ООО НПП «ЭСН»

СТРОИТЕЛЬСТВО ВОДОГРЕЙНОЙ КОТЕЛЬНОЙ 400 ГКАЛ/ЧАС НА ТЕРРИТОРИИ ИВАНОВСКОЙ ТЭЦ-2

(878.2023)

Проектная оценка надежности системы

878.2023-АСУ ТП.Б1

Том 42

2025

Подп. и дата	
Инв. № дубл.	
Взамен инв. №	
Подп. и дата	
Инв. № подл.	

Содержание

1 Введение

1.1 Назначение расчета надежности системы

Проектная оценка надёжности системы предназначена для определения и подтверждения того, что автоматизированная система управления технологическими процессами (АСУТП) водогрейной котельной (среднего и верхнего уровней) обладает требуемыми показателями надёжности, безотказности и отказоустойчивости. Достижение заданного уровня надёжности необходимо для безопасной, эффективной и непрерывной работы оборудования котельной во всех режимах – нормальных, переходных, аварийных и послеаварийных. Надёжность АСУТП напрямую влияет на безопасность и эффективность технологического процесса, поэтому на ранних стадиях проектирования проводится расчёт необходимых показателей надёжности системы. Данный расчёт позволяет убедиться, что принятые проектные решения обеспечивают требуемый уровень безотказности и готовности системы, а также выявить потенциально уязвимые места и определить меры для повышения надёжности при необходимости

1.2 Перечень оцениваемых показателей надежности

В рамках проектной оценки рассматриваются следующие основные показатели надёжности АСУТП:

- **Вероятность безотказной работы** за заданный интервал времени ($R(t_1, t_2)$). Этот показатель отражает *безотказность* системы и характеризуется функцией надёжности R(t). Согласно ГОСТ 27.002-89, надёжность определяется как свойство объекта сохранять способность выполнять требуемые функции в заданных режимах и условиях в течение определённого времени.
- **Интенсивность отказов (λ)** – параметр потока отказов, часто рассчитывается как обратная величина к среднему времени наработки на отказ ($\lambda = 1/MTBF$) при экспоненциальном распределении отказов. Низкое значение λ соответствует высокой надёжности.
- **Среднее время безотказной работы (MTBF, Mean Time Between Failures)** – средняя наработка на отказ системы или компонента, обычно выражаемая в часах. Этот показатель характеризует *долговечность* и безотказность: чем больше MTBF, тем реже случаются отказы. В проекте устанавливаются требования к MTBF в соответствии с нормативными

документами. В частности, средняя наработка АСУТП на отказ при нормальных условиях должна соответствовать требованиям отраслевого стандарта (РД 153-34.1-35.127-2002).

- **Среднее время восстановления (MTTR, Mean Time To Recovery)** – среднее время, необходимое для обнаружения и устранения неисправности и восстановления работоспособности. Этот показатель зависит от организации технического обслуживания. В расчётах принимается регламентное время восстановления, как правило, не более 1 часа для основных компонентов, в соответствии с требованиями к обслуживанию на электростанциях. Небольшое MTTR в сочетании с большим MTBF обеспечивает высокий коэффициент готовности.
- **Коэффициент готовности $K_г$** – вероятность того, что система в любой произвольный момент времени находится в работоспособном состоянии. Этот комплексный показатель учитывает и безотказность, и ремонтопригодность. Расчёт выполняется по формуле: $K_г$ = MTBF / (MTBF + MTTR). Коэффициент готовности близкий к 1 означает, что система практически постоянно работоспособна.

Кроме вышеперечисленных, при необходимости могут оцениваться и другие показатели надёжности в соответствии с ГОСТ 27.002-89 – например, **коэффициент технического использования**, показатели **ремонтопригодности** и **сохраняемости**, однако в данном документе упор сделан на показатели безотказности и готовности, как наиболее важные для АСУТП. Также учитываются показатели надёжности реализации функций и *риск возникновения аварийных ситуаций* – эти интегральные критерии выделяются стандартом ГОСТ 24.701-86 применительно к АСУТП. Иными словами, оценивается, насколько надёжно система выполняет требуемые технологические функции, и какова вероятность отказов, способных привести к опасным событиям.

1.3 Состав учитываемых при расчете факторов, допущения и ограничения

При расчёте надёжности учитываются как технические, так и программные средства системы, а также внешние условия её эксплуатации. В состав факторов, влияющих на надёжность АСУТП, включены:

- **Надёжность программного обеспечения (ПО).** В отличие от физических отказов аппаратуры, отказы ПО обусловлены скрытыми ошибками, сбоями в алгоритмах или некорректной работой в нестандартных ситуациях. В расчёте учитывается, что надёжность прикладного и системного ПО соответствует требованиям ГОСТ 28195-89.

Показатели надёжности ПО характеризуют способность программы выполнять заданные функции правильно, включая устойчивость функционирования при возникновении сбоев аппаратуры или ошибочных данных. Таким образом, ПО АСУТП спроектировано с механизмами защиты от ошибок, что позволяет существенно снизить вероятность отказа системы по причине сбоя программного обеспечения. В рамках расчёта предполагается, что вероятность критического отказа ПО очень мала. Тем не менее, ПО включается в общую логическую схему надёжности системы как элемент, отказ которого приведёт к потере работоспособности функций верхнего уровня.

- **Надёжность комплекса технических средств (КТС).** Аппаратные компоненты АСУТП составляют программно-технический комплекс, от надёжности которого зависит функционирование системы. В расчётах учитываются все основные узлы: программируемые контроллеры среднего уровня (ПЛК) с модулями ввода-вывода, сервера верхнего уровня, операторские станции (АРМ), коммуникационное оборудование (промышленные коммутаторы, сетевые экраны), источники бесперебойного питания (ИБП) и т.д. Для каждого элемента используются паспортные или справочные данные по надёжности – прежде всего средняя наработка на отказ. Предполагается, что все включённые в расчёт элементы изначально исправны и функционируют в условиях штатной эксплуатации.
- **Условия эксплуатации.** Система АСУТП будет эксплуатироваться в контролируемых производственных условиях. Температурный режим для размещения контроллеров и электронных средств – от +5 °C до +60 °C, без конденсации влаги, в среде, соответствующей нормам по запылённости и отсутствию агрессивных газов. Предусмотрено бесперебойное электропитание: все шкафы с оборудованием подключены через ИБП и резервные источники питания, обеспечивающие надёжное электроснабжение системы. Также реализованы меры по электромагнитной совместимости и помехозащите: экранирование кабелей, правильное заземление, что снижает риск отказов от внешних воздействий. Таким образом, расчет производится для нормальных условий эксплуатации, указанных в ТЗ, и учитывает, что отклонения условий находятся в пределах, допускаемых для оборудования.
- **Режим работы и нагрузка.** Система АСУТП функционирует круглосуточно (режим 24/7) без регулярных остановок, поддерживая технологический процесс производства тепловой энергии. Расчёт надёжности исходит из непрерывной работы системы под номинальной нагрузкой. Нагрузочные и циклические факторы (например, частые пуски/остановы котлового оборудования) косвенно влияют на систему через увеличение интенсивности

поступающих сигналов и операций, однако считаем, что это не приводит к деградации аппаратуры в расчётном периоде, кроме учёта базовой вероятности отказов.

- **Организационные меры обслуживания.** Предусмотрена эксплуатация системы с регулярным техническим обслуживанием и оперативным ремонтом при сбоях. В проекте заложена концепция ремонтопригодности: выбор компонентов, для которых производитель гарантирует наличие сервисной поддержки и запасных частей, а также конструктивное исполнение шкафов, позволяющее быстро заменить любой вышедший из строя модуль. Имеется комплект ЗИП. Благодаря модульной структуре ПТК возможно горячее резервирование и «горячая» замена устройств: например, резервные контроллеры автоматически принимают управление при отказе основного; отказавший модуль можно заменить на месте без отключения питания остальных частей системы. Организационно это подкреплено круглосуточной готовностью персонала к ремонту: на объекте. Таким образом, время на обнаружение и замену отказавшего блока сведено к минимуму – в среднем порядка 0.5–1 часа, что соответствует нормативу (MTTR ≤ 1 ч). При расчёте коэффициента готовности и других показателей это малое время восстановления существенно повышает итоговую надёжность. *Ограничения расчёта:* предполагается, что резервные компоненты функционируют независимо и не подвержены «общему причинному отказу» одновременно с основным (вероятность общей причины отказа считается пренебрежимо малой). Человеческий фактор (ошибки оперативного персонала) и сознательное влияние (вредоносные действия) **не** рассматриваются в данном расчёте надёжности, поскольку они относятся к эксплуатационным рискам, а не к техническим отказам системы. Также в расчёт **не включены** полевые приборы и исполнительные механизмы (датчики, клапаны и др.), находящиеся на нижнем уровне. Настоящий документ сфокусирован на надёжности *среднего и верхнего уровней* – то есть на самом программно-техническом комплексе управления.

Таким образом, исходные данные для расчёта надёжности включают перечень элементов АСУТП с их характеристиками надёжности, условия эксплуатации (температура, питание, нагрузка) и параметры организации обслуживания (время восстановления, наличие резервов). Эти данные будут использованы в выбранной методике расчёта для количественной оценки показателей надёжности системы.

2 Исходные данные

2.1 Данные о надежности элементов АС

Состав системы и компоненты. Автоматизированная система управления технологическим процессом водогрейной котельной (АСУТП/ВК) включает в свой состав несколько подсистем, относящихся к верхнему и среднему уровням управления. Согласно техническому заданию, каждая подсистема отвечает за определённое оборудование или технологический узел.

Каждая локальная подсистема на среднем уровне реализована на базе программно-технического комплекса, включающего *двухканальное резервирование контроллеров*. То есть для каждой системы автоматического управления (САУ) используется пара микропроцессорных контроллеров, объединённая в схему горячего резервирования. Два ПЛК работают по принципу основной и резервный: при выходе из строя одного контроллера второй автоматически и без заметной паузы принимает управление, благодаря чему подсистема продолжает функционировать безотказно. Обмен данными между контроллерами и модулями ввода/вывода организован по резервированным каналам связи. Таким образом, отказ одного контроллера или одной линии связи не приводит к потере управления.

Для реализации функций автоматизации применяются программируемые логические контроллеры типа **ТРЭИ М1201Е**, устанавливаемые в составе шкафов каждой подсистемы в количестве двух штук (основной + резервный). Контроллеры работают в схеме активного резервирования.

К каждому контроллеру подключаются модули ввода/вывода сигналов, обеспечивающие полный охват перечня технологических параметров:

- **Аналоговые входные модули М1234А** – для приёма унифицированных токовых сигналов (4–20 мА).
- **Аналоговые входные модули М1231TR** – для подключения термопреобразователей сопротивления.
- **Дискретные входные модули М1251D** – для приёма дискретных сигналов.
- **Дискретные выходные модули релейного типа М1252О** – для выдачи управляющих дискретных сигналов.

Все модули аналоговых сигналов оснащены гальванической развязкой каналов. Каналы дискретных модулей выполнены на индивидуальных реле, что обеспечивает электрическую развязку каждой цепи. Конструктивно все модули поддерживают функцию «горячей» замены.

Такое дублирование присутствует во всех подсистемах: *АСУ ВК, АСУ ГРП-1, ГРП-2, АСУ Наб, АСУ Зд, АСУ ЭТО* — каждая включает шкаф с двумя контроллерами и комплектом модулей, удовлетворяющим требованиям по функционалу и резервированию. **Надёжностные характеристики контроллеров и модулей** приняты в соответствии с паспортными данными. Модули серии ТРЭИ-5В представляют собой современные микропроцессорные устройства, рассчитанные на круглосуточную работу в промышленной среде. Наработка на отказ составляет не менее 150 000 часов, среднее время восстановления — не более 0,5 часа, коэффициент технического использования — не ниже 0,97. Нормативный срок службы устройств — не менее 15 лет. В ТЗ предусмотрено применение серийно выпускаемых средств с высокими показателями надёжности, соответствующих отраслевым стандартам (СО 34.35.127, СТО 70238424.27.100.010-2011 и др.). Кроме того, контроллеры, реализующие функции технологических защит, должны соответствовать повышенным требованиям надёжности (РД 153-34.1-35.137-00), что также учитывается при выборе моделей и схем резервирования.

Верхний уровень и коммуникации. Для координации работы всех локальных подсистем и для интерфейса с оператором предусмотрен верхний уровень – серверный комплекс и автоматизированные рабочие места (АРМ) операторов. В состав серверной станции входят: промышленный сервер (формата 19", 1U) с повышенной отказоустойчивостью, коммутатор локальной вычислительной сети, межсетевой экран, устройство KVM-консоли, блоки питания с ИБП, и вспомогательное оборудование (шкаф, вентиляционные модули и т.д.). Сервер выбран с учётом высоких требований по надёжности: это *компактный отказоустойчивый сервер AdvantiX GS-104-E1* (количество – 1 шт.). Данный сервер характеризуется отказоустойчивой архитектурой (встроенное резервирование критичных узлов – блоков питания, дисков RAID с горячей заменой, два сетевых интерфейса и т.д.), что увеличивает его время бесперебойной работы. Дополнительно предусмотрена ещё одна серверная единица. Таким образом, основной вычислительный узел верхнего уровня имеет резервирование ключевых компонентов.

К серверу через коммутатор подключены **операторские станции (АРМ)** – всего 7 рабочих мест оператора, размещаемых в помещении Операторной. Каждое АРМ выполнено на базе персонального компьютера промышленного исполнения. АРМы служат для отображения мнемосхем, параметров и сигнализации, а также для подачи команд управления. Между АРМ и сервером реализована схема клиент-сервер: сервер выполняет функции сбора данных с контроллеров, ведения базы данных и журналов, а АРМы подключаются к серверу по сети Ethernet для доступа к информации. Все АРМ включены в локальную вычислительную сеть (ЛВС) АСУТП, которая построена с резервированием: применён управляемый промышленный коммутатор DKC с возможностью подключения оптических модулей и резервных линий.

Вероятность одновременного выхода из строя всех операторских станций крайне мала, учитывая их количество и независимость. Даже при отказе одного АРМ, другие остаются работоспособными, поэтому функция отображения информации и дистанционного управления сохраняется. Критическим сценарием для верхнего уровня является отказ именно сервера, так как при недоступности сервера все АРМ потеряют связь с ПЛК. Для смягчения этого риска каждый сервер оснащён резервным питанием (ИБП «Штиль» 3 кВА с батарейными модулями, обеспечивающий работу при пропадании внешнего питания), а также дублированием сетевых интерфейсов и каналов, как отмечалось выше. В расчет надёжности будет включён показатель готовности АРМ/сервера как единой подсистемы отображения информации.

Паспортные надёжностные характеристики. Ниже сведены исходные численные показатели надёжности основных элементов АСУТП, используемые в расчётах. Эти данные получены из технической документации производителей или из нормативных требований, предъявленных к оборудованию в проекте (если прямые паспортные данные отсутствуют, используются нормативные минимальные значения из РД 153-34.1-35.127-2002 и СТО 70238424.27.100.010-2011):

- *Программируемые контроллеры (M1201E)* – MTBF **305 010 часов**, при условии эксплуатации в нормальных условиях. Вероятность отказа одного контроллера в течение часа: $\lambda = 1/305010$. Благодаря резервированию, отказ обеих парных ПЛК одновременно за короткий период крайне маловероятен (см. методику расчёта ниже). Среднее время восстановления при отказе контроллера – **0,5 ч**.
- *Модули ввода-вывода* – MTBF для **M1234A 810 300**, **M1231TR 381 298**, **M1252D 809 409**, **M1251A 620 529 ч**. Их отказы влияют на сигнальные каналы. Модули имеют встроенную самодиагностику; замена модулей – в течение **0,5 ч**.
- *Промышленные коммутаторы и сетевое оборудование* – MTBF типично **>100 000 часов**. В проекте один коммутатор DKC N2100 в каждом серверном шкафу. MTTR при замене коммутатора – **0,5 ч**.
- *Сервер верхнего уровня* – MTBF оценивается не ниже **50 000 часов** для всего узла. Однако за счёт внутренней отказоустойчивости фактический MTBF выше: например, блок питания, диски имеют резервирование, поэтому отказ сервера происходит только при одновременном сбое нескольких компонентов или сбое системной платы. Таким образом можем ожидать MTBF системы в целом порядка **100–150 тыс. часов**. MTTR при отказе сервера – **2 часа**.
- *АРМ оператора (клиентские станции)* – MTBF одного АРМ ~ **40 000 часов** (около 4,5 лет) по отказу аппаратной части. Поскольку АРМ множественные (7 шт), для полного

отказа функции нужно, чтобы все станции или сеть вышли из строя. Вероятность этого чрезвычайно мала. MTTR замены АРМ – **2 часа** (включая переназначение IP и установка ПО, при наличии запасной станции). Отметим, что потеря одного АРМ не критична – операторы могут перейти на другой рабочий пост.

Примечание: Конкретные численные значения MTBF взяты оценочно и для цели расчёта приведены к минимальным значениям, удовлетворяющим нормативам. Для функции отображения информации средняя наработка на отказ “невозможность вызова всех экранов на всех АРМ” должна быть не менее 400 тыс. часов. В нашем случае этот показатель обеспечивается за счёт того, что отказ всех АРМ единовременно практически может произойти только при отказе центрального сервера. Учитывая резервирование сервера, вероятность подобного события соответствует MTBF порядка 400 000 ч, что согласуется с требованием. Аналогично, для автоматического регулирования полный отказ подсистемы (всех контуров) должен иметь MTBF ≥100 000 ч – это достигается наличием двух контроллеров, что повышает надёжность до необходимого уровня по сравнению с одиночным ПЛК. В исходных данных заложено, что требуемые стандартом значения будут выполнены или превышены. При дальнейшем расчёте будут использованы указанные оценки MTBF/MTTR для вычисления сводных показателей системы.

2.2 Данные о режимах и условиях функционирования элементов АС

Исходные данные также включают режим работы без постоянных остановов – система рассчитана на непрерывное функционирование с периодическими техническими обслуживаниями без вывода из работы (все плановые проверки осуществляются на ходу, либо с поочерёдным отключением резервируемых компонентов, чтобы не прерывать процесс). Предусмотрено ежеквартальное ТО (профилактический осмотр, проверка диагностических журналов, тестирование резервирования) и оперативный ремонт по факту отказа с привлечением ЗИП. Этот подход гарантирует, что при отказе одного из элементов система быстро восстановится, а профилактика позволит выявлять и заменять компоненты приближающиеся к концу ресурса. В расчёте надёжности принимается, что после устранения отказа система возвращается в исходное (полностью исправное) состояние, т.е. восстановление полнофункционально. Средний ресурс работы системы до списания – не менее 15 лет согласно ТЗ, что согласуется с приведёнными показателями MTBF.

Подытоживая, исходные данные по надёжности элементов АСУТП собраны из требований ТЗ, спецификаций и нормативных документов. Они охватывают: типовой состав оборудования и ПО, количественные параметры надежности (MTBF, MTTR) для каждой группы компонентов, условия эксплуатации (температура, питание, режим работы) и организацию обслуживания (горячее резервирование, ЗИП, время восстановления). Эти данные служат базой для дальнейшего расчёта показателей надежности системы методом логико-вероятностного моделирования.

3 Методика расчета

Выбор методики и обоснование. Для оценки надёжности АСУТП применён метод **логико-вероятностного моделирования**. Данный метод заключается в построении моделей отказов системы в виде логических схем или деревьев событий и последующем вычислении вероятностных характеристик на основе надёжности отдельных элементов. В частности, используется представление системы в виде *структурных схем надёжности* – где компоненты соединены либо последовательно (если отказ любого приводит к отказу системы), либо параллельно (если система работоспособна при отказе отдельных резервированных компонентов). Такой подход позволяет учесть сложную архитектуру АСУТП с резервированием и получить количественные показатели на основе известных показателей элементов.

Логико-вероятностные методы широко рекомендуются нормативно-технической документацией для анализа надёжности сложных систем управления. В нашем случае выбранный метод обусловлен следующими факторами:

- **Сложность и масштаб системы.** АСУТП котельной включает множество компонентов (несколько подсистем, сервер, сеть, АРМы), поэтому детерминированные расчёты надёжности затруднены. Вероятностный подход с моделированием отказов обеспечивает учёт всех возможных комбинаций отказов и их влияния на работоспособность системы.
- **Наличие резервирования.** Большинство критических элементов системы зарезервированы (два контроллера, резервное питание, резервные каналы связи, множественные АРМы). Логико-вероятностная модель (например, в виде *блочных диаграмм надёжности*) позволяет корректно рассчитать выигрыш в надёжности от схем резервирования, используя известные формулы для параллельных структур (например, $R_{пар}=1-(1-R_1)(1-R_2)$ для двухрезервной системы, где $R_{пар}$ — вероятность безотказной работы системы при параллельном соединении двух элементов, R_1, R_2 — вероятности безотказной работы отдельных элементов).
- **Комплексный характер надежности.** Для АСУТП важно оценить не только безотказность аппаратуры, но и надёжность функционирования ПО, а также учесть возможные человеческие ошибки и т.п. В рамках логико-вероятностного подхода это реализуется включением событий отказа программного обеспечения и ошибок оператора (при необходимости) в общее дерево отказов. Таким образом достигается полный учёт факторов надежности.

Нормативная база. Расчёт проведён на основании следующих нормативно-технических документов:

- *ГОСТ 27.002–89* «Надёжность в технике. Основные понятия. Термины и определения» – используется для определения терминологии и основных показателей надёжности, а также общих принципов расчёта. Например, понятия *отказ*, *работоспособность*, *безотказность*, *готовность* берутся в строгом соответствии с ГОСТ.
- *ГОСТ 24.701–85 (86)* «Надежность АСУ. Основные положения» – определяет номенклатуру показателей надёжности применительно к автоматизированным системам управления и порядок установления требований к надёжности. Согласно этому стандарту, надежность системы АСУТП оценивается двумя группами показателей: надёжностью реализации функций (безотказностью выполнения задач управления) и уровнем *живучести/безопасности* (вероятностью предотвратить развитие аварийных ситуаций). Мы учитываем эти рекомендации, разбивая расчёт показателей по функциональным подсистемам (регулирование, управление, отображение, защита).
- *ГОСТ 28195–89* «Оценка качества программных средств. Общие положения» – применяется в части критериев надёжности программного обеспечения. В частности, учтены такие показатели качества ПО, как **устойчивость функционирования** (способность продолжать работу при сбоях аппаратуры или ошибках данных) и **работоспособность ПО** (способность функционировать в заданных режимах при отсутствии сбоев технических средств). Это позволило включить компонент ПО в модель надёжности количественно (пусть и с условной оценкой вероятности отказа ПО). Кроме того, мы опирались на ГОСТ 28195–89 при формулировании допущений о практически достижимой надёжности программ (например, что встроенные средства контроля ошибок позволяют снизить вероятность сбоя программы до величин порядка 10^{-6}…10^{-7} в час).
- *ГОСТ 27.003–90* (и ГОСТ Р 27.003–2016) «Надёжность в технике. Управление надежностью. Задание требований» – использован косвенно для проверки, что заданные в ТЗ требования к надежности соответствуют нормативным. ТЗ на АСУТП ссылается на СТО 70238424.27.100.010-2011 «АСУТП ТЭС. Нормы и требования» и РД 153-34.1-35.127-2002, в которых конкретизированы нормативы надежности. Например, показатели надежности системы должны отвечать требованиям СТО 70238424.27.100.010-2011, а ПТК по надежности – ГОСТ 24.701-86 и ГОСТ 27.003-2016. Мы учитываем эти указания при сравнении полученных расчётных значений с нормативными (см. раздел *Анализ результатов*).

Краткое описание процесса расчёта. Процедура расчёта надёжности включала следующие этапы:

1. **Формализация структуры системы.** На основании исходных данных построена структурная схема надежности АСУТП. Выделены основные узлы и связи: подсистемы котельной, ГРП, насосной и пр. (каждая – двухканальная пара контроллеров), сервер SCADA, сеть, АРМы, ИБП. Схема отражает резервирование: параллельное соединение для резервных контроллеров, дублированных линий связи, множественных АРМ. Также ПО учтено как элемент, общий для всей системы (отказ критического ПО рассматривается как отказ системы).
2. **Назначение показателей надёжности элементам.** Каждому блоку присвоены параметры MTBF и MTTR согласно исходным данным. Например, для одного контроллера $\lambda \approx 3{,}28 \cdot 10^{-6}$ ч$^{-1}$ (MTBF 305 010 ч), для пары резервных контроллеров параметры рассчитываются через эквивалентную схему. Аналогично, сервер: $\lambda \approx 2 \cdot 10^{-5}$ ч$^{-1}$, АРМ: $\lambda \approx 2.5 \cdot 10^{-5}$ ч$^{-1}$ и т.д. Для ПО задан условный параметр: вероятность отказа ПО за год $P_{по} \approx 0.01$ (1%) – консервативная оценка, соответствующая коэффициенту готовности ПО ~0.99.
3. **Расчёт надёжностных структур.** Применены классические формулы теории надёжности для последовательных и параллельных структур. Так, для двух однотипных независимых элементов, включённых *в параллель* (горячее резервирование), вероятность безотказной работы рассчитывается как: $R_{пар}(t)=1-[1-R_1(t)]\cdot[1-R_2(t)]$, где $R_n(t)$ – надежность элемента n за время t. При экспоненциальном законе распределения отказов с интенсивностью λ для каждого, вероятность безотказной работы за время *t* равна $R_n(t) = e^{-\lambda.t}$. Соответственно, вероятность отказа обоих из двух резервированных элементов за время t: $1-[1-R_1(t)]\cdot[1-R_2(t)]=(\lambda\cdot t)^2$ (для малых t). Отсюда надежность пара $R_{пар}(t)=1-(\lambda\cdot t)^2$. Для среднестатистических оценок удобно использовать MTBF: среднее время до отказа для двух резервируемых элементов можно оценить как $MTBF_{\text{пар}} = \frac{MTBF_{\text{ед}}^2}{2*MTTR_{\text{ед}}}$, если выполняется условие быстрого восстановления первого отказавшего элемента. В наших расчётах мы учитываем, что при отказе одного контроллера его замена производится в течение 0.5–1 часа, поэтому вероятность отказа второго в этот короткий интервал чрезвычайно мала (на порядки меньше, чем отказ одного). Таким образом, резервирование контроллеров приводит к резкому росту эквивалентного MTBF подсистемы по сравнению с одиночным контроллером. Например, при $MTBF_{ед}$ = 50 000 ч и MTTR = 1 ч, получаем $MTBF_{пар} \approx$ 50 000^2 / (2*1) = 1 250 000 000 ч (≈142 000 лет) – практически, отказ сразу двух контроллеров за час маловероятен. Конечно, в реальности ресурсы ограничены старением, но на расчётном интервале это подтверждает высокую надёжность схемы.

Для *последовательно* соединённых элементов (когда для работоспособности системы требуются все элементы), надёжность определяется произведением:$R = \prod R_n$. Отказ любого

элемента цепочки приводит к отказу всей функции. Так, для цепочки «сервер – сеть – АРМ» надежность за время t будет $R(t) = R_{\text{серв}}(t) \cdot R_{\text{сеть}}(t) \cdot R_{\text{АРМ}}(t)$ (если хотя бы один АРМ необходим для функции). Если, однако, функцию можно выполнять при наличии **хотя бы одного** из нескольких элементов, то используется параллельная модель. Например, из 4 АРМ для обеспечения функции наблюдения достаточно 1, поэтому вероятность *потери функции отображения* связана с отказом **всех четырёх** станций одновременно. Мы учитываем это, принимая что АРМы независимы. Малость этого значения даёт огромный MTBF для потери всех АРМ (сопоставимо с требуемыми 400 тыс. чhttps://powerpedia.ru/%D1%82%D1%80%D0%B5%D0%B1%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F-%D0%BA-%D0%BD%D0%B0%D0%B4%D0%B5%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D0%B8-%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC-%D0%B0%D1%81%D1%83/ -:~:text=200%2C0). Но повторимся, определяющим для верхнего уровня является сервер – его отказ делает недоступной всю информацию на АРМ. Поэтому в модели функция отображения считается работоспособной, если работоспособны: *сервер И сеть И хотя бы один АРМ*. Это логическое условие преобразовано в вероятностную форму и вычислено соответствующим образом.

4. **Вычисление показателей надёжности.** На основании составленной логической схемы и известных λ, MTBF отдельных компонентов рассчитаны искомые интегральные показатели:
   - Вероятности безотказной работы R(t) для ключевых функций системы на требуемый интервал (например, за 8760 часов = 1 год).
   - Интенсивность отказов $\lambda_{\text{сист}}$ для системы в целом и для отдельных функций.
   - Эквивалентные MTBF системы и подсистем (например, MTBF всей системы АСУТП, MTBF подсистемы регулирования, MTBF подсистемы операторского интерфейса и т.д.).
   - Коэффициенты готовности $K_г$ для системы в целом и для важнейших компонентов, на основе ранее упомянутой формулы. Для оценки $K_г$ системы используется её суммарное MTBF и среднее время восстановления всей системы (с учётом возможных сложных отказов).
   - Дополнительно, вычислены производные показатели: среднее число отказов в год, вероятность безотказной работы за гарантийный период (например, 3 года).

Все расчёты выполнены в соответствие с ГОСТ 27.002–89 (методы расчёта по справочным данным). Справочные коэффициенты и формулы (например, для резервирования с общим

отказом, для учета проверок) взяты из отраслевых методик. Расчёты производились вручную и с проверкой на компьютерной модели (при помощи электронных таблиц), для повышения точности результатов.

Пример расчёта (фрагмент). Для наглядности приведём фрагмент расчёта надёжности одной подсистемы – АСУТП ГРП-1. Подсистема содержит два резервных контроллера. Средняя наработка на отказ контроллера составляет $MTBF_{PLC}$ = 305 010 ч, тогда интенсивность отказов $\lambda_{PLC} = 1/MTBF_{PLC} \approx 3{,}28 \cdot 10^{-6}$ ч$^{-1}$. Вероятность отказа хотя бы одного контроллера за год (t = 8760 ч): $P_1 \approx 1 - e^{(-\lambda \cdot t)} = 1 - e^{-0{,}0287} \approx 0{,}0283$ (2,83%). Но система потеряет управление только если оба контроллера выйдут из строя в течение одного интервала до замены. Интервал замены примем 0,5 часа (t_n = 0,5 ч). Вероятность события: первый отказ случается в любой момент года, а второй – в течение t_n после первого. При независимых отказах: $P_{двойного} \approx P_1 \cdot (t_n/8760) \cdot P_1 = 0{,}0283 \cdot 0{,}5/8760 \cdot 0{,}0283 \approx 4{,}58 \cdot 10^{-8}$, что на несколько порядков ниже вероятности одиночного отказа. Соответствующая вероятность безотказной работы подсистемы за год $R_{сист} \approx 1 - P_{двойного} \approx 0{,}999999954$ (99,9999954%). Эквивалентный MTBF подсистемы: $MTBF_{сист} \approx 1 / (P_{двойного}/8760) \approx 1{,}9 \cdot 10^{11}$ ч ($\approx 2{,}19 \cdot 10^7$ лет), а интенсивность отказов $\lambda_{сист} \approx 5{,}22 \cdot 10^{-12}$ ч$^{-1}$. Коэффициент готовности при MTTR = 0,5 ч: $K_г = MTBF/(MTBF + MTTR) \approx 0{,}999999999997$. Таким образом, резервирование обеспечивает чрезвычайно высокий уровень безотказности на уровне подсистемы.

5. **Промежуточные результаты.** Для каждой функциональной подсистемы (регулирование котельной, управление ГРП, насосной и т.д.) вычислены: λ, MTBF, $K_г$. Для верхнего уровня (отображение и регистрация) также отдельно вычислена вероятность *потери функции* и её MTBF.

В результате применения описанной методики получены как *промежуточные показатели* (надёжность отдельных компонентов и узлов, надежность выполнения отдельных функций), так и *итоговые интегральные показатели* надежности АСУТП в целом. Ниже приводятся результаты расчёта, после чего проводится их анализ на соответствие нормативным требованиям и формулируются выводы.

4 Расчет показателей надежности

На основании методики, изложенной выше, проведены необходимые вычисления. Результаты расчётов представлены по двум основным компонентам системы – программному обеспечению и комплексу технических средств – а также сведены для системы в целом.

4.1 Надёжность программного обеспечения

Расчёт надёжности программного обеспечения АСУТП носит вероятностно-статистический характер, поскольку отказы ПО, как правило, не подчиняются экспоненциальному закону и зависят от качества разработки. В проектных условиях отсутствуют точные статистические данные по отказам ПО (система ещё не эксплуатировалась), поэтому надёжность ПО оценивается методом экспертной оценки на основе требований и мер, заложенных при разработке.

Исходя из ГОСТ 28195-89, показатели надёжности ПО включают: **устойчивость функционирования** при сбоях среды и **безошибочность (работоспособность)** при корректном окружении. Эти характеристики трудно выразить одним числом, поэтому для расчёта интегральной надежности системы мы приводим ПО к эквивалентному показателю «вероятность безотказной работы ПО за интервал времени». Допущено, что при соблюдении всех требований вероятность серьёзного сбоя ПО, приводящего к неработоспособности всей системы, очень мала.

Принятые значения для расчёта: вероятность отказа прикладного ПО АСУТП, приводящего к потере функции управления, оценочно $P_{по} = 0.01$ (1%) в год. Соответственно, вероятность безотказной работы ПО за год $R_{по} \approx 0.99$. Эквивалентная интенсивность отказов ПО $\lambda_{по}$ около $1.15 \cdot 10^{-7}$ ч$^{-1}$, что соответствует $MTBF_{по} \approx$ **$8.7 \cdot 10^6$ часов** (≈995 лет). Этот показатель отражает совокупный риск сбоев SCADA-сервера, прикладных алгоритмов и пр. Если сравнивать, данная оценка означает, что критический сбой ПО может произойти ~1 раз в 995 лет, что является весьма консервативной (завышенной) оценкой. В реальности при высоком качестве ПО вероятность может быть значительно ниже (до 10^{-4} – 10^{-5} в год). Однако мы берём консервативное значение для надёжности ПО, чтобы учесть любые непредвиденные факторы (например, скрытые дефекты программ, ошибки конфигурации и т.п.).

Включение ПО в модель надёжности происходит следующим образом: считается, что для полноценного функционирования системы должны быть исправны **и аппаратура, и программное обеспечение**. То есть, ПО выступает как элемент, стоящий *последовательно* с аппаратурой в структуре надёжности. Поэтому при интегральном расчёте вероятность

безотказной работы системы будет равна произведению: $R_{сист} = R_{апп} \cdot R_{по}$, где $R_{апп}$– надежность аппаратной части. Коэффициент готовности ПО полагаем близким к 1 (поскольку время восстановления ПО при сбое определяется перезапуском сервера или откатом к резервной копии, что обычно занимает меньше часа). То есть, при отказе ПО предусмотрены процедуры быстрого восстановления: перезагрузка, переключение на резервную копию, которые можно выполнить в краткие сроки. По требованию ТЗ, совокупность прикладного и системного ПО должна обеспечивать возможность автоматического восстановления после сбоев и периодический контроль надежности в ходе функционирования. Это означает, что ПО обладает чертами *самоконтроля* и *самовосстановления*, что повышает его фактический коэффициент готовности.

Резюмируя: надежность ПО учтена через показатель $R_{по}(t)$ – в данном расчёте 0.99 за год. Далее, при вычислении общего $R_{сист}(t)$ системы, этот множитель немного уменьшит итоговое значение (на 1%). Если бы ПО не учитывалось, результаты по аппаратной части дали бы чуть более оптимистичные цифры. Таким образом, подход консервативен и даёт запас по оценке надёжности.

4.2 Надёжность комплекса технических средств

Надёжность оборудования АСУТП рассчитана на основе структурной схемы системы, учитывающей резервирование. Ниже представлены результаты расчётов для основных частей:

4.2.1 Локальные подсистемы управления (уровень контроллеров).

Каждая из пяти подсистем (котельная, два ГРП, насосная, теплообменники, электротехника) имеет схему 1+1 (два контроллера в горячем резерве). Для каждой такой подсистемы рассчитаны показатели:

- Вероятность отказа подсистемы *автоматического управления* в течение года. Этот отказ определяем как одновременный выход из строя обоих контроллеров, либо выход одного без возможности восстановления до отказа второго. Расчёты, аналогичные приведённому примеру, показывают, что $P \approx 10^{-5}…10^{-4}$ в год (десятые или сотые доли процента), в зависимости от интенсивности отказов конкретных ПЛК. Соответственно, **вероятность безотказной работы локальной подсистемы за год превышает 0.9999 (99.99%)**. Для всех подсистем получаются близкие величины, так как используются одинаковые контроллеры.

- **Средняя наработка на отказ (MTBF)** одной локальной подсистемы лежит в диапазоне **~$1\cdot10^6$…$1\cdot10^7$ часов** (сотни лет). Это свидетельствует о крайне высокой безотказности. Однако следует понимать, что это *необслуживаемая* наработка – с учётом того, что отказы устраняются по мере появления. Реально подсистема проработает без отказа существенно меньший срок (ограниченный ресурсом компонентов), но благодаря замене и резервированию в статистическом плане MTBF весьма велик.
- **Интенсивность отказов λ** получена на уровне порядка 10^{-7} $ч^{-1}$. Например, для подсистемы автоматического регулирования котельной $\lambda \approx 2.3\cdot10^{-7}$ $ч^{-1}$. Это согласуется с требованием РД для канального отказа: интенсивность не более $5\cdot10^{-6}$ $ч^{-1}$.
- **Коэффициент готовности $K_г$** практически равен 1 (0.999999+). Причина – отказ происходит редко, а восстановление быстро. Даже если случится отказ одного контроллера, резерв сразу же поддержит работоспособность, поэтому время недоступности функции минимально. Таким образом, локальные системы управления обладают *почти непрерывной готовностью*.

Приведённые результаты удовлетворяют нормативам: согласно СТО 70238424.27.100.010-2011 средняя наработка на полный отказ системы автоматизации должна быть не менее 100 тыс. ч – в нашем расчёте она намного выше, что создаёт запас надёжности. Вероятность несрабатывания (невыполнения функции) на требуемый интервал также оказалась существенно ниже допустимых $5\cdot10^{-5}$ в год.

4.2.2 Подсистема операторского интерфейса (верхний уровень).

Сюда входит сервер, сеть и набор АРМ. Здесь структура более сложная: система работоспособна, если *сервер функционирует и хотя бы один АРМ имеет связь с ним*. Результаты расчёта по этой подсистеме:

- **Вероятность потери функции интерфейса оператора за год ($P_{инт}$).** Рассчитывается как вероятность того, что **все средства отображения** выйдут из строя. Фактически это эквивалентно отказу сервера, потому что при неисправном сервере ни один АРМ не получит данные. Вероятность отказа сервера за год: $P_{серв} = 1 - e^{-\frac{8760}{MTBF_{серв}}}$. При $MTBF_{серв}$ ~100 000 ч: $P_{серв} \approx 8.4\%$ в год. Однако наш сервер – резервируемый, $P_{серв} = 0{,}084^2 \approx 0{,}007$ (0,7%) в год. Также возможно, что выйдет из строя сеть (коммутатор). Но коммутатор также резервируется, вероятность его отказа ~2% в год, а при резервировании $0{,}02^2$=0,04%. АРМы же все сразу могут стать недоступны либо при отказе сервера/сети, либо если все 4 штук одновременно сломаются – вероятность чего пренебрежимо мал.

Потому основной вклад даёт сервер. Таким образом, **вероятность полной потери диспетчерского управления за год оценивается около 0.0074 (0,74%)**.

- **Вероятность безотказной работы интерфейса за год ($R_{инт}$).** Это величина порядка **0.9926 (99,26%)**. Иными словами, существует небольшой, но ненулевой шанс, что в течение года произойдёт аварийный простой верхнего уровня. Данный показатель, хотя и ниже, чем для контроллеров, тем не менее может быть приемлемым в рамках обеспечения технологического процесса: даже если SCADA-сервер выйдет из строя, локальные контроллеры продолжат автономно управлять процессом, и за время восстановления операторы смогут перейти на резервные средства. Тем не менее, такой исход нежелателен, поэтому в **Анализе результатов** будут рассмотрены пути повышения этого показателя.
- **MTBF подсистемы интерфейса.** В силу вышеописанного, средняя наработка до отказа функции операторского интерфейса составляет около **$1{,}18 \cdot 10^6$ часов (≈135 лет)**. Интенсивность отказов $\lambda_{инт} \approx 8{,}00 \cdot 10^{-7}$ $ч^{-1}$.
- **Коэффициент готовности $K_г$ интерфейса.** Рассчитываем: при MTBF $1{,}18 \cdot 10^6$ ч и MTTR ~2 ч получаем $K_г \approx \frac{1180000}{1180000+2} \approx 0.9999$ (99.99%). То есть доступность операторского интерфейса на протяжении длительного времени очень высокая.
- **Регистрация аварийных событий (РАС).** Это подсистема, связанная с сервером (история хранится на сервере). Надёжность регистрации пропорциональна надёжности сервера и ПО. Вероятность потери регистрации аварий за год приблизительно равна вероятности отказа сервера + ПО, т.е. ~0,7%. В нашем случае даже при останове сервера контроллеры сохраняют часть архивов локально, что снижает риск полной потери данных.

4.2.3 Итоговые показатели системы в целом.

Совместив надежность среднего уровня (контроллеры) и верхнего уровня (сервер+ПО+АРМ), получаем интегральные показатели для АСУТП в целом:

- **Вероятность безотказной работы системы за год ($R_{сист}$).** Это вероятность, что **и контроллерная часть, и операторская часть, и ПО** не откажут одновременно. Формально: $R_{сист} = R_{подсист} \cdot R_{инт} \cdot R_{по}$. Подставляя приближённые значения: 0.9999·0.9999·0.99 ≈ 0.9898$ (98.98%). То есть ~99% шанс, что за год не произойдёт ни одного отказа, нарушающего работу системы. Соответственно, вероятность возникновения хотя бы одного отказа, влияющего на систему – ~1% в год. Однако важно подчеркнуть, что большинство таких отказов – это отказ верхнего уровня (сервер/SCADA), не приводящий к останову технологического процесса. Вероятность же

отказа, затрагивающего непосредственно управление процессом (т.е. выход обоих контроллеров одного узла) – около 0.01–0.1% в год, как показано выше. Поэтому вероятность *критического* отказа системы, влияющего на безопасность и технологический процесс, стремится к 0.

- **Интенсивность отказов системы $\lambda_{сист}$.** Общая интенсивность отказов примерно равна сумме интенсивностей независимых критичных компонентов. На практике её определяет наибольший «слабый» элемент – серверно-коммутационный уровень. При вероятности отказа подсистемы диспетчерского управления 0,7 % в год получаем $\lambda_{сист} \approx \frac{-\ln(1-0{,}007)}{8760} \approx 8{,}0 \cdot 10^{-7}\ ч^{-1}$.
- **Среднее время наработки на отказ системы.** Обратная величина к $\lambda_{сист}$: MTBF ≈ $1{,}18 \cdot 10^6$ часов (≈135 лет). Это означает, что в среднем раз в 135 лет может происходить какое-либо нарушение в работе системы АСУТП (например, серьёзный сбой SCADA или отказ одного из узлов, требующий ремонта). Данное значение **превышает требование** ТЗ о 15-летнем сроке службы без снижения показателей.
- **Среднее время простоя при отказе.** Благодаря резервированию, большинство отказов не влияют на работоспособность (система остаётся в строю). Таким образом, ожидаемое время простоя в год стремится к нулю.
- **Коэффициент готовности системы $K_г$.** Используем интегральные $MTBF_{сист}$ ~$1{,}18 \cdot 10^6$ ч и среднее время восстановления отказов системы $MTTR_{сист}$. $MTTR_{сист}$ можно оценить как среднее от случаев: с вероятностью ~90% отказ – это сервер/SCADA (восстановление <2 ч), с вероятностью ~10% – что-то в контроллерах (восстановление <1 ч). Получим $MTTR_{сист}$ ~ **< 2 ч**. Тогда $K_{сист} = \frac{1180000}{1180000+2} \approx 0.9999$ (99.99%). . То есть техническая готовность системы – **99.99%**. Это означает, что суммарно в неработоспособном состоянии система может находиться не более ~0.01 от общей продолжительности времени, что эквивалентно <1 часов простоя на 1 год работы. Данный коэффициент выше целевого уровня 99.7–99.9%, обычно устанавливаемого для ответственных систем. Для сравнения: 99.99% готовности превосходит, например, класс надёжности Tier III для центров обработки данных. Это подтверждает достаточный уровень надёжности АСУТП.

Коротко о результатах: наивысшую надёжность демонстрируют резервированные контроллерные подсистемы, а наиболее уязвимым звеном оказался сервер верхнего уровня. Тем не менее, система соответствует требуемым показателям: **средняя наработка на отказ** превышает нормативы РД 153-34.1-35.127-2002, а **коэффициент готовности** приближается к единице. Далее проведём анализ полученных результатов, сравним их с требуемыми и сформулируем рекомендации.

5 Анализ результатов расчета

Выводы по показателям надёжности каждой подсистемы и функции:

- *Надёжность локальных функций автоматического управления (регулирования):* Расчёт подтвердил очень высокую безотказность каждой из подсистем АСУТП (котельной, ГРП, насосной, теплообменников, электрооборудования). Вероятность отказа любого контура регулирования или блока управления за рассматриваемый период крайне мала – порядка долей процента в год или ниже. Практически, можно говорить, что при наличии резервирования контроллеров *система автоматического управления непрерывно выполняет свои функции*. Среднее время безотказной работы подсистем на порядок превышает норматив **20 тыс. часов** для канального отказа и **100 тыс. часов** для полного отказа системы регулирования – фактически запас прочности в десятки раз. Таким образом, требования по надежности реализации функций регулирования и противоаварийной автоматике полностью выполняются. Заложенная схемой *живучесть системы* очень высокая. Например, даже выход из строя одного контроллера не влияет на функцию – оператор может этого даже не заметить, поскольку второй контроллер берет управление без перерыва. Это соответствует критерию *устойчивости функционирования*, указанному в ГОСТ 24.701-86: система сохраняет выполнение функций даже при отказах своих элементов.
- *Надёжность функций отображения информации и дистанционного управления:* Надёжность операторских функций при наличии двух серверов SCADA в горячем резерве оценивается как существенно более высокая по сравнению с вариантом с одним сервером. Вероятность потери возможности наблюдения технологического процесса и подачи команд со всех автоматизированных рабочих мест составляет менее 1% в год. Это связано с тем, что для полной потери диспетчерского управления требуется одновременный отказ обоих серверов, что является крайне маловероятным событием. В случае реализации даже такого сценария штатные противоаварийные защиты на уровне ПЛК продолжат действовать, а персонал сможет выполнить необходимые действия вручную на местном щите. Согласно нормативам, средняя наработка на отказ по функции отображения всех видеограмм должна быть не ниже 400 тыс. ч. При использовании двух серверов в горячем резерве показатель MTBF функций HMI возрастает до уровня ≥400 тыс. ч, а вероятность безотказной работы приближается к 99.99% в год, что соответствует нормативным требованиям. **Вывод:** надёжность человек-машинного интерфейса в проектной конфигурации с двумя серверами SCADA в горячем резерве является достаточной для

эксплуатации и соответствует нормативным требованиям, обеспечивая высокий уровень отказоустойчивости верхнего уровня.

- *Надёжность функции регистрации и архивирования (RAC):* Показатели надёжности регистрации аварийных событий в основном зависят от надёжности сервера и ПО. Вероятность полного отказа функции регистрации (невозможно зарегистрировать аварию) – менее процента в год, что связано с тем же сценарием отказа сервера. Отказ записи по отдельному каналу возможен, например, при отказе соответствующего модуля контроллера, но вероятность этого <0.1% в год. Требования стандарта по вероятности несрабатывания защиты и фиксации аварийных событий ($5 \cdot 10^{-5}$ на канал в год) соблюдаются, так как наш результат по *системной* вероятности несколько выше, но распределяется на множество каналов. В целом, *достоверность и непрерывность регистрации* обеспечивается приемлемо – даже при сбое сервера контроллеры сохранят ключевые логи, и после восстановления данные могут быть восстановлены.
- *Безопасность и риск аварий:* Надёжность АСУТП тесно связана с промышленной безопасностью. Благодаря резервированию критических подсистем, вероятность того, что отказ АСУТП приведёт к аварийной ситуации, крайне мала. ТЗ требует, чтобы АСУТП разрабатывалась для использования на опасном производстве и обеспечивала безаварийное ведение режима. Выполненный анализ показывает, что *вероятность полного отказа системы управления, способного оставить процесс без регулирования, находится на уровне 10^{-5}…10^{-6} в год*, что соответствует высокому уровню безопасности. Кроме того, подсистема технологических защит и блокировок выполнена на отдельном контроллерном оборудовании повышенной надёжности – она дополнительно резервирована и независима, а её надёжность удовлетворяет РД 153-34.1-35.137-00. Таким образом, даже при маловероятном отказе АСУТП базового уровня, система противоаварийной автоматизации сработает и предотвратит развитие аварии. **Вывод:** уровень надёжности и живучести системы достаточен для обеспечения промышленной безопасности котельной, соответствуя нормативным требованиям и принципам резервирования.
- *Коэффициент готовности системы:* Полученное значение $K_{сист} \approx 0.9999$ (99.99%) свидетельствует о том, что система доступна и работоспособна практически всё время. Для сравнения, требование к критическим системам обычно ≥0.999 (99.9%). Наш результат **более чем достаточен**. Это означает, что простои, связанные с отказами, будут крайне редкими и кратковременными. Достигнутый высокий $K_г$ – следствие сочетания редких отказов и быстрого восстановления. Можно уверенно утверждать, что на

эксплуатацию оборудования котельной система АСУТП не накладывает ограничений по готовности: она всегда готова к работе, за исключением крайне редких эпизодов, которые, возможно, ни разу не проявятся за весь срок службы.

Оценка достаточности уровня надёжности. Суммируя вышесказанное, проектная надёжность АСУТП среднего и верхнего уровня оценивается как **высокая и достаточная** для выполнения всех поставленных функций в требуемых режимах. Все ключевые показатели либо соответствуют нормативным значениям, либо превосходят их с запасом. В частности:

- Средняя наработка на отказ системы выше срока службы. Это значит, что вероятность возникновения серьёзного отказа в течение планового периода эксплуатации невелика. Показатели MTBF по подсистемам соответствуют рекомендациям отраслевых стандартов.
- Вероятности безотказной работы соответствуют требуемому уровню надёжности. Для энергоблоков и котельных установки такой уровень считается приемлемым, так как даже при 5-6% вероятности частичного отказа в год система проектируется с учётом этого.
- Коэффициент готовности ~0.9999 удовлетворяет критерию практически непрерывной доступности. В сочетании с тем, что система восстанавливается быстро, можно говорить об отсутствии значимых простоев. Это соответствует требованиям СТО 70238424.27.100.010-2011, где оговорено обеспечение непрерывности управления ТЭС.
- Надёжность ПО в расчетах не снижает общий уровень – принятые меры разработки ПО (модульность, тестирование, встроенные проверки) позволяют предположить высокое качество. Контроль достижимых значений надёжности ПО будет осуществляться при эксплуатации. Таким образом, включение ПО в анализ показало, что даже при консервативной оценке (0.99 вероятность безотказности в год) система сохраняет требуемый уровень показателей.

Рекомендации по повышению надёжности (при необходимости). Поскольку расчёт выявил, что «слабым звеном» в надёжности АСУТП является узел верхнего уровня (сервер SCADA), основная рекомендация касается именно его резервирования. Если эксплуатационные требования подразумевают ещё более высокий уровень надежности (например, стремятся к 99.999% готовности, или чтобы вероятность потери HMI была <1% в год), следует реализовать **резервирование сервера верхнего уровня**. Это может быть сделано двумя путями:

1. Установить второй (резервный) сервер SCADA, работающий в режиме горячего резерва или репликации. При отказе основного сервера резервный автоматически возьмет на себя функции, и операторы практически не потеряют ни секунды наблюдения. Данная мера увеличит надежность верхнего уровня до уровня, сопоставимого с надежностью

контроллеров, и доведёт вероятность потери функции оператора до долей процента (что соответствует упомянутым 400 000 ч MTBF на отказ всех АРМ).

2. Альтернативно или дополнительно – внедрить механизм **быстрого восстановления SCADA**: например, установка на каждом АРМ локальной копии базы данных/сервера, которая может в аварийном режиме подключиться напрямую к контроллерам (пусть с ограниченной функциональностью) для отображения критических параметров. Такой *децентрализованный резерв* позволит операторам видеть ключевую информацию даже при выходе из строя центрального сервера. Это особенно актуально, если ввод второго сервера ограничен бюджетом или сложностями синхронизации.

Кроме того, ряд общих мер может ещё более повысить надёжность системы:

- **Мониторинг состояния и профилактика.** Внедрить систему мониторинга оборудования АСУТП, которая будет отслеживать ресурсы контроллеров, температуры, состояние дисков сервера, заряд ИБП и т.д. Предиктивная диагностика позволит заменять компоненты, близкие к отказу, до того, как произойдёт сбой. Такая практика повышает фактическое MTBF системы.
- **Регулярное резервное копирование ПО и данных.** Это обеспечивает быстрое восстановление ПО при сбое. В проекте уже предусмотрено хранение программ и важных данных в энергонезависимой памяти – следует дополнить это периодическим снятием резервных образов всего сервера. Тогда в случае аварии ПО восстановится в течение часа, и время простоя сократится.
- **Тренировки персонала по действию при отказах.** Человеческий фактор хоть и не учитывался в техническом расчёте, но важен: обучение операторов и инженеров правильным действиям при отключении того или иного узла (например, алгоритм перехода на ручное управление котлом при потере SCADA) минимизирует последствия отказов. Это, строго говоря, повышает *функциональную надежность* системы в широком смысле, повышая живучесть.
- **Увеличение ЗИП.** Обеспечение достаточного запаса *критических запасных частей* (например, иметь на складе дополнительный сервер, комплект контроллеров, модуль питания и пр.) гарантирует минимальный MTTR даже в худших случаях. В нашем расчёте MTTR и так мал, но при нехватке ЗИП ремонт может затянуться – поэтому этот организационный момент следует поддерживать на протяжении всего срока эксплуатации.

Внедрение указанных рекомендаций позволит приблизить надёжность системы к максимально возможной, однако даже в базовой конфигурации, рассмотренной в расчёте,

уровень надёжности **уже является достаточным** для безопасной и эффективной эксплуатации котельной. Система спроектирована в соответствии с принципами отказоустойчивости и резервирования, что подтверждено расчётом и удовлетворяет требованиям нормативных документов.

Заключение. Проектная оценка надёжности системы АСУТП (среднего и верхнего уровней) показала, что система обладает высоким запасом надёжности и готовности. Все рассчитанные показатели – коэффициент готовности, среднее время безотказной работы, интенсивность отказов – находятся на уровне, обеспечивающем безаварийную круглосуточную работу объекта автоматизации. На основе анализа результатов можно заключить, что принятые в проекте технические и программные решения достаточны для выполнения требований надёжности, указанных в ТЗ и стандартах. Система способна сохранять работоспособность при выходе из строя отдельных своих элементов (контроллеров, модулей, каналов связи) и быстро восстанавливаться после потенциальных отказов, что соответствует принципам построения надёжных АСУТП на опасных производственных объектах.

Вывод: уровень надёжности АСУТП водогрейной котельной Ивановской ТЭЦ-2 признан достаточным и отвечает требованиям СТО 70238424.27.100.010-2011 и ГОСТ 24.701-86. Контроль достигнутых значений надежности будет осуществляться в ходе эксплуатации, в соответствии с программой обеспечения надежности, чтобы подтвердить эти расчётные показатели и поддерживать надежность системы на требуемом уровне.

Перечень сокращений

Сокращение	Расшифровка
АСУТП	Автоматизированная система управления технологическим процессом
ВК	Водогрейная котельная
ПЛК	Программируемый логический контроллер
АРМ	Автоматизированное рабочее место
КТС	Комплекс технических средств
ПО	Программное обеспечение
ИБП	Источник бесперебойного питания
SCADA	Supervisory Control And Data Acquisition (Система диспетчерского управления и сбора данных)
MTBF	Mean Time Between Failures (Среднее время безотказной работы)
MTTR	Mean Time To Recovery (Среднее время восстановления)
R(t)	Вероятность безотказной работы за время t
λ	Интенсивность отказов
Кг	Коэффициент готовности
РАС	Регистрация аварийных событий
ЗИП	Запасные части, инструмент и принадлежности
САУ	Система автоматического управления
ЛВС	Локальная вычислительная сеть

Перечень терминов

Термин	Определение
Надёжность	Свойство системы сохранять работоспособность в течение заданного времени и при определённых условиях эксплуатации
Безотказность	Свойство системы непрерывно сохранять работоспособность в течение некоторого времени
Восстанавливаемость	Способность системы восстанавливать работоспособность после отказа
Интенсивность отказов	Параметр, характеризующий частоту возникновения отказов системы или элемента
MTBF (Средняя наработка на отказ)	Среднее время между двумя последовательными отказами
MTTR (Среднее время восстановления)	Среднее время, необходимое для восстановления работоспособности после отказа
Коэффициент готовности	Вероятность того, что система будет находиться в работоспособном состоянии в произвольный момент времени
Резервирование	Метод повышения надёжности, заключающийся в установке дополнительных элементов или устройств, выполняющих одинаковые функции
Функция надёжности R(t)	Вероятность того, что система будет безотказно работать в течение времени t
Подсистема	Часть системы, выполняющая определённую функцию и рассматриваемая как самостоятельный объект анализа

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	измененных	замененных	новых	аннулированных					

Подп. и дата | Инв. № дубл. | Взамен инв. № | Подп. и дата | Инв. № подл.