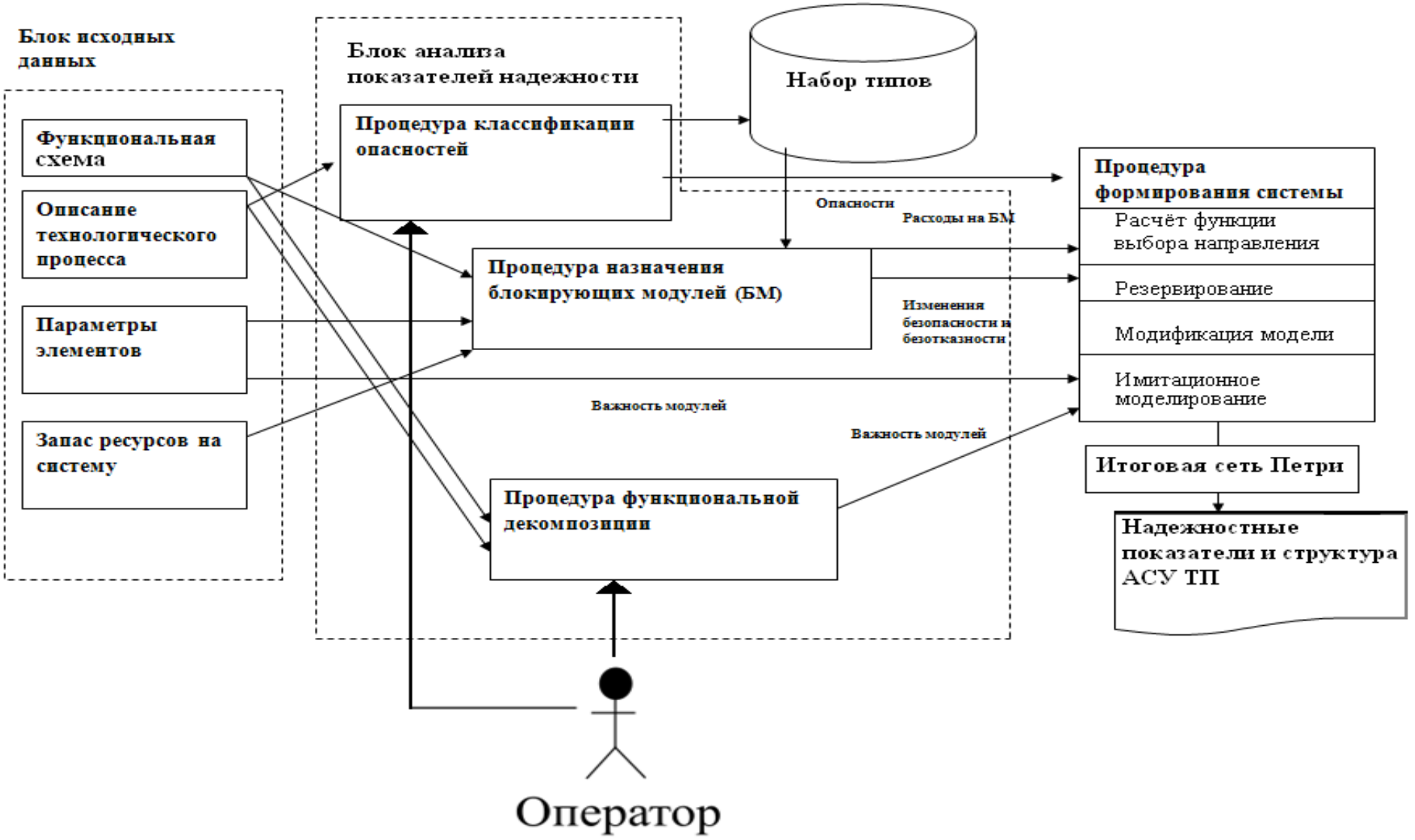


Рисунок 3.8 – Структурная схема автоматизированной системы

Вывод

1. В представленной системе применяется методика декомпозиции АСУ ТП на функциональные последовательности, в которой реализуется учет важности той или иной функции АСУ ТП, позволяющий ограничить последствия отказов, повышая вероятность безотказности наиболее существенных функций.

2. Также в ней реализуется разработанный алгоритм учета опасностей, способ их анализа, позволяющий системе дать оценку негативного эффекта избыточности, учесть случаи комплексных отказов и обеспечить приоритет резервирования модулей с наиболее опасными отказами.

3. Реализован механизм включения блокирующих модулей, позволяющих понизить вероятность отказов, а также уменьшить или полностью нейтрализовать опасные воздействия.

4. Приведенные алгоритмы, методики и методы реализуются в виде единой системы анализа надежности. Данная система автоматизируется.

4. Применение системы

Рассмотрим применение метода к реальным АСУ ТП.

В главе рассматривается АСУ опасных технологических процессов. В качестве первой рассматриваемой системы выбран участок процесса получения поликарбоната. В качестве второй – АСУ ТП испытания энергетического агрегата.

Данные технологические процессы выбраны исходя из высокой важности его надежной работы, так как они используют опасные вещества. Также причиной выбора этих технологических процессов является перспективность развития производства полимеров и энергетических агрегатов [3].

4.1 Анализ надежности участка АСУ ТП получения поликарбоната

Технологическое описание участка

Технологически участок описывается следующим образом (рисунок 4.1). Водный раствор дифенолята натрия непрерывно поступает в реактор 2 каскада реакторов. Сюда же подается метиленхлорид из резервуара 1 и фосген. Синтез поликарбоната на основе дифенолята проводится фосгенированием дифенолята, данный процесс протекает 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.

Системой анализа рассматривается надежность именно АСУ ТП.

Технологические аппараты надежней средств автоматизации из-за более высокой сложности последних.

Типичные устройства, вроде теплообменников, мешалок, экстракционных колонн, также при типичных условиях эксплуатации несут вполне определённую нагрузку, температуру, плотность или кислотность

среды, воздействие которой можно предусмотреть на стадии проектирования аппарата и применить соответствующие материалы, что обеспечит пренебрежимо малую интенсивность отказов.

Исправность и безотказность технологических аппаратов определяется параметрами технологического процесса, условиями, в которых они функционируют, и, следовательно, исправностью средств сбора и обработки информации, регулирования параметров.

То, что отказы оборудования происходят из-за значительного отклонения технологических параметров, определяет подход к повышению надежности управления этими параметрами.

При расчёте надежности следует учитывать исправность средств, регулирующих параметры эксплуатации. Средства автоматизации функционально связаны с оборудованием, осуществляющим технологический процесс.

Схема технологического процесса представлена на рисунке 4.1.

Сбор исходных данных для анализа надежности

Первым шагом в анализе надежности будет нахождение для каждого модуля максимально надежной версии.

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) для измерения расхода газа. Регулируется расход фосгена клапаном (4-2), выполненном в специальном исполнении для регуляции опасных веществ.

Уровень метиленхлорида в резервуаре 1 контролируется расходомером LT (1-1). Реакционная смесь перемешивается в реакторе мешалкой с приводом M1.

Температура в реакторе стабилизирована, реакционная смесь подогревается горячей водой. Температура смеси измеряется датчиком TT (5-1), расход воды регулируется клапаном (5-2).

Уровень реакционной смеси в реакторе контролируется уровнемером LT (3-1).

Измерительная информация от процесса передаётся на шину сбора данных ET200m. Включение шины сбора данных в АСУ обеспечивает дополнительный потенциал для резервирования верхнего уровня.

Предполагая в качестве устройств автоматизации высокого уровня устройства из номенклатуры Simatic, выбираем количество (и тип) модулей.

Шина сбора данных и управления ET200m формируется из интерфейсного модуля IM, модуля питания PS и модулей ввода-вывода. Набор модулей сбора данных формируется исходя из количества входов (выходов) в данном модуле и количества входных и выходных сигналов от датчиков и к исполнительным устройствам.

Данные, собранные шиной, передаются на контроллер.

Каждый из модулей ввода-вывода включаются в структуру системы один раз, так как их отказ в любом случае приведёт к отказу функциональной последовательности, к которой они принадлежат.

Несмотря на то, что один модуль собирает, обрабатывает и выводит несколько сигналов, они находятся в одной последовательности, так как каждая функция АСУ предполагает сбор и обработку информации, иначе пропадает факт управления и АСУ перестаёт быть таковой [68,69, 103, 104, 105].

В качестве контроллера применяется контроллер S7-400h, допускающий резервирование.

Все датчики и устройства сбора данных подключаются к контроллерам через станции распределённой периферии ET 200M производства SIEMENS AG. Станция распределённой периферии ET 200M представляет собой конструкцию формата серии SIMATIC S7-400, состоящую из профильной шины с возможностью «горячей замены» любого модуля, интерфейсного модуля IM 153-2, набора модулей аналогового и дискретного ввода/вывода S7-400 и батареи питания PS 307. Интерфейсные модули IM 153-2

осуществляют подключение станции ET 200M к процессорам системы PLC S7-400, используя шину PROFIBUS-DP на скорости до 12 Mbps. Встроенные средства диагностики модулей и станций ET 200M обеспечивают возможность мониторинга состояния каждого модуля и всей стойки в целом на операторских и инжиниринговых станциях верхнего уровня.

В системе используются следующие модули ввода-вывода производства SIEMENS AG:

- модуль аналогового ввода SM 331 – 8 оптоизолированных аналоговых входов, ввод токового сигнала 4…20 мА или сигнала с термопреобразователей сопротивления;
- модуль дискретного ввода SM 321 – 32 оптоизолированных дискретных входа 24V DC
- модуль аналогового вывода SM 332 – 4 оптоизолированных аналоговых выхода, вывод токового сигнала 4…20 мА;
- модуль дискретного вывода SM 322 – 16 оптоизолированных дискретных вывода 24V DC/0.5A.

Параметрирование и программирование станций распределённого ввода/вывода и сети PROFIBUS-DP осуществляется с помощью стандартного программного обеспечения STEP7 от SIEMENS AG, входящего в комплект инжинирингового программного обеспечения PCS7 на инжиниринговых станциях и программаторах [63, 72].

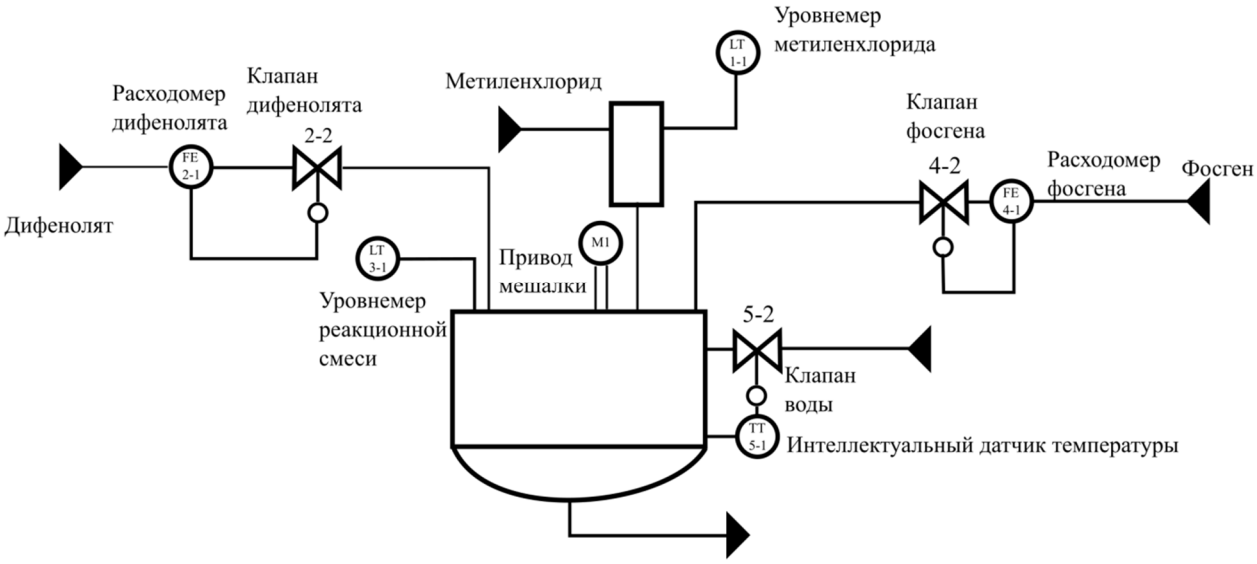


Рисунок 4.1 – Схема технологического процесса

Необходимо учитывать, что элементы шины сбора данных ET200m являются неотъемлемыми частями шины, поэтому данное устройство должно резервироваться целиком. Таким же неразделяемыми элементами являются электропневмопреобразователи на клапанах [73]. Все возможные версии реализации перечисленных модулей приведены в таблице 4.1.

Таблица 4.1 – Список версий модулей

№	№ сквоз	Обозначение	Название	Модель	MTBF (срок службы)
1	2	3	4	5	6
1	1	FE (2-1)	Измерение расхода дифенолята	Promass 80, 83	57 лет
2	2	(2-2),3	Клапан дифенолята с ЭП	26нж18кр ЭП3211	5,4 года
		IM	Интерфейсный модуль IM	IM154-4	45 лет
		PS	Блок питания PS	SITOP	45 лет
		AI	Модуль аналогового ввода	SM336	63 года
		AO	Модуль аналогового вывода	SM332	63 года
		DI	Модуль дискретного ввода	SM326	81 год
		DO	Модуль дискретного вывода	SM322	81 год
3	3	ET	Шина сбора данных	ET200m	9,9 лет
4	4	CPU	Контроллер	Simatic S7-400HF	35 лет
5	5	FE (4-1)	Измерение расхода фосгена	Promass 80, 83	57 лет
6	6	(4-2)	Клапан фосгена с ЭП	Fluoroseal (ЭП3211)	8 лет
7	7	TT (5-1)	Интеллектуальный измеритель температуры	Метран 281	3 года

1	2	3	4	5	6
	8			Метран 286	6 лет
	9			Метран 288	4 года
	10			Метран 231	~3 года
8	11	(5-2)	Регулирование расхода воды	25кч945нж ЭП 3211	5 лет
9	12	M1	Привод мешалки	Двигатель (АИР80а2)	12 лет
10	13	LT (1-1)	Уровнемер	Rosemount 5600	12 лет
	14			Rosemount 5300	12 лет
	15			Rosemount 3300	17 лет
11	16	LT(3-1)	Уровнемер	Rosemount 5600	12 лет
	17			Rosemount 5300	12 лет
	18			Rosemount 3300	17 лет

Для сравнения эффективности известных методов повышения надежности с предлаемым, приведем показатели надежности, полученные с их применением. 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 нами метод, получим следующие результаты.

В результате 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.

Контролируемыми параметрами является уровень метиленхлорида в резервуаре 1, уровень реагирующих веществ в реакторе 2.

Регулируемыми параметрами будут расход фосгена, расход дифенолята натрия, температура в реакторе 2.

Функциями, выполняемыми системой, будут функция получения реакционной смеси и функции контроля уровня в резервуаре 1 и реакторе 2.

Для выполнения функции контроля уровня метиленхлорида в резервуаре 1 необходимо, чтоб исправным были шина сбора данных ET200m и контроллер S7200h.

Для исправности функции контроля уровня реакционной смеси в реакторе 2 необходимо, чтоб данная смесь была правильно составлена. Таким образом, необходимо, чтоб были исправны контур регулирования дифенолята (расходомер FE (2-1) и клапан (2-2) с электропневмопреобразователем), контур регулирования фосгена (расходомер FE (4-1) и клапан (4-2) с электропневмопреобразователем) и воды (датчик температуры TT (8-1) и клапан (8-2) с электропневмопреобразователем). Также необходима исправность привода M1 и, собственно, уровнемера LT (3-1).

Для исправности функции получения реакционной смеси также необходима исправность всех контуров регулирования, верхнего уровня автоматизации - шины сбора данных и контроллера.

Вышеприведённые последовательности переводятся в формат массива последовательностей, используемый процедурой функциональной декомпозиции.

Вводятся точки разветвления структуры системы, количество модулей в каждом ответвлении последовательности и важность этой последовательности.

Важность – параметр, показывающий, насколько важен модуль той или иной последовательности для достижения системой своей цели.

По предложенной методике декомпозиции возможным множеством значений W важности могут быть:

2 - модуль, участвующий в регулировании технологического процесса или в его выполнении.

1 – модуль, участвующий в сборе информации о параметре процесса.

Важность W=2 выбирается для первой функции – функции получения реакционной смеси.

Важность W=1 – для функций контроля уровней в накопителе и реакторе.

Полученный массив приведён в таблице 4.2.

Структурная схема технологического процесса приведена на рисунке 4.2, цифры соответствуют номеру модуля из таблицы 4.1.

Таблица 4.2 – Массив последовательностей для процедуры декомпозиции

Количество модулей главной последовательности	Количество модулей ответвляющейся последовательности	Важность последовательности
9	0	2
4	1	1
9	1	1

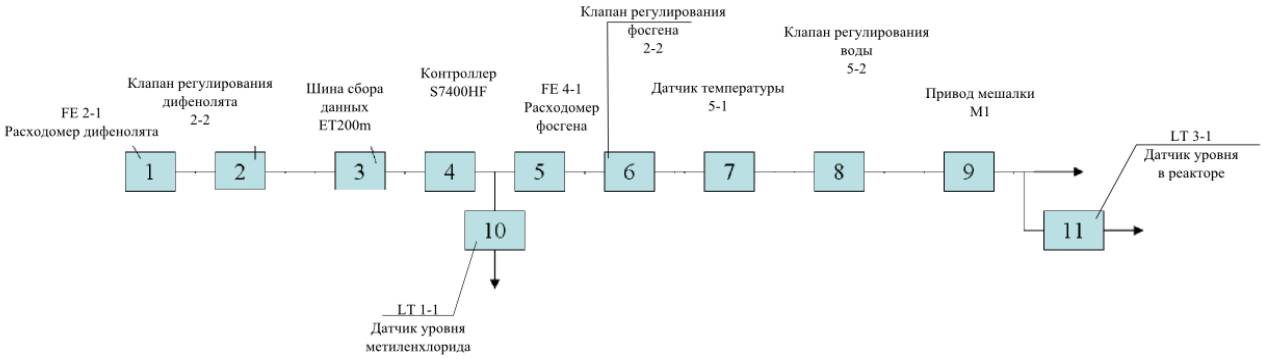


Рисунок 4.2 – Структурная схема технологического процесса

Учёт опасностей участка получения поликарбоната

Дальнейшим действием будет применение алгоритма учета опасностей технологического процесса.

В процессе используются два вида опасных веществ с автоматической регуляцией. Следовательно, отказы клапанов, регулирующих расход этих веществ, может нести опасность. Для анализа опасности строится схема структуры событий, приведённая на рисунке 4.3.

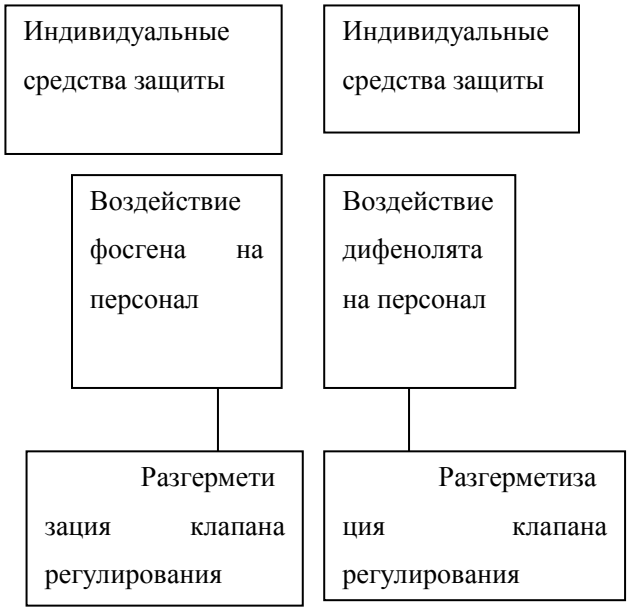


Рисунок 4.3 – Схема структуры событий

Следующим этапом будет определение количественной оценки опасности, несомой отказами модулей по алгоритму учёта опасностей.

Прекращение подачи метиленхлорида не рассматривается в качестве возможного отказа, так как регулирование его расхода лежит за пределами рассматриваемой системы.

Разгерметизация клапана дифенолята может привести к разливу данного вещества и воздействию его на персонал.

Разгерметизация клапана фосгена – также приведёт к воздействию его на персонал.

Для оценки опасности того или иного отказа необходимо знать величину средне-смертельной концентрации веществ (ССКВ) в воздухе в случае фосгена и среднесмертельной концентрации при попадании внутрь в случае дифенолята.

В случае с фосгеном ССКВ составляет 334 мг/м^3, в случае с фенолом – 427 мг/кг [25, 48].

Целевая вероятность безотказной работы всей АСУ ТП будет равна 0,99. Для того чтоб считаться достаточно безопасной, она должна будет иметь

SIL 3, исходя из чего целевой вероятностью безопасной работы клапанов будет 0,994 и 0,989 соответственно.

Полученная информация сводится (таблица 4.3) и используется процедурой классификации опасностей системы.

Таблица 4.3 – Классификация опасностей системы

Первая причина	Вторая причина	Следствие	Количественная оценка опасности (средне-смертельная концентрация)	Источник опасности
Разгерметизация клапана фосгена (клапана 4-2)	Отсутствует	Воздействие фосгена на персонал	334 мг/м^3	Элемент
Разгерметизация клапана фенола (клапана (2-2))	Отсутствует	Воздействие фенола на персонал	427 мг/кг	Элемент

Построение безопасной структуры АСУ ТП с избыточностью

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 (3.7).

Идентифицировав опасности, необходимо задействовать механизм включения блокирующих опасности и отказы модулей (БМ). Для включения блокирующих опасности модулей необходимо определить, к какому типу относятся модули с опасными отказами.

Модуль регуляции расхода фосгена – клапан, регулирующий расход газов. Следовательно, модулем используется опасный газ. Для защиты от газообразных АХОВ применяются средства индивидуальной защиты органов дыхания.

Фосген является химическим веществом 2ого класса опасности.

Защита от воздействия фосгена - использование противогаза [39,49].

Модуль регуляции фенола – клапан, регулирующий расход раствора. Для защиты от жидких АХОВ используются средства индивидуальной защиты.

При работе с фенолом следует применять средства индивидуальной защиты от попадания продукта на кожные покровы и слизистые оболочки в соответствии с типовыми отраслевыми нормами бесплатной выдачи специальной одежды, специальной обуви и других средств защиты рабочих и служащих химических производств [19].

Блокирующие отказы модули выбираются исходя из используемых функциональными модулями энергий. Модули, использующие электрическую энергию напряжением 220 вольт, запитываются от источников бесперебойного питания, которые служат блокирующими отказы модулями, так как предотвращают лишние циклы включения-выключения и скачки напряжения. Выбранные блокирующие модули приведены в таблице 4.4.

Таблица 4.4 - Блокирующие модули

№	Модуль функциональный	Модуль блокирующий	Цена
1	FE (2-1)	ИБП	2
2	Клапан фенола (2-2)	Индивидуальные СЗ	21
3	ET	ИБП	2
4	CPU	ИБП	2
5	FE 4-1	ИБП	2
6	Клапан фосгена (4-2,3)	Противогазы	25
7	TT 5-1	ИБП	2

Следующим этапом работы системы анализа является процедура формирования автоматизированной системы управления. Для формирования системы выделяется объём ресурсов в размере 1 200 тыс. руб.

Проверяя прохождение допуска, система определяет, что все модули проходят допуск и по объёму требуемых ресурсов пригодны для резервирования.

Теперь применим автоматизированную систему анализа надежности и сравним результаты их работы.

Интерфейс ввода представлен на рисунке 4.4, 4.5.

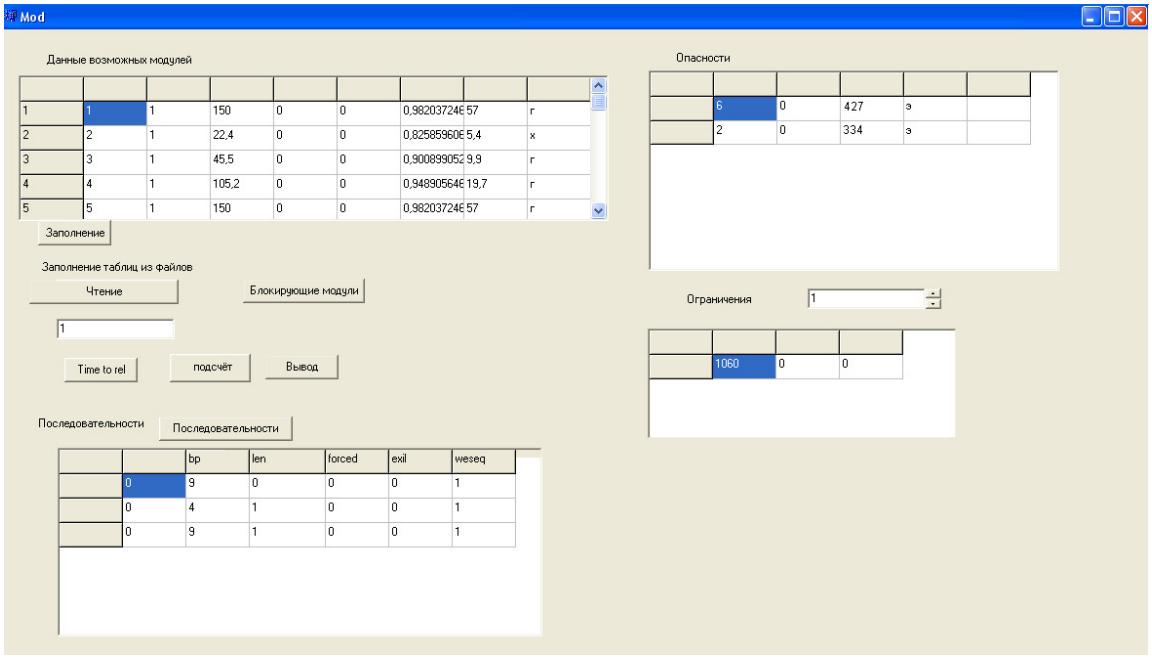


Рисунок 4.4 – Интерфейс ввода параметров надежности

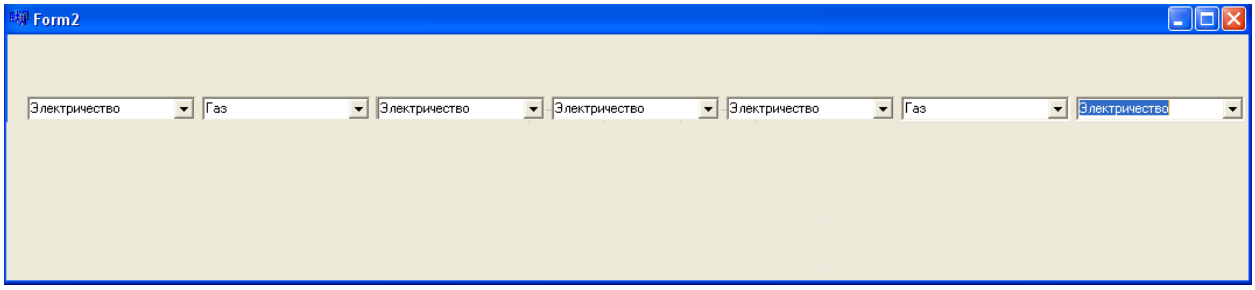
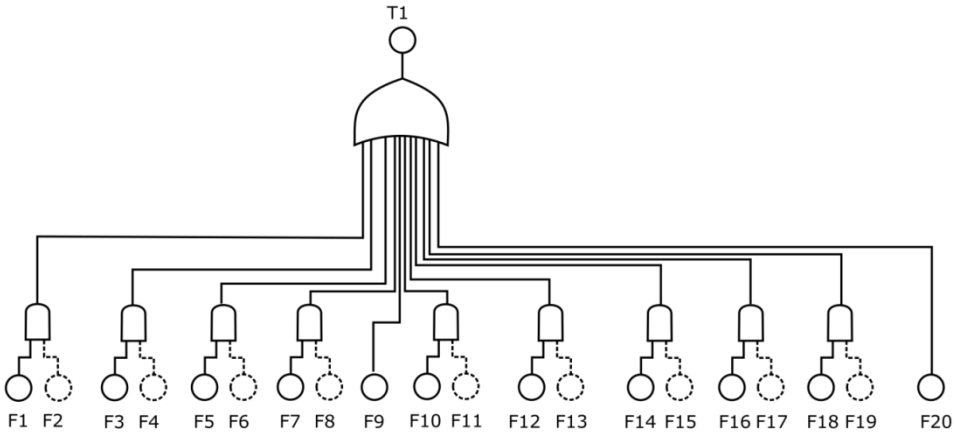


Рисунок 4.5 - Интерфейс ввода типов блокирующих модулей

Представление структуры АСУ ТП

В результате работы автоматизированной системы с учётом приоритетов резервирования, формируется структура системы с

избыточностью, учитывающая опасность и важность модулей, выбирается целевая вероятность безотказной работы, отношение интенсивности безопасных отказов к интенсивности всех отказов, а так же вводится набор блокирующих опасность и отказы модулей. Вероятность исправной работы АСУ, построенной с учётом безопасности и блокирования отказов даёт вероятность безотказной работы главной функции – 0,94, а всей системы – 0,96. На рисунке 4.6 приведено дерево отказов созданной АСУ ТП с введенными резервными модулями, выделенными пунктиром. Оно использует аппарат и обозначения математической логики и позволяет проследить возникновение событий в системе. Таким событиями будет отказ всей системы или главной её функции.



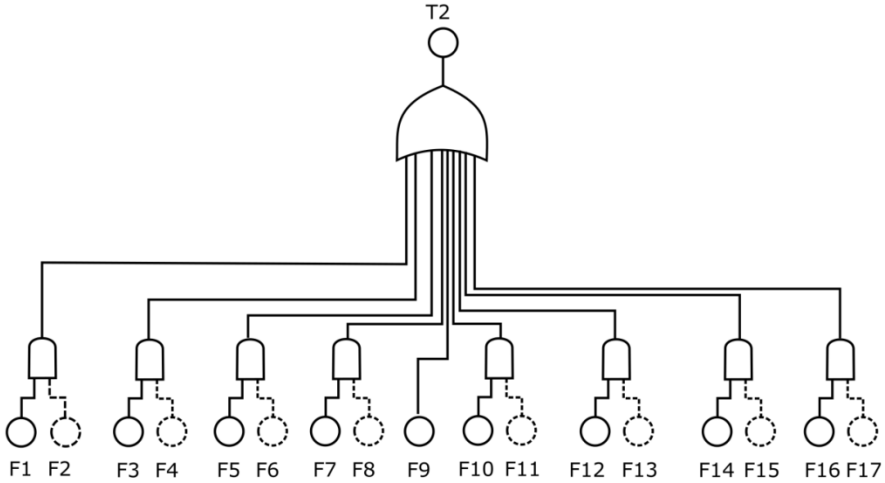


Рисунок 4.6 – Деревья отказов АСУ ТП

Обозначение событий, представленных в дереве отказов приведены ниже

F1 - Отказ основного расходомера дифенолята;

F2 - Отказ резервного расходомера дифенолята;

F3 - Отказ основного клапана дифенолята;

F4 - Отказ резервного клапана дифенолята;

F5 - Отказ основной шины сбора данных;

F6 - Отказ резервной шины сбора данных;

F7 - Отказ основного контроллера;

F8 - Отказ резервного контроллера;

F9 - Отказ расходомера фосгена;

F10 - Отказ основного клапана фосгена;

F11 - Отказ резервного клапана фосгена;

F12 - Отказ основного термопреобразователя;

F13 - Отказ резервного термопреобразователя;

F14 - Отказ основного клапана теплоносителя;

F15 - Отказ резервного клапана теплоносителя;

F16 - Отказ основного привода;

F17 - Отказ резервного привода;

F18 - Отказ основного уровнемера метиленхлорида;

F19 - Отказ резервного уровнемера метиленхлорида;

F20 - Отказ уровнемера реакционной смеси;

T1 - Отказ всей АСУ ТП;

T2 - Отказ функции регулирования АСУ ТП.

Выходные параметры, рассчитанные автоматизированной системой анализа надежности – на рисунке 4.7.

Модуль 11 не резервируется, так как его важность ниже остальных, так как он выполняет функцию контроля.

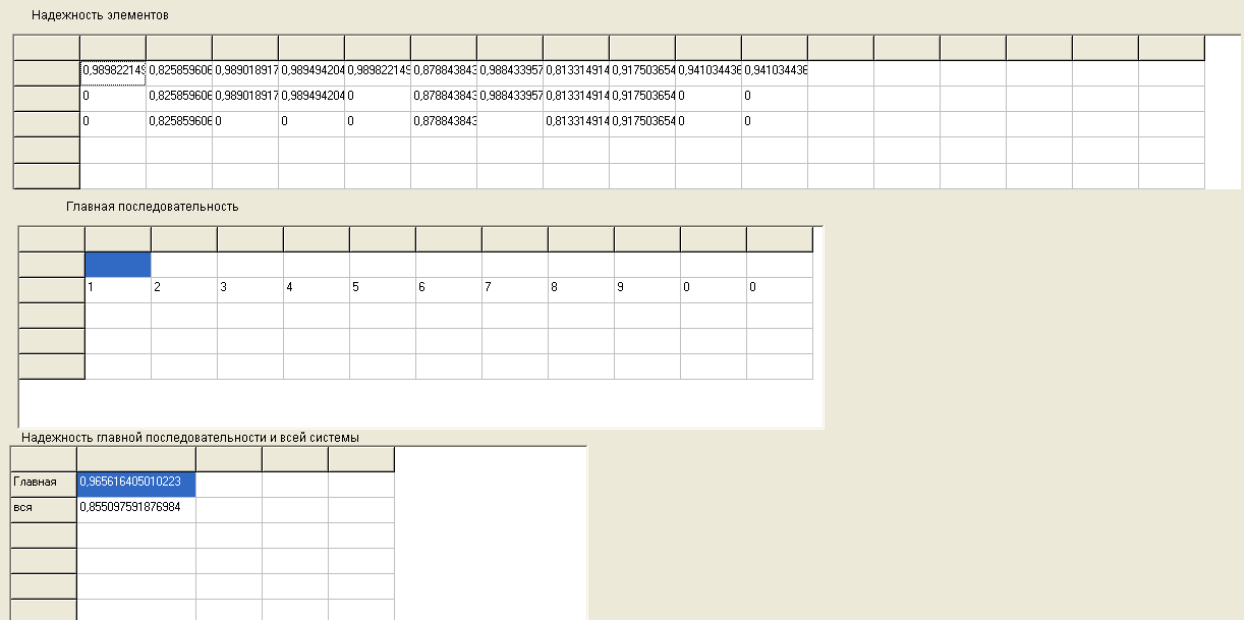


Рисунок 4.7 – Интерфейс вывода показателей надежности АСУ ТП

Для проверки итоговой надежности АСУ ТП следует провести эксперимент, имитирующий сетью Петри процесс возникновения отказов в системе.

Состояние всей системы определяется по формулам. Надежность АСУ ТП, построенной при помощи системы анализа надежности:

$$T1 = (F1 \vee F2) \wedge (F1 \vee F2) \wedge (F3 \vee F4) \wedge (F5 \vee F6) \wedge (F7 \vee F8) \wedge F9 \wedge (F10 \vee F11) \wedge (F12 \vee F13) \wedge (F14 \vee F15) \wedge (F16 \vee F17) \wedge (F18 \vee F19) \wedge F20$$

Надежность главной функции АСУ ТП, построенной при помощи системы анализа надежности:

$$T2 = (F1 \vee F2) \wedge (F1 \vee F2) \wedge (F3 \vee F4) \wedge (F5 \vee F6) \wedge (F7 \vee F8) \wedge F9 \wedge (F10 \vee F11) \wedge (F12 \vee F13) \wedge (F14 \vee F15) \wedge (F16 \vee F17)$$

Вероятность исправной работы АСУ, построенной с учётом безопасности и блокирования отказов даёт вероятность безотказной работы главной функции 0,94, а всей системы – 0,96, что приводит к повышению вероятности безотказной работы главной функции на 7,8%, а всей системы на 8%.

4.2 Анализ надежности АСУ ТП испытания

Второй рассматриваемой системой будет автоматизированная система управления технологическим процессом испытания энергетических агрегатов.

Рассматриваемой системой будет участок автоматизированной системы испытания агрегатов, собирающий информацию об их параметрах. Данный участок был выбран исходя из актуальности повышения надежности испытания. Примером подобного энергетического агрегата могут быть газотурбинные установки, использующиеся в различных отраслях промышленности, в том числе для транспортировки газа [117].

Описание системы испытаний

В своей работе агрегат использует топливную смесь. Подача компонентов топлива регулируется контуром управления, включающим в себя датчики расхода топлива и окислителя FEт и FEо, клапанами КТ и КО. В качестве топлива может быть рассмотрен природный газ, в качестве окислителя кислород, который в свою очередь может быть применен в различных видах, от атмосферного воздуха до сжиженного. Причем, в качестве условия агрегат оснащён набором датчиков – температуры, давления, вибрации, уровня, а также датчиком качества работы агрегата.

Информация с датчиков и на исполнительный механизм клапана топлива передаётся через промышленную сеть.

Для преобразования измерительной и управляющей информацией применяются конвертеры Ethernet.

Собранная в ходе работы энергетического агрегата информация собирается и выводится на промышленный компьютер.

Температура во время его работы считывается набором датчиков температуры, условно обозначенных на структурной схеме как «ТТ». Сбор информации о давлении, вибрации и качестве - соответственно датчиками «РТ», «VT» и «Q». Дополнительно датчиками, обозначенными $LT_т$ и $LT_о$

контролируется уровень компонентов в баках, из которых они подаются к испытательной установке.

Подача топлива регулируется контуром управления, включающим в себя датчики расхода топлива и окислителя $FE_т$ и $FE_о$, клапанами КТ и КО.

Автоматизированной системой анализа надежности рассматривается и повышается только надежность средств АСУ ТП.

Безотказность же самого испытываемого энергетического агрегата является контролируемым показателем. Повышение надежности агрегата является предметом отдельного цикла работ и никак не пересекается с повышением надежности испытаний.

В качестве устройств автоматизации высокого уровня выберем устройства из номенклатуры Simatic – шину сбора данных ET200m и контроллер S7400h.

В системе используются модули ввода-вывода производства SIEMENS. Шина сбора данных и управления ET200m формируется из интерфейсного модуля IM, модуля питания PS и модулей ввода-вывода. Данные, собранные шиной, передаются на контроллер.

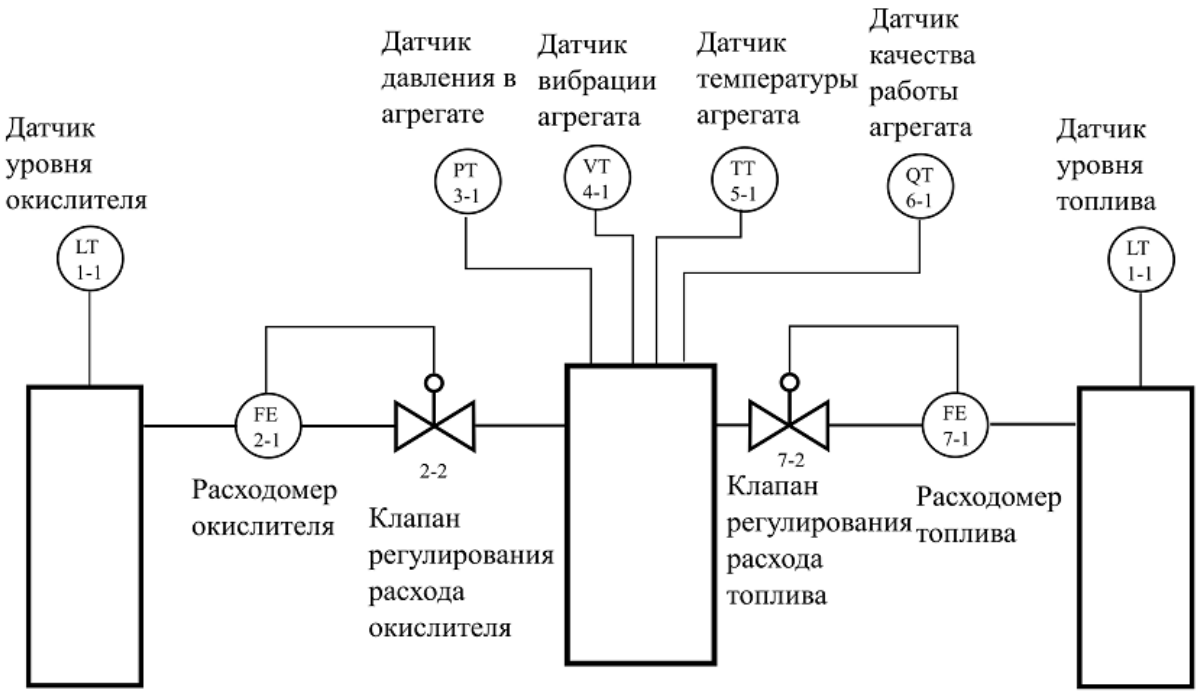


Рисунок 4.8 – Схема процесса испытания

Необходимо учитывать, что элементы шины сбора данных ET200m являются неотъемлемыми частями шины, поэтому данное устройство должно резервироваться целиком.

Все возможные версии реализации перечисленных модулей приведены в таблице 4.1.

Таблица 4.1 – Список версий модулей

№ модуля	Обозначение	Название	MTBF (срок службы)	Цена, тыс. руб.
1	TT	Интеллектуальный измеритель температуры	13 лет	120
2	PTд	Датчик давления	13 лет	100
3	FEo	Измерение расхода	13 лет	200
4	FEт	Измерение расхода	13 лет	200
5	KT	Клапан	27 лет	150
6	KO	Клапан	27 лет	150
7	ET	Шина сбора данных (укомплектованная)	45 лет	80
8	CPU	Контроллер	45 лет	80
9	APM	Персональный компьютер	10 лет	30
10	Q	Датчик	11 лет	125
11	VT	Вибродатчик	12 лет	125
12	SITOP	Блок питания	80 лет	60
13	LTo	Датчик уровня	13 лет	100
14	LTт	Датчик уровня	13 лет	100

Таблица 4.2 - Структура шины сбора данных

IM	Интерфейсный модуль IM	IM154-4
PS	Блок питания PS	SITOP
AI	Модуль аналогового ввода	SM336
AO	Модуль аналогового вывода	SM332

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 Ps1 равная 0,974.

Сбор исходных данных для анализа надежности АСУ ТП испытаний

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 испытательной установки.

Автоматизированная система испытаний собирает информацию о температуре, вибрации в турбине, а также обеспечивает работу самого энергетического агрегата, подачу в него компонентов топливно-воздушной смеси.

Дополнительно система контролирует наличие давления в трубопроводах подачи топливно-воздушной смеси.

По предложенной методике декомпозиции возможным множеством значений W важности могут быть:

2 – модуль, участвующий в сборе информации об испытываемом энергетическом агрегате или обеспечивающий его работу.

1 – модуль, участвующий в контроле параметров самой автоматизированной системы испытаний или иных параметров, не относящихся к испытываемому энергетическому агрегату.

Важность W=2 выбирается для первой функции – функции получения данных о параметрах работы агрегата.

Важность W=1 – для функций контроля давления в трубопроводах компонентов топливно-воздушной смеси.

Заметим, что функция получения данных о параметрах работы агрегата может быть разделена на одинаково важные подфункции сбора каждого отдельного параметра для более детализированной оценки безотказности системы.

Определяются модули, выполняющие эти функции, функции сбора информации об испытании назначается высокая важность (w=2), а функции контроля параметров испытательной установки назначается важность низкая. Для модулей, выполняющих только её, понижается приоритет резервирования.

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.

Первым шагом в анализе надежности будет нахождение для каждого модуля максимально надежной версии.

Следующим шагом будет разбиение системы на функции по разработанной методике декомпозиции.

По результатам декомпозиции получена структурная схема, представленная на рисунке 2. Номера модулей указаны в соответствии с таблицей 1.

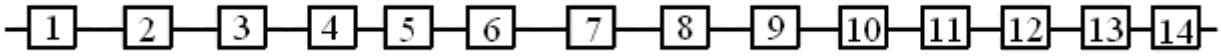


Рисунок 4.9 – Структурная схема АСУ ТП испытаний

Учёт опасностей процесса испытаний

Дальнейшим действием будет применение алгоритма учета опасностей технологического процесса.

В процессе используются опасное вещество с автоматической регуляцией. Следовательно, отказы клапана, регулирующего расход этого вещества, может нести опасность. Для анализа опасности строится схема структуры событий, приведённая на рисунке 4.3.

Рисунок 4.10 – Схема структуры событий

Разгерметизация клапана может привести к воздействию его на персонал.

Для оценки опасности отказа необходимо знать величину средне-смертельной концентрации вещества (ССКВ) в воздухе.

Далее по алгоритму выбирается целевая вероятность безотказной работы, равная 97% которую система анализа надежности будет стараться обеспечить и к которой будет стремиться вероятность безотказной работы АСУ ТП, структуру которой она синтезирует.

Показатель доли безопасных отказов SFF выбираем равным 90%, что соответствует третьему уровню интегральной безопасности.

Полученная информация сводится (таблица 4.3) и используется процедурой классификации опасностей системы.

Таблица 4.3 – Классификация опасностей системы

Первая причина	Вторая причина	Следствие	Количественная оценка опасности (средне-смертельная концентрация)	Место возникновения отказа
Разгерметизация клапана КТ		Воздействие топлива на персонал	400	Элемент

При целевой вероятности безотказной работы равной 97%, вероятность отказа будет составлять 3%.

Для обеспечения целевой доли безопасных отказов вероятность опасного отказа должна составлять 10% от этой величины, то есть 0,3%.

Опасный отказ наступает, когда отказывает клапан КТ. Следовательно, целевая вероятность отказа отдельного модуля 0,0015, вероятность безотказной работы 0,9985.

Причём данной вероятностью безотказной работы должен обладать именно отдельный клапан.

Построение безопасной структуры АСУ ТП с избыточностью

Идентифицировав опасности, необходимо задействовать механизм включения блокирующих опасности и отказы модулей (БМ). Для включения блокирующих опасности модулей необходимо определить, к какому типу относятся модули с опасными отказами.

Модуль регуляции расхода – клапан, регулирующий расход газов. Следовательно, модулем используется опасный газ. Для защиты от газообразных АХОВ применяются средства индивидуальной защиты органов дыхания.

Защита от воздействия - использование противогаза [39,49].

Блокирующие отказы модули выбираются исходя из используемых функциональными модулями энергий. Модули, использующие электрическую энергию, питаются от источников бесперебойного питания, которые служат блокирующими отказы модулями, так как предотвращают лишние циклы включения-выключения и скачки напряжения.

Таблица 4.4 - Блокирующие модули

№	Модуль функциональный	Модуль блокирующий	Цена
1	Датчики	ИБП	2
3	Клапаны	Противогазы	21
3	ET	ИБП	2
5	CPU	ИБП	2

Следующим этапом работы системы анализа является процедура формирования автоматизированной системы управления. Для формирования системы выделяется объём ресурсов в размере 2200 тыс. руб.

Сравним эффективность построения структуры АСУ ТП при помощи базового метода наискорейшего спуска и при помощи разработанной нами системы анализа.

Метод предусматривает добавление в систему модулей, отдавая приоритет резервирования модулям с наименьшей вероятностью безотказной работы.

Итогом расчёта, учитывающего только безотказность, будет структура системы с избыточностью, обеспечивающая безотказность.

Все элементы, кроме контроллера, шины сбора данных и блоков питания, резервируются.

В результате работы автоматизированной системы с учётом приоритетов резервирования, формируется структура системы с избыточностью, учитывающая опасность и важность модулей, выбирается целевая вероятность безотказной работы, отношение интенсивности безопасных отказов к интенсивности всех отказов, а так же вводится набор блокирующих опасность и отказы модулей.

Модули РТо и РТт не резервируются, так как его важность ниже остальных, он выполняет функцию контроля параметров самой АСУ ТП.

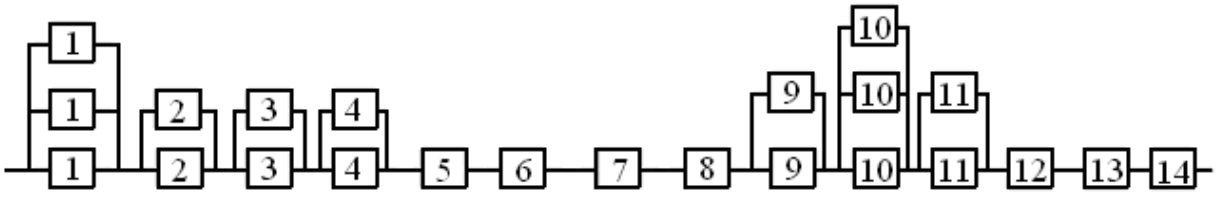


Рисунок 4.11 – Структура АСУ ТП, построенная с учетом приоритета

Система анализа надежности использует эти данные и предлагает структуру АСУ с вероятностью исправности всей системы P, равной 0,964 и вероятностью исправности главной функции Ps1 - 0,985.

Результаты работы системы анализа надежности в виде дерева отказов построенной структуры АСУ ТП испытания с резервированием приведены на

рисунке 4.12.

Обозначения событий отказов приведены ниже

F1 - Отказ основного измерителя температуры;

F2 - Отказ резервного измерителя температуры;

F3 - Отказ основного датчика давления;

F4 - Отказ резервного датчика давления;

F5 - Отказ основного расходомера окислителя;

F6 - Отказ резервного расходомера окислителя;

F7 - Отказ основного расходомера топлива;

F8 - Отказ резервного расходомера топлива;

F9 - Отказ клапана топлива;

F10 - Отказ клапана окислителя;

F11 - Отказ основной шины данных;

F12 - Отказ резервной шины данных;

F13 - Отказ основного контроллера;

F14 - Отказ резервного контроллера;

F15 - Отказ основного автоматизированного рабочего места;

F16 - Отказ резервного автоматизированного рабочего места;

F17 - Отказ основного датчика качества;

F18 - Отказ резервного датчика качества;

F19 - Отказ основного вибродатчика;

F20 - Отказ резервного вибродатчика;

F21 - Отказ основного блока питания;

F22 - Отказ резервного блока питания;

F23 - Отказ основного датчика уровня окислителя;

F24 - Отказ резервного датчика уровня окислителя;

F25 - Отказ датчика уровня топлива;

T1 - Отказ всей АСУ ТП;

T2 - Отказ функции регулирования АСУ ТП.

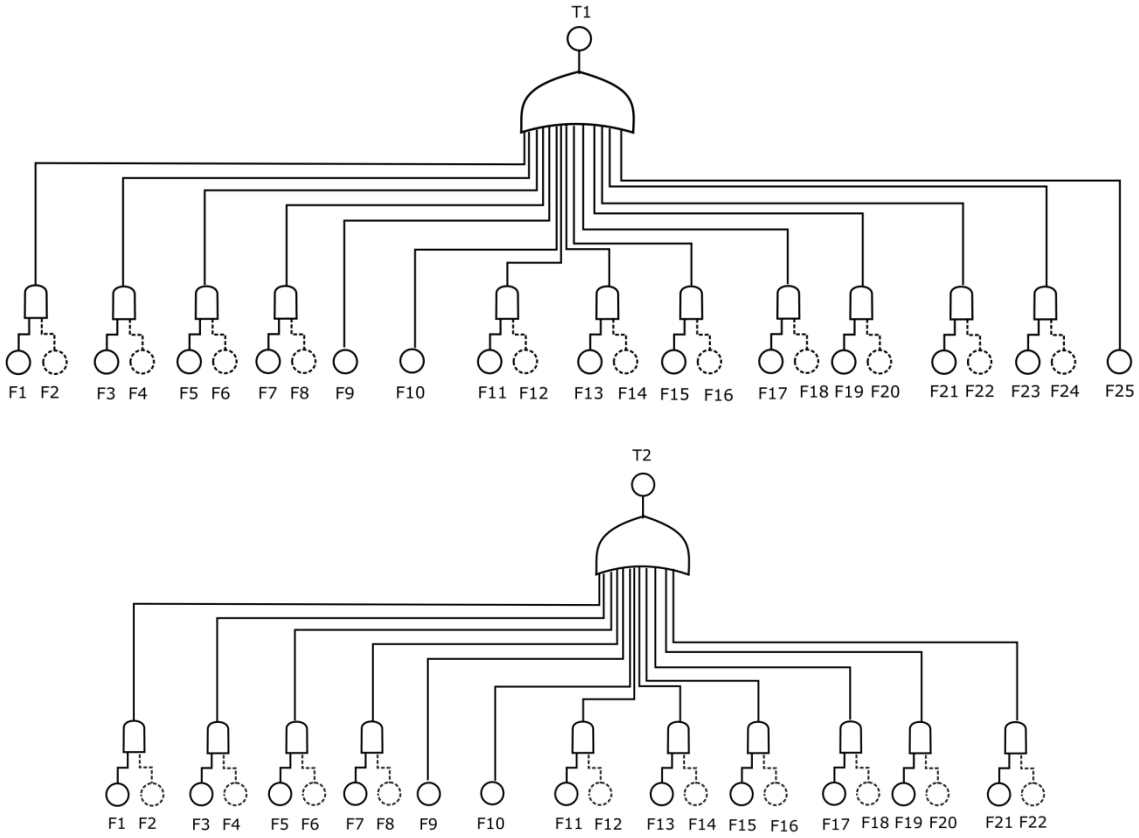


Рисунок 4.12 – Дерево отказов АСУ ТП испытания

Результаты расчётов показателей надежности рассмотренных АСУ приведены в таблицах 4.5 и 4.6.

Таблица 4.5 - Вероятность исправности анализируемой системы

Система	Метод дублирования	Базовый метод	Модифицированный метод
АСУ испытания агрегата	0,93	0,963	0,964
АСУ получения поликарбоната	0,87	0,91	0,94

Таблица 4.6 - Вероятность безотказной работы главной функции системы

Система	Метод дублирования	Базовый метод	Модифицированный метод
АСУ испытания агрегата	0,94	0,974	0,985
АСУ получения поликарбоната	0,89	0,916	0,96

Таким образом, сравнивая величины вероятности исправности, можно сделать вывод, что применение метода позволяет повысить безотказность всей системы на 3,6%, а главной функции на 4,7%.

В структуру анализируемой АСУ ТП введены блокирующие опасности и отказы модули, позволяющие повысить безотказность системы и уменьшить опасность отказов.

Учитывая введение в структуру блокирующих опасности модулей, делается вывод о том, что опасные отказы блокируются и, следовательно, анализируемая АСУ ТП становится безопасной.

Проведён анализ надежности АСУ ТП испытаний энергетического агрегата.

Для анализируемой АСУ ТП проведена функциональная декомпозиция по разработанной методике. В результате декомпозиции выявлена функция, являющаяся наиболее важной для достижения системой своей цели.

При помощи алгоритма анализа опасностей выявлен источник вреда – регулирующий расход аварийно-опасных химических веществ клапан.

Разработанная автоматизированная система анализа обеспечивает построение надежной структуры АСУ ТП с блокировкой опасностей и отказов, с приоритетным резервированием важных и опасных модулей и, таким образом, с высокой безотказностью и безопасностью.

В результате работы системы анализа обеспечено повышение безотказности автоматизированной системы управления до 4,7%.

Выводы

1. Сравнивая величины вероятности исправности, можно сделать вывод, что применение метода позволяет повысить безотказность главной функции на 4,7%.

2. В структуру анализируемой АСУ ТП введены блокирующие опасности и отказы модули, позволяющие повысить безотказность системы и уменьшить опасность отказов.

3. Учитывая введение в структуру блокирующих опасности модулей, делается вывод о том, что опасные отказы блокируются и следовательно, анализируемая АСУ ТП становится безопасной.

4. Проведён анализ надежности автоматизированной системы управления участком процесса получения поликарбоната с дальнейшим построением высоконадежной системы.

5. Для анализируемой АСУ ТП проведена функциональная декомпозиция по разработанной методике. В результате декомпозиции выявлена функция, являющаяся наиболее важной для достижения системой своей цели.

6. При помощи алгоритма анализа опасностей выявлены источники вреда – регулирующие расход аварийно-опасных химических веществ клапаны.

7. Разработанная автоматизированная система анализа обеспечивает построение надежной структуры АСУ ТП с блокировкой опасностей и отказов, с приоритетным резервированием важных и опасных модулей и, таким образом, с высокой безотказностью и безопасностью.

8. В результате работы системы анализа обеспечено повышение безотказности автоматизированной системы управления до 10%.

Заключение

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.

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.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Nowark, T.J. Reliability of J.C. by screening / T.J. Nowark. – In: Proc. 22-th Annu Symp. On Reliability, New York, 1968. – 54 p.

2. McIntyre, J.E. The historical development of polyesters / J.E. McIntyre // Modern Polyesters: Chemistry and technology of polyesters and copolyesters. Ed. by J. Scheirs and T.E. Long. – John Wiley & Sons, 2003.

3. Kuznetsov, P.A. Dangerous failures in multifunctional systems / P.A. Kuznetsov, I.V. Kovalev and P.V. Zelenkov // IOP Conf. Series: Materials Science and Engineering 94 (2015) 012019 doi: 10.1088/1757-899X/94/1/012019.

4. Kovalev, I.V. Multi-version design of fault-tolerant software in control systems / I.V. Kovalev, M.Ju. Slobodin, R.Ju Tsarev // Проблемы машиностроения и автоматизации. – 2006, № 5. – С. 61–69.

5. Porter D.C., Finke W.A. Reliability characterization and prediction of J.G. London [a.o.] van Nostrand, 1970. – P. 232.

6. Programmable control products. Genius modular redundancy for fire and gas applications. - GE Fanuc Automation, GFK-1649A, Sept. 1999. - 50 p.

7. Prokop R., Korbel J., Matusu R. Relay-based autotuning: a second order algebraic design. - IEEE International Workshop on Intelligent Signal Processing, 2005. 1-3 Sept. 2005, p.

8. Proper grounding for the automation industry. - Pulp and Paper Industry Technical Conference, Portland, OR 2001, 18-22 June 2001, p. 110-113.

9. Prytz G. Redundancy in Industrial Ethernet Networks. - 2006 IEEE International Workshop on Factory Communication Systems, June 27, 2006 p. 380 - 385.

10. Qingcang Yu; Bo Chen; Cheng, H.H. Web based control system design and analysis. - IEEE Control Systems Magazine, vol. 24, No. 3, Jun 2004, p. 45 - 57.

11. Risk Spectrum PSA Professional 1.20 / Theory Manual. RELCON AB, 1998. – 57 p.

12. W. Maly and P. Nigh Built-in Current Testing – A Feasibility Study // International Conference on Computer Aided Design, 1988. – P. 340–343.

13.Александровская, Л.Н. Современные методы обеспечения безотказности сложных технических систем : Учебник для студ. вузов, обучающихся по инженерно-техническим направлениям и спец. / Л.Н. Александровская, А.П. Афанасьев, А.А. Лисов. – М. : Логос, 2001. – 206 с.

14.Алексанян, И.Т. Состояние и тенденции развития теории надежности / И.Т. Алексанян, В.Д. Вернер // Электронная техника. – Сер. Управление качеством, стандартизация, испытания. – 1981. – Вып. 4. – С. 5–7.

15.Алгоритмы, математическое обеспечение и архитектура многопроцессорных вычислительных систем. – М. : Наука, 1982. – 336 с.

16.Анашкин А.С., Кадыров Э.Д., Харазов В.Г. Техническое и программное обеспечение распределенных систем управления. Под редакцией Харазова В.Г. - Санкт- Петербург: Изд-во "Р-2", 2004. - 367 с.

17.Анфилатов, В.С. Системный анализ в управлении / В.С. Анфилатов, А.А. Емельянов, А.А. Кукушкин. – М. : Финансы и статистика, 2003. – 368 с.

18.Астраханский, Ю.Л. Имитационное моделирование процессов переноса в элементах ИС / Ю.Л. Астраханский, Ю.Т. Рубаник, С.И. Волков // Электронная техника. – Сер. Управление качеством, метрология, стандартизация, испытания. – 1981. – Вып. 4. – С. 36–38.

19.Барлоу, Р. Статистическая теория надежности и испытания на безотказность / Р. Барлоу, Ф. Прошан. – М. : Наука, 1984. – 328 с.

20.Басманов, П.И. Средства индивидуальной защиты органов дыхания : Справочное руководство / П.И. Басманов. – СПб. : ГИИП «Искусство России», 2002. – 400 с.

21.Бахвалов, Н.С. Численные методы / Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков. – М. : Наука, 1987. – 640 с.

22.Бахметьев, А.М. Отчет о научно-исследовательской работе «Верификация и обоснование программы CRISS 4.0 для моделирования и анализа систем

безопасности ядерной установки при выполнении вероятностного анализа безопасности». Ч. 1 (Заключительная редакция) / А.М. Бахметьев, И.А. Былов, Ю.В. Милакова – Нижний Новгород : ФГУП ОКБМ им. И.И. Африкантова, 2005. – 88 с.

23.Бесекерский, В.А. Теория систем автоматического управления / В.А. Бесекерский, Е.П. Попов. – 4-е изд., перераб. и доп. – СПб. : Профессия, 2003. – 747 с.

24.Боллинджер, Н. NIOSH Guide to Industrial Respiratory Protection / Н. Боллинджер, Р. Шюц. – Вашингтон : NIOSH Publ. – 1987.

25.Боломытцев В. Замена элементов управляющей вычислительной системы без отключения питания. - СТА, №2, 2000, с. 72-77.

26.Большая Советская Энциклопедия : справочное издание / Гл. ред. А. М. Прохоров [и др.] : В 30 т. – Т. 27. Ульяновск – Франкфурт. – М. : Советская энциклопедия, 1977.

27.Васильев, Ф.П. Численные методы решения экстремальных задач / Ф.П. Васильев. – М. : Наука, 1980.

28.Венцель, Е.С. Теория вероятностей / Е.С. Венцель. – М. : Физматгиз. – 1962. – 564 с.

29.Викторова, В.С. Relex – программа анализа надежности, безопасности, рисков / В.С. Викторова, Х. Кунтшер, Б.П. Петрухин, А.С. Степанянц // Надежность. – 2003, № 4 (7). – С. 42–64.

30.Вознесенский, В.В. Средства защиты органов дыхания и кожи / В.В. Вознесенский. – М. : Военные знания, 2011. – 80 с.

31.Гаврищук, В.И. Защита органов дыхания при работе с минеральными удобрениями / В.И. Гаврищук, Б.М. Тюриков // Пути ускорения нормализации условий труда работников сельского хозяйства : Сб. трудов. – Орел : ВНИИОТ ГАП СССР. – 1988. – С. 116–121.

32.Гарайшина Э.Г. Идентификация опасностей, анализ и оценка рисков в нефтехимии // Вестник. Казанского технологического университета. - 2014. - №5

33.Гарайшина Э.Г. Принципы обеспечения промышленной безопасности ОАО «Нижнекамскнефтехим» //Вестник Казан. технол.ун-та. – 2013. - №7. – С. 225.

34.Гмурман В.Е. Теория вероятностей и математическая статистика. - М.: Высшая школа, 2001. - 479 с.

35.Гнеденко, Б.В. Математические методы в теории надежности / Б.В. Гнеденко, Ю.К. Беляев, А.Д. Соловьев. – М. : Наука, 1965. – 524 с.

36.Горюнкова Анна Александровна Современное состояние и подходы к разработке систем мониторинга загрязнения атмосферы // Известия ТулГУ. Технические науки. 2013. №11.

37. ГОСТ 12.4.189-99: Система стандартов безопасности труда. Средства индивидуальной защиты органов дыхания. Маски. Общие технические условия. – М. : Стандартинформ, 1999. – 32 с.

38. ГОСТ EN 1827-2012: Система стандартов безопасности труда. Средства индивидуальной защиты органов дыхания. Полумаски из изолирующих материалов без клапанов вдоха со съемными противогазовыми, противоаэрозольными или комбинированными фильтрами. Общие технические условия. – М. : Стандартинформ, 2012. – 41 с.

39.ГОСТ Р МЭК 61508-1-2012: Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Ч.1. Общие требования. – М.: Стандартинформ, 2012. – 53 с.

40.ГОСТ Р МЭК 62340-2011: Атомные станции. Системы контроля и управления, важные для безопасности. Требования по предотвращению отказов по общей причине. – М. : Стандартинформ, 2011. – 24 с.

41.ГОСТ Р МЭК 61511-1-2011: Безопасность функциональная. Системы безопасности приборные для промышленных процессов. – М. : Стандартинформ, 2011. – 74 с.

42.ГОСТ 12.1.007-76: Система стандартов безопасности труда. Вредные вещества. Классификация и общие требования безопасности.– М. : Стандарт-информ, 1976. – 7 с.

43.ГОСТ Р 12.4.233-2012: Система стандартов безопасности труда. Средства индивидуальной защиты органов дыхания. Термины, определения и обозначения. – М.: Стандартинформ, 2012. – 19 с.

44.ГОСТ Р 54149-2010: Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения. – М. : Стандартинформ, 2010. – 20 с.

45.ГОСТ 22.0.05-97: Безопасность в чрезвычайных ситуациях. Техногенные чрезвычайные ситуации. Термины и определения. – М. : Стандартинформ, 1997. – 16 с.

46.ГОСТ Р 22.10.01-2001: Безопасность в чрезвычайных ситуациях. Оценка ущерба. Термины и определения. – М. : Стандартинформ, 2001. – 8 с.

47. ГОСТ 23519-93. Фенол синтетический технический

48.ГОСТ 24.702-85. Эффективность автоматизированных систем управления. Основные положения.[Электронный ресурс]. - Режим доступа: http://www.rgost.ru/

49. ГОСТ 27 310 95 Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения [Электронный ресурс]. - Режим доступа http://vsegost.com/Catalog/93/9354.shtml

50.ГОСТ 27.002-89: Надежность в технике. Основные понятия. Термины и определения. – М. : Стандартинформ, 1989. – 24 с.

51.ГОСТ 27.310.95: Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения. – М. : Стандартинформ, 1995. – 14 с.

52.ГОСТ 34.601-90: Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. – М. : Стандартинформ, 1990. – 6 с.

53.ГОСТ 34.602-89: Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. – М. : Стандартинформ, 1989. – 12 с.

54. ГОСТ 34.201-89: Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем. – М. : Стандартинформ, 1989. – 11 с.

55.ГОСТ 24.701-86: Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения. – М. : Стандартинформ, 1986. – 12 с.

56.ГОСТ 27.310-95: Анализ видов, последствий и критичности отказов. Основные положения. – М. : Стандартинформ, 1995. – 14 с.

57.Гражданская защита. Понятийно-терминологический словарь. – М. : Флайст ; Инф.-изд. центр «Геополитика». – 2001.

58.Гринин, А.С. Безопасность жизнедеятельности / А.С. Гринин, В.Н. Новиков. – М. : ФИАР-ПРЕСС. – 2003. – 288 с.

59.Гришаков Кирилл Владимирович, Панарин Владимир Михайлович, Горюнкова Анна Александровна Разработка автоматизированных систем мониторинга загрязнения атмосферы объектами газовой и химической промышленности // Известия ТулГУ. Технические науки. 2015. №8-2.

60.Гроп Д. Методы идентификации систем. М.: Мир, 1979, 302 с.

61.Гулько С.В., Джоврей Н. Обзор стандарта IEC 61499. - ПиКАД, №4, 2005 г.

62.Жимерин, Д.Г. Автоматизированные и автоматические системы управления / Д.Г. Жимерин, В.А. Мясников. – М. : [б.и.]. – 1975. – 680 с.

63.Заплатинский, В.М. Терминология науки о безопасности // Zbornik prispevkov z medzinarodnej vedeckej konferencie «Bezhecnostna veda a bezpecnostne vzdelanie. – Liptovsky Mikulas: AOS v Liptovskom Mikulasi. – 2006. – CD nosic.

64.Игнатьев А.С. Создание распределенных систем управления на базе высокоскоростного последовательного интерфейса // Москва, Промышленные АСУ и Контроллер,. №12, 2008.

65.Изерман Р. Цифровые системы управления. М.: Мир, 1984, 541 с.

66.Имитационные методы в теории надежности // Электронная техника. – Сер. Управление качеством, метрология, стандартизация, испытания. – 1981. – Вып. 4. – С. 7–9.

67.Инструкция о порядке выдачи разрешений на применение технических устройств на опасных производственных объектах по хранению, переработке и использованию сырья в агропромышленном комплексе" №52 от 05.06.2003.

68.Исаев, В.С. Аварийно химически опасные вещества / В.С. Исаев, В.А. Владимиров // Стратегия гражданской защиты: проблемы и исследования. – 2012. – № 1. – С. 87.

69.Ицкович Э.Л. Конкурентоспособность российских производителей контроллеров на рынке средств автоматизации производства. - Промышленные контроллеры АСУ, №2. 2008. - с. 4 - 10.

70.Ицкович Э.Л. Современные алгоритмы автоматического регулирования и их использование на предприятиях. - Автоматизация в промышленности, №6. 2007. - с. 39-44.

71.Карякин Р.Н. Заземляющие устройства электроустановок. Справочник. М., 1998, 374 с.

72.Кирсанов В.В. К вопросу о систематизации и конкретизации профилактической работы по повышению уровня промышленной

безопасности предприятий нефтехимической промышленности // Вестник Казан. технол.ун-та. – 2013. - №24. – С. 138.

73.Киселев В. Промышленный Ethernet в стиле Hirschmann. - СТА, №2, 2005, с. 6 - 12.

74. Клюев, А.С. Проектирование систем автоматизации технологических процессов : Справочное пособие / А.С. Клюев, Б.В. Глазов, А.Х. Дубровский, А.А. Клюев ; под ред. А.С. Клюева. – 2-е изд., переработанное и доп. – М. : Системы управления. – 1990. – 464 с.

75.Ковалев, И.В. Мультиверсионный метод повышения программной надежности информационно-телекоммуникационных технологий в корпоративных структурах / И.В. Ковалев, Р.В. Юнусов // Дистанционное и виртуальное обучение. – № 2t. – 2003. – С. 50–55.

76.Ковалев, И.В. Программная поддержка анализа кластерных структур отказоустойчивых информационных систем / И.В. Ковалев, Е.А. Энгель, Р.Ю. Царев // Научно-техническая информация. – Сер. 2: Информационные процессы и системы. – 2007. – № 5. – С. 15–17.

77.Кокшаров, С.В. Влияние технического обслуживания на надежность техники связи : Сб. трудов / С.В. Кокшаров, В.Г. Ольшанский // IV МНТК, т. 1. – Краснодар : КВИ, 2003. – С. 185–188.

78.Козлов, Б.В. Справочник по расчету надежности аппаратуры радиоэлектроники и автоматики / Б.В. Козлов, И.А Ушаков. – М. : Советское радио». – 1975. – 472 с.

79.Косырев О.А. Совершенствование охраны труда на основе концепции профессионального риска [Электронный ресурс]/ О.А. Косырев, А.В. Москвичев, Н.И. Симонова // Охрана труда и техника безопасности на промышленных предприятиях. – 2012. - №11. Кнунянц, И.Л. Краткая химическая энциклопедия : Справочное издание / Гл. ред. И.Л. Кнунянц. – В 5 т. – М. : Советская энциклопедия, 1961–1967. – Т. 5. – 1184 с.

80. Курносов, В.И. Методология проектных исследований и управление качеством сложных технических систем электросвязи / В.И. Курносов, А.М. Лихачев. – СПб. : ТИРЕКС. – 1998. – 495 с.

81. 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.

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

83.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.

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

85.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. – Т. 16, № 4. – 2015. – С. 941–945.

86.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).

87.Кузнецов, П.А. Надежность автоматизированных систем управления / П.А. Кузнецов // Сб. статей по итогам Всероссийской научно-практической конференции «Молодые ученые в решении актуальных проблем науки». – В 2 т. – Т. 2. – Красноярск. – 2012. – С. 259–261.

88.Кузнецов, П.А. Реализация метода Волковича и Михалевича при проектировании системы автоматического регулирования параметра технологического процесса / П.А. Кузнецов // Сб. статей по материалам Всероссийской научно-практической конференции «Лесной и химический комплексы – проблемы и решения». – В 2 т. – Т.2. – Красноярск. – 2012. – С. 250–254.

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

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

91.Кузнецов, П.А. Надежность АСУ ТП с учетом ее функциональности / П.А. Кузнецов, И.В. Ковалев // Тезисы X Всероссийской науч.-практ. конференции творческой молодежи «Актуальные проблемы авиации и космонавтики». – В 2 т. – Т. 1. – Красноярск. – 2014. – С. 316–317 .

92. Кузнецов, П.А. Опасные отказы в АСУ ТП / П.А. Кузнецов // Сб. мат. IV Международной молодежной научно-практической конференции «Научные исследования и разработки молодых ученых». – Новосибирск. – 2015. – С. 97–101.

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

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

95.Кузнецов, П.А. Надежность АСУ ТП с учетом ее функциональности / П.А. Кузнецов, И.В. Ковалев // Тезисы X Всероссийской научно-практической конференции творческой молодежи «Актуальные проблемы авиации и космонавтики». – В 2 т. – Т. 1. – Красноярск. – 2014. – С. 316–317.

96.Курочкин, Ю.А. Надежность и диагностирование цифровых устройств и систем / Ю.А. Курочкин, А.С. Смирнов, В.А. Степанов. – Спб. : Изд-во С.-Петербургского ун-та. – 1993. – 320 с.

97.Левин, А.П. Контакты электрических соединителей радиоэлектронной аппаратуры / А.П. Левин. – М. : Сов. радио, 1972. – 216 с.

98.Литюга, А.М. Теоретические основы построения эффективных АСУ ТП / А.М. Литюга, Н.В. Клиначев, В.М. Мазуров [Электронный ресурс]. – Режим доступа: http://model.exponenta.ru/auto_reg.html.

99.Липаев, В.В. Системное проектирование сложных программных средств для информационных систем. – 2-е изд., перер. и доп. / В.В. Липаев. – М. : СИНТЕГ, 2002. – 268 с.

100. Ллойд, Д. Надежность: организация, исследования, методы и математический аппарат / Д. Ллойд ; пер. с англ. М. Липов. – М. : Сов. радио. – 1964. – 686 с.

101. Макдональд Д. Промышленная безопасность, оценивание риска и системы аварийного останова. - М.: ООО "Группа ИДТ", 2007. - 416 с.

102. Маслов, А.П. Повышение надежности радиоэлектронной аппаратуры / В.Ю. Татарский. – М. : Сов. радио, 1972. – 264 с.

103. Менделевич В.А. Интеллектуальное управление арматурой //Москва, Автоматизация и IT в энергетике, №6, 2011.

104. Менделевич В.А. Интеллектуальные СК и стенды датчиков - значительный шаг в создании распределенных систем ответственного управления //Москва, Автоматизация и IT в энергетике, №12, 2010.

105. Менделевич, В.А., Коновалова, М.Ф., Луховицкий, И.В. Опыт внедрения технологических защит на базе ПТК «САРГОН» // Москва, "Промышленные АСУ и контроллеры", №12, 2002.

106. Методические рекомендации по применению и действиям нештатных аварийно-спасательных формирований при приведении в готовность гражданской обороны и ликвидации чрезвычайных ситуаций / Под ред. В.А. Пучкова [Электронный ресурс]. – Режим доступа: http://59.mchs.gov.ru/document/3002833.

107. Михайлов, А.В. Эксплуатационные допуски и надежность в радиоэлектронной аппаратуре / А.В. Михайлов. – М. : Сов. радио, 1970. – 216 с.

108. Михалевич, В.С. Вычислительные методы исследования и проектирования сложных систем / В.С. Михалевич, В.Л. Волкович. – М. : Наука. – 1982. – 286 с.

109. Можаев, А.С. Общий логико-вероятностный метод анализа надежности сложных систем : Уч. пособие / А.С. Можаев. – Л. : ВМА. – 1988. – 68 с.

110. Перроте, А. И. Вопросы надежности РЭА / А.И. Перроте, М.А. Сторчак. – М. : Сов. радио. – 1976. – 185 с.

111. Попов, В.Н. Нормы и допуски на параметры функциональных узлов / В.Н. Попов. – М. : Энергия, 1976. – 72 с.

112. Правила безопасности в нефтяной и газовой промышленности» ПБ 08-624-03 -[Электронный ресурс] - URL: http://www.complexdoc.ru.

113. Предупреждение и ликвидация чрезвычайных ситуаций [Электронный ресурс]. – Режим доступа: http://obzh.ru/pre/

114. РД 03-418-01 РД 03-418-01: Методические указания по проведению анализа риска опасных производственных объектов [Электронный ресурс]. – Режим доступа: http://ohranatruda.ru/ot_biblio/ normativ/data_normativ/ 10/10314.

115. Родионов, М.Г. Информационно-измерительные системы: теория систем и системный анализ : уч. пособие / М.Г. Родионов. – Омск : Изд-во ОмГТУ. – 2011. – 83 с.

116. Российская энциклопедия по охране труда. – В 3 т. – Т.1 – 2-е изд., перераб. и доп. – М. : Изд-во НЦ ЭНАС. – 2007. – 440 с.

117. Рудаченко А.В. Газотурбинные установки для транспорта природного газа: учебное пособие: учебное пособие / А.В. Рудаченко, Н.В. Чухарева; Национальный исследовательский Томский политехнический университет. − Томск: Изд-во Томского политехнического университета, 2010. – 217с.

118. Рябинин, И.А. Основы теории и расчета надежности судовых электроэнергетических систем / И.А. Рябинин. – Л. : Судостроение, 1967 . – 456 с.

119. Рябинин, И. А. Логико-вероятностные методы исследования надежности структурно-сложных систем / И.А. Рябинин, Г.Н. Черкесов. – М. : [б.и.]. – 1981. – 264 с.

120. Рябинин, И.А. Надежность и безопасность структурно-сложных систем / И.А. Рябинин. – СПб. : Изд-во С.-Петерб. ун-та. – 2007. – 276 с.

121. Самыгин, С.И. Школа выживания: Обеспечение безопасности жизнедеятельности : уч. пособие / С.И. Самыгин, О.П. Самыгина. – Ростов-на-Дону : Феникс, 2002. – 544 с.

122. Сапожников, В.В. Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В.В. Сапожников, Вл. В. Сапожников, Х.А. Христов, Д.В. Гавзов ; под ред. Вл. В. Сапожникова. – М. : Транспорт. – 1995.

123. Словарь терминов МЧС [Электронное издание]. – Режим доступа: http://www.mchs.gov.ru/dop/terms, 2010.

124. Симлянский, Г.Л. Справочник проектировщика АСУТП / Г.Л. Симлянский. – М. : Машиностроение. – 1983. – 528 с.

125. Смелков, Г.И. Классификация и области применения электроустановок в пожаровзрывоопасных зонах : справочное пособие / Г.И. Смелков, В.Н. Черкасов, Е.Л. Шеститко, В.А. Пехотиков, В.Н. Веревкин, Н.Е. Чубарова. – М. : ВНИИПО, 2001. – 112 с.

126. Сотсков, Б.С. Основы теории и расчета надежности элементов и устройств автоматики и вычислительной техники / Б.С. Сотсков. – М. : Высшая школа. – 1970. – 272 с.

127. Аврамчук, Е.Ф. Технология системного моделирования / Е.Ф. Аврамчук, А.А. Вавилов, С.В. Емельянов и др. ; под общ. ред. С.В. Емельянова и др. – М. : Машиностроение ; Берлин : Техника. – 1988.

128. Федеральный закон «О промышленной безопасности опасных производственных объектов». – 2-е изд, с изм. – М. : ФГУП «НТЦ по безопасности в промышленности Госгортехнадзора России». – 2004. – 28 с.

129. Федоров, Ю.Н. Справочник инженера по АСУ ТП: Проектирование и разработка : уч.-практ. пособие / Ю.Н. Федоров. – М. : Инфра-инженерия. – 2008. – 928 с.

130. Физика надежности / Под ред. Е.И. Декабрун. – М. : Наука. – 1981. – 164 с.

131. Химмельбау Д. Анализ процессов статистическими методами / Д. Химмельбау. – М. : Мир. – 1973. – 960 с.

132. Хорошев, А.Н. Введение в управление проектированием механических систем : уч. пособие / А.Н. Хорошев. – Белгород. – 1999. – 372 с.

133. Чрезвычайные ситуации на химически опасных объектах с выбросом аварийно химически опасных веществ в окружающую природную среду : метод. разработка для студентов всех специальностей дневной формы обучения [Электронный ресурс]. – Режим доступа: www.nntu.ru/RUS/otd_sl/gochs/posobiya/posob13.doc.