ПОКАЗАТЕЛИ НАДЕЖНОСТИ И ИНЖЕНЕРНАЯ ПРАКТИКА

А.М. ПРОКОПЬЕВ, П.В. ПОЛЯНСКИЙ
(ЗАО ПК "Промконтроллер")

Рассматриваются основные понятия в области надежности систем автоматического управления и методика их практического применение в промышленности. Показано, что при определении требований к надежности системы управления необходимо исходить из надежности выполнения ею наиболее ответственных функций, как основного элемента, определяющего безопасность и экономические параметры работы технологического процесса.

Инженерный и производственно-технический персонал на практике зачастую сталкивается с задачами формирования требований к показателям надежности или с необходимостью обоснованного выбора одного из вариантов технических решений для реконструируемой или вновь создаваемой системы автоматического управления или защиты. Решение такого рода задач требует ясного понимания смысла применяемых показателей надежности, а также влияния значений выбранных показателей надежности на производственную деятельность и безопасность.

В современной экономической ситуации сотрудникам, отвечающим за модернизацию производства, при выборе оптимального варианта будущей системы наряду с техническими данными, приходится анализировать сметы затрат и оценивать их обоснованность. Поэтому ясное понимание смысла показателей надежности становится фактором оптимизации не только для систем управления производственного процесса, но и условием оптимизации издержек предприятия.

При определении требований к показателям надежности системы приходится сталкиваться с ситуацией, когда принятие решений, касающихся одного из элементов повышения надежности – резервирования элементов системы, осуществляется на основании сложившихся стереотипов. В практической работе нередки случаи, когда представители фирм, специализирующиеся в области безопасности, ссылаясь на недавно опубликованные ГОСТ Р МЭК 61508, выдвигают требования к резервированию модулей контроллера системы САУ/ПАЗ (модулей УСО или процессорного модуля) в зависимости от отнесения объекта к одной из групп согласно интегральным показателям безопасности. На наш взгляд, такой подход является упрощенным и не учитывает тот факт, что основным показателем безопасности является надежность выполнения функции безопасности, которая обеспечивает недопущение аварийных ситуаций, а в случае их возникновения переводит объект в безопасное состояние. Требования к надежности (а резервирование является одним из элементов обеспечения надежности) должны формироваться с учетом сопоставления потерь, связанных с отказами, и затрат, связанных с обеспечением надежности.

Предлагаемая статья рассчитана на инженера-практика (производственника), занимающегося эксплуатацией автоматических и технических систем, и учитывает, что в его повседневную работу не входит работа с формулами из теории надежности и теории вероятности. Цель данной статьи – помочь инженерно-техническому персоналу правильно трактовать показатели надежности, которые встречаются в технической документации, и значения которых требуется определить или оценить в процессе разработки вновь создаваемых или реконструируемых систем автоматического управления (САУ) и автоматических защит (ПАЗ). В статье мы стараемся доступным и понятным образом осветить некоторые наиболее проблемные, на наш взгляд, вопросы, касающиеся показателей надежности, и на простых примерах продемонстрировать влияние рассматриваемых показателей надежности на наиболее существенные характеристики системы. Изложение материала, представленно-

го в литературе по теории надежности [1, 2, 3], остается за рамками данной статьи.

Как уже сказано выше, резервирование – это один из способов обеспечения заданных показателей надежности, а определение (задание) показателей надежности – это способ обеспечения обусловленных потребностями производства показателей безопасности и качества технологического процесса. В работах [1, 2, 5] указывается, что требования к резервированию и показателям надежности должны определяться на основе анализа технологического процесса и описания возможных аварийных ситуаций с учетом влияния социальных и экономических последствий отказа функций, выполняемых автоматизированной системой управления и защит. Другими словами, довольно часто требуется обеспечить не просто надежность системы, а определенную надежность отдельных функций системы, ответственных за безопасность технологического процесса или обеспечивающих минимизацию экономических потерь.

В производственной практике встречаются случаи, когда требования к резервированию отдельных элементов системы, сделанные под ожидание улучшения качественных характеристик и получения системы с высокой надежностью, оборачивается высокой интенсивностью отказов в системе, что вызывает рост объема работ обслуживающего персонала и требует увеличения затрат на приобретение большого количества запасных элементов (ЗИП).

Для подсистем автоматических защит, выполняемых на контроллерной технике, требования по резервированию модулей контроллера, дублированию, а в некоторых случаях и троированию (резервированию с кратностью три), выдвигаются без должного предварительного анализа, а вопрос об их обоснованности воспринимается как кощунственный: “Это же система защит!” Такой подход обусловлен исторически сложившимся мнением, что резервирование является необходимым условием в подсистемах ПАЗ. Мы исходим из утверждения, что выдвигаемые требования должны быть обоснованы и направлены на максимальное повышение эффективности решения поставленной задачи. Чтобы оценить реальную эффективность принятых решений, необходимо ответить на один вопрос: “Какие задачи мы пытаемся решить, выставляя требования на резервирование тех или иных модулей?”

Поскольку повышенные требования к надежности и резервированию существенно влияют на стоимость внедрения и обслуживания системы, набор таких критериев должен формироваться на основании некоторого компромисса между приемлемым уровнем безопасности, с учетом рисков, и затратами на его достижение. Другими словами, обоснованность требований к надежности системы должна определяться ожидаемым экономическим эффектом от их выполнения. Кроме того, необходимо ясно представлять себе тот факт, что применение резервирования, увеличивая надежность отдельных узлов системы, повышает стоимость системы, а значит ухудшает ее экономические показатели. Вводя в систему резервирование элементов, мы преследуем цель увеличить надежность некоторых выполняемых системой функций, однако при этом в системе возрастает общее число элементов, и увеличивается частота отказов.

В настоящей статье рассмотрены следующие вопросы:

1) показатель надежности – “вероятность безотказной работы”;
2) показатель надежности – “среднее время безотказной работы”;
3) решаемая задача определяет требования к показателям надежности;
4) повышение надежности системы путем резервирования наиболее ненадежных элементов;
5) время восстановления в системах с дублированием элементов оказывает существенное влияние на надежность системы;
6) обоснованность требований на резервирование с кратностью три отдельных элементов системы.

1. ПОКАЗАТЕЛЬ НАДЕЖНОСТИ – “ВЕРОЯТНОСТЬ БЕЗОТКАЗНОЙ РАБОТЫ”

На практике специалисты часто сталкиваются с необходимостью определения одного из показателей надежности – значения вероятности безотказной работы. Интуитивно понятно, что чем выше данный параметр, тем лучше. Но возникает вопрос, на какой промежуток времени работы (эксплуатации системы) устанавливать этот показатель и как определить его оптимальное значение. Для ответа на этот вопрос необходимо понимать сущность данного параметра.

Если с определением промежутка времени

понятно – он определяется периодом между плановыми остановами на регламентные работы, то с определением значения вероятности безотказной работы обычно возникают трудности, что вызвано вероятностным характером данной величины. Принимая решение по установке требований к вероятности безотказной работы, необходимо оценить, что для производства означает разница в одну сотую показателя вероятности безотказной работы? Например, необходимо выбрать один из двух предлагаемых вариантов реализации системы. Первый – система с вероятностью безотказной работы 0,99 и стоимостью 2 млн рублей. Второй – система с вероятностью безотказной работы 0,98 стоимостью 1,5 млн рублей. Другими словами, принятие решения сводится к ответу на простой вопрос: стоит одна сотая в вероятности безотказной работы 500 тысяч рублей или нет.

Наиболее наглядно "вероятность безотказной работы" можно представить, если взять её определение в терминах статистики [1, 2]. Тогда "вероятность безотказной работы" за время $t = t_1$ определяется как отношение числа элементов, безотказно проработавших от момента времени $t = 0$ до момента времени $t = t_1$, к числу элементов, исправных к начальному моменту времени $t = 0$. Другими словами, при вероятности безотказной работы элемента системы (прибор, модуль, задвижка и т.п.), равной 0,99 (обозначается как $P(t) = 0,99$), в системе из 1000 различных элементов за заданное время $t = t_1$ можно ожидать 10 отказов, а при вероятности безотказной работы $P(t) = 0,98$ – 20 отказов. Если в эксплуатации находится 100 элементов, то можно ожидать соответственно 1 и 2 отказа за аналогичный промежуток времени (Примечание 1). Теперь для решения вопроса, стоит ли одна сотая в вероятности безотказной работы 500 тысяч рублей или нет, требуется оценить, соответствуют ли экономические потери от прогнозируемых отказов оборудования предложенному увеличению стоимости технического решения.

Примечание 1.

1. Статистическое определение вероятностных величин наиболее наглядно, однако надо учитывать, что вероятностная величина, вычисленная по статистическим данным, обладает тем меньшей погрешностью, чем больше выборка, т.е. чем больше количество элементов, участвующих в определении вероятностной величины.

2. ПОКАЗАТЕЛЬ НАДЕЖНОСТИ – "СРЕДНЕЕ ВРЕМЯ БЕЗОТКАЗНОЙ РАБОТЫ"

В производственной практике часто используется другой показатель надежности – среднее время безотказной работы (Tср), тесно связанное с вероятностью безотказной работы. Этот параметр в литературе также называют "средним временем наработки до отказа" или "средним временем наработки до первого отказа" [1, 2]. Нетрудно заметить, что, зная вероятность безотказной работы и закон распределения отказов, можно определить и среднее время безотказной работы, и наоборот [1, 2]. В документации на техническую продукцию обычно указывается именно значение "среднего времени наработки до отказа".

Сталкиваясь с необходимостью определить требования к среднему времени безотказной работы, нужно ответить на несколько основных вопросов. Можно ли ожидать, что не будет отказа за время, меньшее чем "среднее время безотказной работы"? Соответствуют ли технические средства (элементы системы) заявленному в документации показателю надежности – среднему времени безотказной работы, если в течение времени эксплуатации, меньшим, чем заявленное среднее время безотказной работы, отказало два изделия? Сколько отказов технических средств можно ожидать за время, равное заявленному на изделие "среднему времени безотказной работы"?

"Среднее время безотказной работы" – это вероятностная величина, определяемая [1, 2] как математическое ожидание времени наработки элемента до отказа, или в терминах статистики – это отношение суммы времен наработки до отказа всех элементов к количеству элементов в выборке, т.е. когда все выбранные элементы отказали. Обычно в технических параметрах на изделие указывается "среднее время наработки до отказа", поскольку этот параметр является важным элементом характеристики надежности элемента. Зная "среднее время наработки до отказа", можно определить и другие значения параметров надежности.

Можно интерпретировать "среднее время наработки до отказа" через число отказавших за указанное время элементов. Для экспоненциального распределения имеем:

$$\lambda = 1/Tср, \quad (2.1)$$

$$P(t) = e^{-\lambda * t} \quad (2.2)$$

$$q(t) = 1 - P(t), \qquad (2.3)$$

где λ – интенсивность отказов элемента; Tср – среднее время наработки на отказ, определенное заводом изготовителем в технических параметрах на элемент; P(t) – вероятность безотказной работы элемента; q(t) – вероятность отказа элемента; t – текущее время эксплуатации элемента.

С учетом статистического определения вероятности отказа элемента в течение времени t, как отношение количества отказавших элементов в течение времени t к общему начальному количеству элементов в момент времени t = 0:

$$q(t) = n/N, \qquad (2.4)$$

где n – количество отказавших элементов за время t; N – первоначальное число исправных элементов, включенных в работу.

С учетом вышеприведенных формул (2.1 – 2.4) можно определить число отказавших элементов в зависимости от относительного времени (t/Tср).

$$n = N*[1 - P(t)] = N*[1 - e^{-(1/Tcp)*Tcp}] = N*[1 - e^{-(t/Tcp)}] \qquad (2.5)$$

Зависимость количества отказавших элементов (n) от логарифма относительного времени наработки [log(t/Tср)] при начальном количестве элементов N = 1000, определенная на основании формулы 2.5, приведена на рис. 1.

Из формулы 2.5 и приведенного графика видно, что "среднее время наработки до отказа" (Tср) – это время, за которое можно ожидать отказа 63,2 % из первоначально работающих элементов.

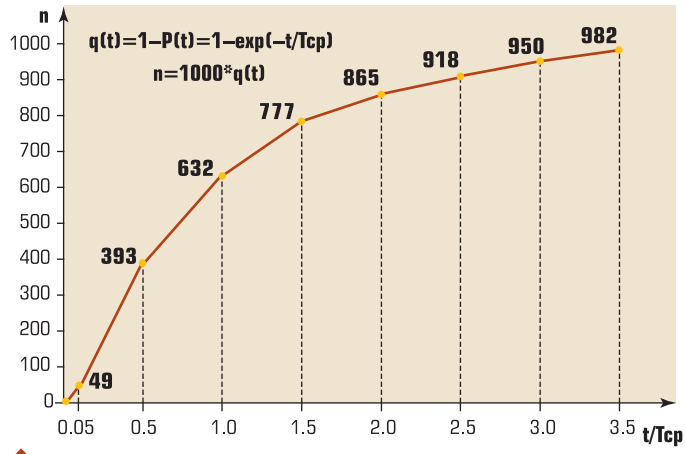

*Рис. 1. Зависимость числа отказавших элементов от времени работы q(t) = 1 – P(t) = 1– exp(–t/Tcp) n=1000*q(t)*

Таким образом, при заданном показателе надежности – времени наработки до отказа, равном 500 часов (Tср = 500 час.), можно ожидать, что из работающих на производстве 1000 элементов (с данной надежностью) за 500 часов откажет 632 элемента.

Учитывая вышесказанное и рис. 1, можно сделать вывод, что если в эксплуатации находится 10 элементов, то за время t = 0,5Tср может отказать 4 элемента (Примечание 1.1).

Примечание 2.

1. Необходимо различать два параметра надежности "*среднее время наработки до отказа*" и "*среднее время наработки между отказами*" в англоязычной литературе – *mean time between failures (MTBF)*. "Среднее время наработки между отказами" применяется для характеристики надежности восстанавливаемых объектов (элементов), при эксплуатации которых допускаются многократно повторяющиеся отказы. ГОСТ 27.002-89 определяет данный параметр как:

$$T = t/M\{r(t)\}, \qquad (2.6)$$

где T – среднее время наработки между отказами; t – суммарная наработка; r(t) – число отказов, наступивших в течение этой наработки; M{r(t)} – математическое ожидание числа отказов, наступивших в течение этой наработки.

Показатель надежности, определяемый как "*среднее время наработки до отказа*", определяет надежность конкретного элемента (типа элемента) в системе, он указывается в технических характеристиках завода изготовителя и используется для определения надежности выполнения системой функции, в которой участвует данный элемент.

Показатель же надежности, определяемый как "*среднее время наработки между отказами*", характеризует время между отказами различных элементов (не конкретного типа элемента или модуля), входящих в систему, с восстановлением отказавших элементов. Обычно этим показателем характеризуют общую надежность системы, содержащей различные типы и виды элементов. Данный показатель не применяют к элементам системы, представляющим типовые элементы замены. *Среднее время наработки между отказами*

обычно используется как показатель надежности для систем с резервированием и восстановлением отказавших элементов, определяет интенсивность отказов в системе, не приводящих к потере её работоспособности, и характеризует загруженность персонала, связанную с ремонтом (заменой) отказавших элементов.

Связь среднего времени наработки на отказ и среднего времени наработки между отказами, для экспоненциального распределения, можно вывести из определения интенсивности отказов [Л (1, 2)] и учитывая определение среднего времени между отказами TMTBF.

$$\lambda = \frac{n}{N * \Delta t} \qquad (2.7)$$

$$T_{MTBF} = \frac{\Delta t}{n} \qquad (2.8)$$

Получим соотношение между средним временем наработки между отказами и средним временем наработки на отказ.

$$T_{MTBF} = \frac{Tcp}{N} \qquad (2.9)$$

2. Для каждого конкретного элемента, по условиям его конкретного применения, может быть определен один из параметров надежности (например, время наработки на отказ). Однако надо иметь в виду, что это будет конкретная реализация данного вероятностного параметра, и нельзя на основании одной реализации вероятностной величины делать вывод о соответствии или не соответствии заявленных в технической документации значений.

3. НАДЕЖНОСТЬ СИСТЕМЫ И НАДЕЖНОСТЬ ВЫПОЛНЕНИЯ ФУНКЦИИ

Важность обоснованного определения значений показателей надежности определяется задачами, которые должны обеспечить заданные показатели. Определение показателей надежности для системы и входящих в неё элементов – это способ обеспечения, обусловленный потребностями производства, показателей безопасности и качества технологического процесса, которые должны определяться на основе учета влияния социальных и экономических последствий отказа выполняемых автоматизированной системой (АС) функций.

Например, при решении задачи обеспечения безопасности управлением технологического процесса возможны три формулировки в постановке задачи, которые приводят к различным решениям:

- Обеспечить надежность выполнения системой функции предотвращения возникновения аварийной ситуации. При этом допустимы остановы технологического процесса по “ложным сигналам аварии” и остановы при отказах элементов системы; главное – не допустить аварии.
- Обеспечить надежность выполнения системой функции предотвращения возникновения аварийной ситуации, при этом недопустимы остановы технологического процесса по “ложным сигналам аварии” и остановы при отказах одного из элементов системы.
- Обеспечить живучесть системы, т.е. любые отказы элементов системы не должны приводить к потере системой контроля и управляемости технологическим объектом, т.е. выделяется несколько функций, которые обеспечивают “живучесть системы” и определяются элементы, обеспечивающие выполнение данных функций.

Первые две приведенные формулировки обеспечивают предотвращение возникновения аварийных ситуаций. Разница в этих определениях заключается в том, что первое определение не требует “обеспечения надежности всех элементов, участвующих в защитах”, а требует безусловного выполнения функции защиты. Другими словами, для обеспечения надежности выполнения функции защиты от возникновения аварийной ситуации необходимо или обеспечить “аварийный” останов технологического объекта при возникновении отказов элементов системы, или резервировать элементы, отказ которых будет препятствовать выполнению функции защиты. Т.е. если элемент при всех возможных видах его отказа (потери работоспособности) обязательно принимает определенное положение (формирует на выходе значение), которое предотвращает возникновение аварийного состояния и развитие аварийной ситуации, то вопрос о необходимости его резервирования необходимо обосновывать. Например, возможность отказа отсечного клапана, вызывающего невозможность отсечки, обосновывает требование на его резервирование.

Вторая формулировка требует обеспечить не только выполнение функции защиты, но

и недопущение остановов технологического оборудования при возникновении единичных отказов элементов системы. Данное требование можно выполнить только резервированием всех элементов, участвующих в выполнении функции предотвращения возникновения аварийных ситуаций.

Третья формулировка требует обеспечить живучесть системы, т.е. допускаются отказы элементов системы, но эти отказы при потере отдельных функций, выполняемых системой, не должны приводить к потере контроля и управляемости технологическим объектом. Данное требование можно обеспечить только резервированием элементов системы, определяющих её живучесть.

ГОСТ 24.701-86 [5] рекомендует формулировать задачу, решаемую установлением требований по надежности на основании анализа требуемого уровня безопасности, и определять требования к надежности путем сопоставления потерь, связанных с отказами и затрат, связанных с обеспечением надежности.

4. ТРЕБОВАНИЯ К ПОКАЗАТЕЛЯМ НАДЕЖНОСТИ ДОЛЖНЫ БЫТЬ ОБОСНОВАНЫ РЕШАЕМОЙ ЗАДАЧЕЙ

Иногда встречается такая ситуация когда, не имея возможности провести анализ необходимого уровня безопасности и обоснованно определять требования к надежности, закладывают требования по резервированию отдельных элементов системы. При этом часть элементов системы (например: датчики, линии связи, исполнительные механизмы), интенсивность отказов которых почти на порядок выше интенсивности отказов резервируемых элементов, не резервируются. Иногда под данные требования включают субъективные пожелания. Например: “Я хочу, чтобы остановов по причине отказа элементов контроллера, не было”. На наш взгляд, вышеприведенный субъективный подход является необоснованным как с технической, так и с экономической стороны. Основной поток отказов в системе, где имеются элементы с существенно различной интенсивностью отказов, определяется элементами с низкой надежностью (высокой интенсивностью отказов), и резервирование более надежных элементов не приведет к снижению числа нежелательных остановов.

Рассмотрим пример

Имеется объект – котельная с котлами небольшой мощности (например, котлы ДЕ-10). Стоимость запуска (розжига) такого котла небольшая, а в котельной предусмотрено обязательное наличие резервного котла, готового по команде оператора включиться в работу и покрыть недостачу тепловой мощности, вызванную остановом работающего котла. Потребитель тепловой энергии не критичен к кратковременному изменению параметров отпускаемой ему тепловой энергии (пара), которое возникает на время запуска резервного котла при остановке одного из работающих котлов.

Заказчиком системы (САУ и ПАЗ) котла ставится требование на резервирование процессорного модуля контроллера, которое обосновывается следующим образом:

- процессорный модуль как центральный модуль контроллера участвует в реализации всех функций системы по управлению и безопасности котлом и поэтому его надо резервировать;
- останова котла по причине отказа элементов контроллера не должно быть.

Недостаток данного подхода обусловлен тем, что требования на резервирование были выдвинуты без анализа требуемого уровня безопасности и формулирования задачи, которую предполагается решить установлением требований к надежности элементов системы; не проведено обоснование значений параметров надежности.

Разберем приведенную в примере ситуацию. Чтобы оценить обоснованность заявленных требований, необходимо определить, как повлияет резервирование процессорного модуля на:

- безопасность работы котла;
- число остановов котла по причине отказа элементов контроллера.

Безопасность работы котла

Безопасность работы котла определяется надежностью выполнения функции защит, которая обеспечивает недопущение появления и развития аварийной ситуации.

Современные микропроцессорные контроллеры, применяемые при построении систем управления и защит, имеют развитую систему диагностики и позволяют обеспечить аварийный останов технологического объекта в случае отказа программно-технических средств системы управления (защит) или при выявлении недостоверности сигнала одного

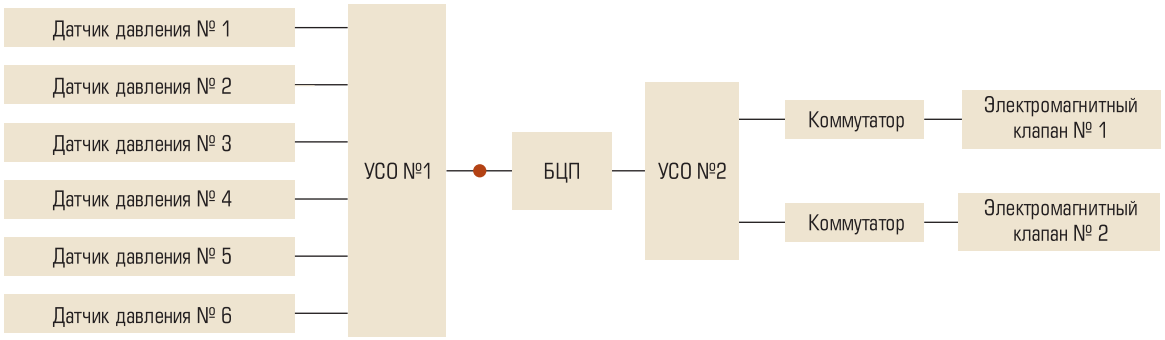

Рис. 2. Структура гипотетической системы защит котла

из датчиков, участвующего в определении аварийной ситуации.

Задача обеспечения надежного выполнения функции ПАЗ (защит), решается отключением подачи газа на горелки котла при выполнении условий:

- появления сигнала аварии, формируемого датчиком с дискретным выходом;
- ухода технологического параметра, измеряемого датчиком с аналоговым выходом за пределы установленных аварийных значений;
- выдачи системой сигнала на аварийный останов котла по условиям, определяемым встроенной системой диагностики:
  - определение недостоверности одного из технологических параметров, по которым осуществляется анализ аварийной ситуации (отказ датчика, обрыв линии связи, пропадание напряжения питания датчика);
  - отказ любого модуля УСО контроллера, воспринимающего сигнал от датчиков, по которым осуществляется анализ аварийной ситуации;
  - отказ модуля УСО контроллера, формирующего управляющие сигналы на аварийный останов технологического объекта;
  - отказ процессорного модуля контроллера.

Как видно из вышеприведенного, резервирование процессорного модуля контроллера не влияет на надежность выполнения системой функции “обеспечение безопасной работы котла”, т.к. в случае отказа процессорного модуля модуль УСО определит отказ и выполнит аварийный останов котла.

Число остановов котла по причине отказа элементов контроллера

Определим, как повлияет резервирование модуля центрального процессора на количество “ложных” остановов котла. Ложные остановы котла могут быть вызваны:

- отказом датчика аварийного параметра;
- отказом модуля УСО, воспринимающего сигнал датчика аварийного параметра;
- отказом модуля УСО, выдающего сигнал на исполнительное устройство, обеспечивающего аварийный останов котла;
- отказом силовых элементов – усилителя мощности сигнала, выдаваемого модулем УСО, и выдающего сигнал на исполнительное устройство, обеспечивающего аварийный останов котла;
- отказом модуля центрального процессора.

Примечание:

1. Отказы блоков питания и элементов линий связи для простоты расчета не учитываем.
2. Считаем, что элемент контроллера (модуль УСО, формирующий выходные сигналы) в случае отказа одного из элементов системы, участвующей в реализации функции защиты, обеспечивает выдачу сигнала на исполнительное устройство для аварийной остановки котла. Эта функция может быть реализована, например, на контроллерах МФК3000, МФК1500, выпускаемых ЗАО ПК “Промконтроллер” ГК “ТЕКОН”.

Определим число остановов котла по причине отказа элементов системы защиты, выполненной с резервированием модуля БЦП (резервирование без восстановления отказавшего элемента) и без резервирования.

Рассмотрим упрощенную структуру системы защит котла, приведенную на рис. 2. Для простоты расчетов примем, что в определении аварийного состояния котла участвуют шесть датчиков давления, а аварийный останов котла обеспечивается двумя отсечными клапана-

Таблица 1

№	Наименование элемента	Интенсивность отказов λ[1/ч]
1	Датчик давления с токовым выходом	$1*10^{-5}$
2	Модули УСО	$1*10^{-5}$
3	Модуль БЦП	$2*10^{-5}$
4	Силовое реле (коммутатор)	$10*10^{-5}$
5	Электромагнитный клапан	$17*10^{-5}$

ми. В контроллере для обеспечения функции аварийных защит участвуют: один модуль УСО, воспринимающий сигналы с датчиков, и один модуль УСО, выдающий управляющие воздействия через промежуточные коммутаторы (силовые реле) на исполнительные органы, модуль БЦП, выполняющий обработку сигналов в соответствии с записанным программным обеспечением. Для упрощения мы не будем учитывать другие, фактически присутствующие в структуре, элементы системы, также участвующие в выполнении функции (блоки питания, клеммные соединители, линии связи и т.п.).

Исходные данные для расчета надежности приведены в таблице 1. Данные для расчета надежности (интенсивность отказов или среднее время наработки на отказ) обычно берутся из справочников по надежности или из технических данных заводов-изготовителей на конкретное изделие (элемент системы).

Примечание.

1. Показатели надежности для модулей контроллера (УСО и БЦП) взяты из технической документации на контроллеры производства ЗАО ПК “Промконтроллер” ГК “ТЕКОН”.
2. Показатели надежности на датчики, силовое реле, электромагнитный клапан взяты из имеющегося у авторов справочного материала.
3. Поскольку, согласно исходной посылки, в выполнении функции участвуют все элементы, приведенные на рис. 2, то в соответствии с теорией надежности [1, 2, 3] интенсивность отказов элементов определяется сложением интенсивности отказов составляющих элементов.
4. Интенсивность отказов резервированных модулей (модули БЦП) определяется как 1/2 интенсивности отказов нерезервированного модуля, т.е. $\lambda_{резерв} = 1*10^{-5}[1/ч]$.
5. Интенсивность отказов силового реле и электромагнитного клапана приведена для отказа типа “ложного срабатывания”, которое выражается в разрыве цепи прохождения тока через электромагнитный клапан.

Определим оценку вероятности безотказной работы за время t = 720 часов (месяц непрерывной работы). Здесь мы не будем приводить выводы той или иной применяемой формулы. Все основные формулы хорошо описаны в известной литературе [1, 2, 3].

Для системы без резервирования вероятность возникновения отказа типа “ложное срабатывание” за время непрерывной работы t = 720 часов получим:

$$q(t) = 1 - P(t) \approx 1 - 0{,}54 = 0{,}46. \qquad (4.1)$$

Для системы с резервирования модуля БЦП вероятность возникновения отказа типа “ложное срабатывание” за время непрерывной работы t = 720 часов получим:

$$q(t) = 1 - P(t) \approx 1 - 0{,}55 = 0{,}45. \qquad (4.2)$$

Используя статистическое определение вероятности отказа, получим, что резервирование блоков БЦП в представленной системе защит котла даст выигрыш в уменьшении на единицу количества “ложных срабатываний” при 100 работающих на данном объекте (котельной) котлов, оснащенных рассматриваемой системой безопасности. При 10 работающих котлах заказчик не сможет определить изменений (улучшений) в числе “ложных остановов” котла, вызванных отказом элементов системы, включая и элементы контроллера.

Выводы.

1. Для достижения оптимальной величины надежности системы, состоящей из некоторого количества элементов, теория надежности рекомендует применять элементы (узлы) с приблизительно равными показателями надежности. Т.е. если мы имеем в системе элементы с существенно различными показателями надежности, то рекомендуется резервировать, в первую очередь, элементы с низкими показателями.
2. Надежность системы не может быть выше надежности её самого ненадежного элемента (узла).

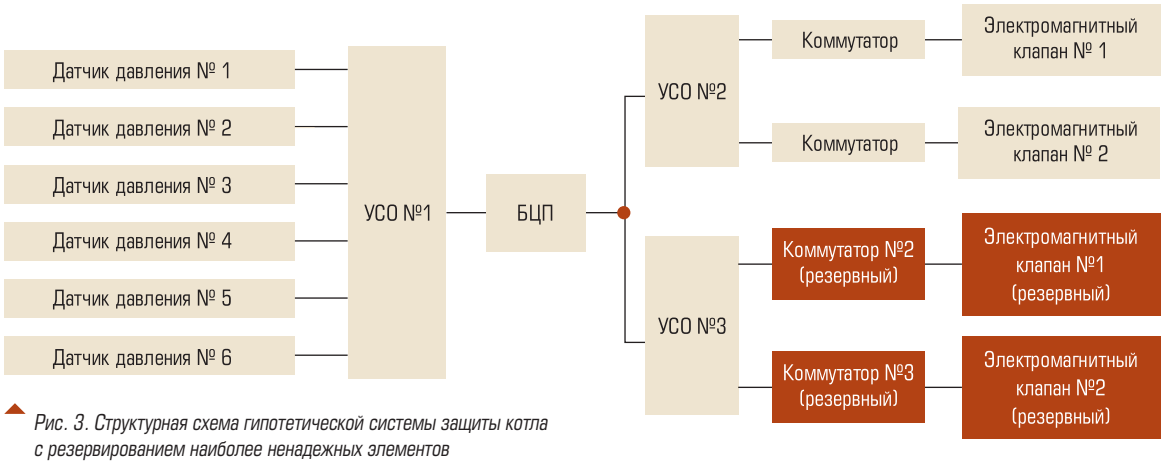

Рис. 3. Структурная схема гипотетической системы защиты котла с резервированием наиболее ненадежных элементов

5. ПОВЫШЕНИЕ НАДЕЖНОСТИ ПУТЕМ РЕЗЕРВИРОВАНИЯ НАИБОЛЕЕ НЕНАДЕЖНЫХ ЭЛЕМЕНТОВ

Для получения оптимальных решений по надежности [1, 2] рекомендуется применять элементы с приблизительно равными значениями интенсивности отказов. Элементы с интенсивностью отказов, значительно превышающей значение для основного количества элементов, необходимо резервировать. По интенсивности отказов, приведенной в таблице 1, мы видим, что основное влияние на уменьшение надежности (основная доля в суммарной интенсивности отказов) оказывают силовые реле и электромагнитные клапаны (т.е. элементы КИПиА).

Определим, как изменится количество “ложных остановов”, вызванных отказами элементов системы защиты, если наиболее ненадежные из них – коммутаторы и электромагнитные клапаны – будут резервированы (дублированы). Первоначально рассмотрим систему с дублированием элементов без восстановления.

Рассчитаем интенсивность отказов для функции и для системы. Расчеты ведем по вышеприведенным формулам (2.1-2.5). Если в системе отказ любого элемента вызывает отказ системы (функции), то для расчета надежности данные элементы представляются как соединенные последовательно, а если элементы резервируются, то данные элементы представляются как соединенные параллельно. При последовательном соединении элементов их интенсивности отказов складываются, а при резервировании (дублировании) интенсивность отказов дублированной пары равна половине интенсивности отказов одного элемента. Расчеты ведем с учетом предположения, что при отказе элемента происходит диагностика отказа – мгновенное отключение отказавшего и включение резервного. Диагностика осуществляется процессорным модулем, а переключение – модулем УСО (№2 и №3). Модуль БЦП контроллера не резервируется. При резервировании внешних элементов рекомендуется сигналы от резервных элементов (датчики или исполнительные элементы) подключать к различным модулям УСО, что повышает функциональную надежность.

Первоначально рассмотрим вариант, когда восстановление отказавших элементов не осуществляется. Структурная схема гипотетической системы защит с резервированием наиболее ненадежных элементов приведена на рис. 3.

Расчеты ведем по формулам (2.1–2.5) из заданного времени (t = 720 часов), для которого определяются вероятности появления отказа элементов системы, которые могут вызвать “ложный” останов котла:

$$q(t = 720)_{\text{функц. резерв}} = 0{,}26, \text{ при } (\lambda_{\Phi} = 36{,}5 * 10^{-5}).$$

При этом вероятность возникновения отказа одного из элементов системы, соответственно:

$$q_{p}(t = 720)_{\text{системы резерв}} = 0{,}86, \text{ при } (\lambda_{\Sigma} = 119 * 10^{-5})$$

$$q_{\text{нр}}(t = 720)_{\text{системы не резерв}} = 0{,}46, \text{ при } (\lambda_{\Sigma_{\text{нр}}} = 64 * 10^{-5}).$$

Используя статистическое определение вероятности возникновения отказа, можем интерпретировать полученные результаты следующим образом. Если на производстве находится в работе 100 систем, то:

- отказ функции резервированной системы, который может повлечь “ложный” останов котла, за 720 часов может произойти 26 раз, что существенно лучше, по сравнению с 46 отказами для нерезервированной системы;
- число вызовов на обслуживание системы и замену отказавшего элемента по причине отказа одного из элементов системы за 720 часов составит:
  – для резервированной системы – 86 раз;
  – для нерезервированной системы – 46 раз.

Таким образом, резервирование наиболее ненадежных элементов приведет к уменьшению количества “ложных” остановов котла по причине отказа одного из элементов системы в 1,77 раза по сравнению с нерезервированной системой.

Приведенные расчеты показывают, что в резервированной системе число отказов в системе (которые требуют обслуживания системы, т.е. замены отказавшего элемента), по сравнению с нерезервированной системой, возрастет в 1,87 раза. Т.е. увеличивая надежность выполнения функции – уменьшая число “ложных” остановов котла, – мы, используя резервирование элементов, повышаем общее число отказов в системе.

Выводы.

1. Надежность функции и надежность системы – это разные понятия, которые в большинстве случаев не тождественны.
2. Надежность функции определяется элементами системы, которые участвуют в выполнении функции, и их структурой (наличием или отсутствием резервирования). Резервирование элементов увеличивает надежность выполнения функции.
3. Надежность системы определяется общим количеством элементов, входящих в систему. Увеличение надежности функции за счет применения резервирования приводит к увеличению интенсивности отказов системы, т.е. к уменьшению её надежности.

6. ВРЕМЯ ВОССТАНОВЛЕНИЯ В СИСТЕМАХ С ДУБЛИРОВАНИЕМ ЭЛЕМЕНТОВ ОКАЗЫВАЕТ СУЩЕСТВЕННОЕ ВЛИЯНИЕ НА НАДЕЖНОСТЬ СИСТЕМЫ

При определении требований к надежности очень часто упускают из вида, что надежность системы определяется не только резервированием элементов системы, но и, в случае применения дублирования, временем, затрачиваемым на ремонт – устранение отказа. При этом далее мы покажем, что, чем меньше время, затрачиваемое на восстановление, тем выше надежность функционала системы.

Надежность системы с резервированием и восстановлением отказавшего элемента

Для определения, как влияет величина временного интервала восстановления на надежность системы рассчитаем, как изменится надежность системы с резервированием элементов, приведенной на рис. 3, для случая с восстановлением отказавшего элемента. Будем считать, и это предположение вполне обосновано, что одновременный отказ двух элементов в резервированной паре невозможен, т.е. имеет крайне низкую вероятность, что позволяет этой вероятностью пренебречь. Для простоты расчетов примем, что диагностика неисправности элементов, отключение отказавшего элемента и подключение вместо отказавшего элемента исправного осуществляется абсолютно надежным элементом. При указанных выше условиях отказ функции системы возможен только при совпадении событий – отказа основного элемента и в течение времени его ремонта отказа дублирующего элемента. Отказ основного или дублирующего элементов, произошедшие по отдельности (не совпадая во времени), не вызывают отказа функции системы.

Каждый элемент резервированной системы с восстановлением отказавшего элемента оценивается двумя показателями: интенсивностью отказов (λ) и интенсивностью восстановления (μ) или средним временем восстановления (Тр). Интенсивность восстановления и среднее время восстановления связаны между собой соотношением 6.1. В рассматриваемом примере резервируются выходные цепочки, выполняющие команды управления: модуль УСО, усилитель (коммутатор) и исполнитель-

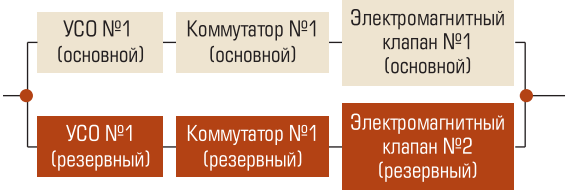

Рис. 4. Структурная схема резервированного узла, для расчета надежности

ный элемент (электромагнитный клапан).

Резервирование с восстановлением предполагает, что после отказа элемента его функции выполняет резервный элемент, и после возникновения отказа в течение времени ($t \le Tp$) осуществляется восстановление отказавшего элемента, т.е. система возвращается в первоначальное состояние.

Определим понятие "узел" как совокупность последовательно соединенных элементов: модуль УСО, усилитель, электромагнитный клапан. Отказ любого элемента, входящего в узел, вызывает отказ узла. Основной и резервирующий узлы составляют резервированный узел. Структурная схема резервированного узла, выдающего управляющее воздействие на останов работы котла (прекращение подачи топлива на котел), приведена на рис. 4.

Теория вероятности [3] определяет, что вероятность совместного появления двух событий равна вероятности появления одного из них, умноженной на условную вероятность появления другого, вычисленную в предположении, что первое событие произошло.

Вероятность отказа резервированного узла при условии, что отказавший элемент восстанавливается за время, не превышающее Тр, определяется по формуле:

$$q_{ру}(t) = q_{осн}(t)*q_{дубл}(Tp), \quad (6.1)$$

где $q_{ру}(t)$ – вероятность отказа резервированного узла; $q_{осн}(t)$ – вероятность отказа основного узла; $q_{дубл}(Tp)$ – вероятность отказа резервирующего узла за время ремонта (замены) отказавшего элемента; Тр – время ремонта (замены) отказавшего элемента.

$$q_{осн}(t) = 1 - P_{осн}(t) = (1 - e^{-\lambda*t}) \quad (6.2)$$
$$q_{дубл}(t) = 1 - P_{дубл}(Tp) = (1 - e^{-\lambda*Tp}) \quad (6.3)$$
$$\lambda = \lambda усо + \lambda к + \lambda эк, \quad (6.4)$$

где λ – интенсивность отказов основного узла, состоящего из модуля УСО, коммутатора, электромагнитного клапана; $\lambda усо$ – интенсивность отказов модуля УСО; $\lambda к$ – интенсивность отказов коммутатора; $\lambda эк$ – интенсивность отказов электромагнитного клапана.

Вероятность безотказной работы резервированного узла определится по формуле:

$$P_{ру}(t) = 1 - q_{ру}(t) = 1 - q_{осн}(t)*q_{дубл}(Tp) = 1 - (1 - e^{-\lambda*t})*(1 - e^{-\lambda*Tp}). \quad (6.5)$$

С учетом того, что при выполнении условия $\lambda*t << 1$, показательную функцию $e^{-\lambda*t}$ можно представить в упрощенном виде:

$$e^{-\lambda*t} = 1 - \lambda*t, \quad (6.6)$$

произведя подстановку, получим:

$$P_{ру}(t) = 1 - (\lambda^2*Tp)*t = 1 - \lambda_{ру}*t. \quad (6.7)$$

Можно ввести обозначение:

$$\lambda_{ру} = (\lambda^2*Tp), \quad (6.8)$$

где $\lambda_{ру} = (\lambda^2*Tp)$ – это интенсивность отказов резервированного узла с временем восстановления отказавшего элемента равным Тр.

Из формулы 6.7 видно, что интенсивность отказов резервированного элемента прямо пропорциональна времени восстановления (ремонта). Определим время восстановления, равным 1 часу (Тр = 1,0 час.) как время, установленное регламентом на восстановление отказавшего элемента. Подставив данные из таблицы и с учетом формул (2.1–2.6) и (6.1–6.8) получим, что интенсивность отказа резервированного узла:

$$\lambda_{ру} = (\lambda^2*Tp) = 0{,}008*10^{-5}[1/час]. \quad (6.9)$$

Вероятность безотказной работы нерезервированного узла при времени непрерывной работы, равном 720 часов, будет равна P(720) = 0,8.

Вероятность безотказной работы резервированного узла без восстановления отказавшего элемента при времени непрерывной работы, равном 720 часов, будет равна $P`_{ру}(720) = 0{,}9$.

Вероятность безотказной работы резервированного узла со временем восстановления не более 1 часа, при времени непрерывной работы, равном 720 часов:

$$P_{ру}(t) = 1 - (\lambda^2*Tp)*t = 1 - (784*10^{-10}*1)*720 = 0{,}99994.$$

Можно самостоятельно интерпретировать полученные результаты, используя статистическое представление вероятности безотказной работы.

Выводы.

1. В случае применения дублирования элементов в системе можно существенно повысить надежность системы, если проводить восстановление отказавшего элемента.

Сокращение времени восстановления отказавших элементов в системах с резервированием является мощным средством повышения надежности.

2. Надежность функции в системе с резервированием существенно зависит от установленного времени восстановления (замены) отказавшего элемента.
3. Для обеспечения быстрого восстановления (ремонта) имеют:
   - наличие средств диагностики, позволяющие определить факт отказа и индицировать отказавший элемент;
   - возможность "горячей" замены отказавших элементов, т.е. замены отказавшего элемента без остановки контроллера и технологического процесса;
   - наличие и доступность ЗИП;
   - организацию службы технического обслуживания и ремонта, регламентацию времени на восстановление отказавшего элемента.

7. ОБОСНОВАННОСТЬ ТРЕБОВАНИЙ НА РЕЗЕРВИРОВАНИЕ ОТДЕЛЬНЫХ ЭЛЕМЕНТОВ СИСТЕМЫ С КРАТНОСТЬЮ ТРИ

Формирование требований к надежности исторически были вызваны потребностью защиты оборудования от аварийных ситуаций. Система защит должна была не пропустить возникновение аварийной ситуации и при её возникновении выработать управляющее воздействие, обеспечивающее защиту технологического оборудования и предотвращение развития аварийной ситуации.

В связи с высокой стоимостью датчиков с аналоговым выходом и их невысокой надежностью, по сравнению с датчиками с дискретным выходом, в качестве датчиков, определяющих аварийное состояние процесса, применялись датчики с дискретным выходным сигналом. Так как определить достоверность сигнала, вырабатываемого датчиком с дискретным выходом невозможно, то для достоверности и надежности определения аварийного состояния применялось дублирование с организацией определения аварийной ситуации – один из двух. Однако возникающие в процессе эксплуатации ложные сигналы от датчиков аварийного состояния вызывали нежелательные ложные остановы защищаемого оборудования. Название "ложные" данные сигналы получили потому, что они возникают тогда, когда фактически аварийной ситуации нет.

Развитие производства вызвало появление технологического оборудования большой единичной мощностью. Остановы или перерывы в работе данного оборудования приводили к значительным потерям в выпускаемой продукции. Таким образом, чтобы ликвидировать экономические потери, появилось требование по недопущению ложных остановов технологического оборудования, т.е. автоматическая система, выполняя свои функции по управлению технологическим процессом и функции по защите технологического оборудования от аварийных ситуаций, не должна вызывать ложных (не обусловленных состоянием технологического процесса) остановов технологического оборудования.

Для объектов, где необходимо было исключить ложные остановы технологического оборудования, вызываемые ложными срабатываниями датчиков аварийных ситуаций с дискретным выходным сигналом, стали применять резервирование с кратностью три (троирование) датчиков с организацией определения достоверного сигнала как "два из трех". При этом "неаварийное" состояние процесса определялось нормально замкнутыми контактами (НЗ), что позволяло контролировать обрывы линий связи. Трехкратное резервирование применялось вследствие невозможности диагностировать достоверность сигнала от датчиков с дискретным выходным сигналом. Иногда приходится слышать суждения, что надежность системы с резервированием кратностью три существенно выше надежности систем с дублированием элементов и восстановлением (заменой) отказавших элементов в течение минимально технически возможного времени.

На наш взгляд, применение резервирования с кратностью три целесообразно в случае невозможности выполнения ремонтных работ по замене отказавшего элемента в течение времени, обеспечивающего требуемые параметры надежности выполнения функции. В большинстве практических случаев, если это не беспилотный космический корабль или не объект в далекой тундре, обслуживающий персонал имеет возможность замены отказавшего элемента в течение небольшого промежутка времени, что позволяет обеспечить высокие показатели надежности. Надо иметь в виду, что в большинстве практических случаев применение резервирования с кратностью три

экономически нецелесообразно. Применение резервирования приводит к существенному увеличению количества элементов в системе, что уменьшает надежность системы, увеличивает трудоемкость обслуживания, увеличивает количество ЗИП, т.е. в целом увеличивает стоимость владения системой. Целесообразность применения резервирования с кратностью три должна быть обоснована расчетом вероятности отказа элемента за время, выделяемое (предписанного регламентом) на ремонт.

Сравним вероятности безотказной работы в течение 7920 часов работы (11 месяцев) элементов системы (например, процессорный модуль МФК3000 РО5-02) для варианта с резервированием кратностью три и варианта резервированием с восстановлением в течение 0,5 часа. Интенсивность отказов модуля в соответствии с технической документацией на МФК3000 составляет $\lambda = 2{,}0*10^{-5}$. Узел, содержащий три резервированных модуля БЦП, будет иметь интенсивность отказов $\lambda_{рез} = (2/3)*10^{-5}$. Для случая дублирования БЦП с восстановлением в течение 0,5 часа с учетом рассмотренных в предыдущем примере формул имеем:

$$\lambda_{РВ} = (\lambda_э)^2*Тр,$$

где $\lambda_{РВ}$ – интенсивность отказов дублированного БЦП с восстановлением; $\lambda_э$ – интенсивность отказов одного БЦП; Тр – время восстановления.

Подставив значения для нашего случая, имеем:

$$\lambda_{РВ} = (2*10^{-5})^2*0{,}5 = 2{,}0*10^{-10}[1/час].$$

Подставив данные значения в формулу вероятности безотказной работы, для времени работы 7920 часов, получим:

- при резервировании с кратностью три вероятность безотказной работы за 7920 часов составит P(7920) = 0,95;
- при дублировании с максимальным временем восстановления не более 0,5 часа вероятность безотказной работы за 7920 часов составит P(7920) = 0,999998.

Сравнивая два результата, можно сделать вывод, что применение резервирования с кратностью три менее эффективно по отношению к дублированию с восстановлением отказавшего элемента как с технической, так и с экономической точек зрения.

Выводы.

1. Если ставятся требования по обеспечению надежности, то при применении резервирования всегда надо стремиться обеспечить быстрое восстановление отказавшего элемента. Чем меньше время, выделяемое на замену отказавшего элемента, тем выше надежность.
2. Применение резервирования с кратностью три целесообразно применять в случае физической невозможности выполнить замену отказавшего элемента за время, обеспечивающее требуемые показатели надежности.
3. Для обеспечения требуемых высоких показателей надежности системы необходимо:
   - обеспечить примерно равную интенсивность отказов узлов, составляющих систему путем применения дублирования наиболее ненадежных элементов;
   - уменьшить время (Тр), требуемое на восстановление системы;
   - применить резервирование ко всем элементам системы;
   - и только в случае, когда вышеприведенные варианты не дают приемлемого значения надежности (например, невозможно обеспечить приемлемое значение времени восстановления по причине большой удаленности или труднодоступности), необходимо выдвигать требования к резервированию элементов системы с кратностью три (троированию).
4. Заявленная ЗАО ПК “Промконтроллер” интенсивность отказов модулей УСО контроллеров МФК3000 и МФК1500 составляет $\lambda=10^{-5}$[1/ч] и время восстановления (замены модуля) не более 0,5 ч. Таким образом, вероятность безотказной работы за время ремонта составит 0,99995, т.е. отказ за установленное время ремонта практически исключается.

Прокопьев Александр Михайлович *– главный специалист отдела системных решений,*
Полянский Павел Владимирович *– к.т.н., зам. начальника отдела системных решений*
ЗАО ПК «Промконтроллер»
Телефон +7 (495) 730-41-12. E-mail: info@tecon.ru

Список литературы

1. *Надежность* технических систем. Под редакцией А.И.Ушакова, М.: “Радио и связь”. 1985.
2. *Дружинин Г.В.* Надежность автоматизированных систем. М.: “Энергия”. 1977.
3. *Козлов Б.А., Ушаков И.А.* Справочник по расчету надежности аппаратуры радиоэлектроники и автоматики. М.: “Сов. Радио”. 1975.
4. *ГОСТ 27.002-89.* Надежность в технике. Основные понятия. Термины и определения.
5. *ГОСТ 24.701-86.* Надежность автоматизированных систем управления. Основные положения.
6. *Можаев А.С., Громов В.Н.* Теоретические основы общего логико-вероятностного метода автоматизированного моделирования систем // ВИТУ. - СПб., 1999.