УДК 621.3.019.3

А.В. ФЕДУХИН*

ГРАВИТАЦИОННАЯ АВТОМАТИКА В СИСТЕМАХ ЗАЩИТЫ ОБЪЕКТОВ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

*Институт проблем математических машин и систем НАН Украины, Киев, Украина

Анотація. *Стаття присвячена ревізії рівня безпеки та живучості системи протиаварійної автоматики ГЕС за результатами аварії на Саяно-Шушенській ГЕС. Проведено класифікацію причин аварії, сформульовано поняття гравітаційної автоматики, розглянуті приклади елементів гравітаційної автоматики, розроблені пропозиції щодо підвищення рівня гарантоздатності систем управління, контролю і захисту ГЕС.*
Ключові слова: *відмовобезпека, живучість, гарантоздатність, гравітаційна автоматика.*

Аннотация. *Статья посвящена ревизии уровня безопасности и живучести системы противоаварийной автоматики ГЭС по результатам аварии на Саяно-Шушенской ГЭС. Проведена классификация причин аварии, сформулировано понятие гравитационной автоматики, рассмотрены примеры элементов гравитационной автоматики, разработаны предложения по повышению уровня гарантоспособности систем управления, контроля и защиты ГЭС.*
Ключевые слова: *отказобезопасность, живучесть, гарантоспособность, гравитационная автоматика.*

Abstract. *The article is devoted to audit of the emergency control system security and survivability of HPP on the results of the accident at the Sayano-Shushenskaya HPP. The classification of the causes of the accident was done, the concept of the gravity automation was formulated, the examples of gravity elements of automation were regarded, proposals on improvement of the level of dependability management, control and protection of the HPP were developed.*
Keywords: *failsafe, survivability, dependability, gravity automation.*

1. Введение

Мировая практика широкого применения сложных систем, в том числе и для критических инфраструктур (КИ), показала их уязвимость не только от отказов техники, проектных ошибок в программном обеспечении, действий злоумышленников, но и от внешних и внутренних воздействий, включая ошибки операторов.

Возникновению проблемы уязвимости сложных КИ и компьютерных систем (КС) управления, контроля и защиты способствовали, с одной стороны, бурное развитие современной компьютерной техники и, с другой стороны, отсутствие необходимого комплексного исследования проектов с позиций гарантоспособности. Эта ситуация побудила, например, правительство США к незамедлительным инициативам по проведению всеобъемлющей ревизии сложных КС и выработке рекомендаций для национальной стратегии безопасности критических инфраструктур и обеспечению их непрерывного функционирования. Результатом этой работы было введение президентской директивой PDD-63 от 22.05.1998 г. «Программы гарантирования всесторонней защиты инфраструктур» (Defense – wide Information Assurance Program – DIAP). Эта программа активно поддерживается оборонными ведомствами, ФБР и НАТО. К ней присоединились и страны Северной Америки, Евросоюза, Японии и др.

Аналогичную работу по ревизии уровня безопасности КС КИ необходимо инициировать и в Украине. В нашей стране это особенно актуально, так как установленные сроки эксплуатации объектов КИ (АЭС, ГЭС, ТЭС, горнодобывающих шахт, котлов высокого давления, трубопроводов и т.д.) в большинстве случаев давно истекли.

2. Цель исследований

Целью данных исследований является ревизия безопасности плотинных гидроэлектростанций (ГЭС) с позиций реализации требований по отказоустойчивости и живучести компьютерных систем противоаварийной автоматики (СПА) по результатам аварии на Саяно-Шушенской ГЭС. В работе проведена классификация причин аварии, разработаны рекомендации по повышению уровня гарантоспособности (отказоустойчивости, безопасности и живучести) аналогичных объектов КИ.

3. Авария – взгляд в прошлое

Современные ГЭС представляют собой одни из самых красивых инженерных сооружений, созданных когда-либо человеком (рис. 1).

Рис. 1. Саяно-Шушенская ГЭС – вид плотины со стороны нижнего бьефа

На дальнем плане, внизу, вблизи от поверхности воды видно здание машинного зала (рис. 2) с расположенными в нем гидроагрегатами и системами управления, контроля и защиты.

Рис. 2. Машинный зал Саяно-Шушенской ГЭС – вид изнутри до аварии

В погоне за дешевизной и эстетической красотой таких техногенных объектов (являющихся следствием развития техники и технологий производства) проектировщики создавали и создают в настоящее время плотинные ГЭС с неудовлетворительным уровнем гарантоспособности.

Примечание 1. Рассматривая первую фотографию ГЭС, необходимо отметить, что в случае аварийного перелива плотины или повышения уровня нижнего бьефа вероятность разрушения или подтопления здания машинного зала, со всеми вытекающими из этого катастрофическими последствиями, очень высока.

Следует разобраться в этом вопросе более детально. Крупные техногенные аварии случались в разных странах, независимо от уровня жизни населения и развития техники и технологий. Рассмотрим в качестве примера недавнюю аварию на российской Саяно-Шушенской ГЭС (СШГЭС). Чтобы понять и осмыслить случившееся на СШГЭС утром 17 августа 2009 года, когда была разрушена самая мощная в РФ гидроэлектростанция и погибли 75 человек обслуживающего и ремонтного персонала [1], необходимо поминутно воскресить в памяти события тех лет.

Итак, время, отмеченное в «черном ящике» ГЭС на графике вертикальной вибрации опоры подпятника: 08.13.25 – момент начала аварии гидроагрегата № 2 (ГА-2) СШГЭС. Время 08.15.34 – момент начала развития аварии ГА-2 до масштабов техногенной катастрофы. С этого момента у всех людей, находившихся в машинном зале станции, не осталось никаких шансов на спасение (рис. 3).

Рис. 3. Машинный зал СШГЭС – вид изнутри после аварии на ГА-2

Из интервью Олега Мякишева – дежурного машиниста СШГЭС, очевидца событий:

«Я стоял наверху, услышал какой-то нарастающий шум, потом увидел, как поднимается, дыбится рифлёное покрытие гидроагрегата. Потом видел, как из-под него поднимается ротор. Он вращался. Глаза в это не верили. Он поднялся метра на три. Полетели камни, куски арматуры, мы от них начали уворачиваться… Рифлёнка была где-то под крышей уже, да и саму крышу разнесло… Я прикинул: поднимается вода, 380 кубов в секунду, и – дёру, в сторону десятого агрегата. Я думал, не успею, поднялся выше, остановился, посмотрел вниз – смотрю, как рушится всё, вода прибывает, люди пытаются плыть… Подумал, что затворы надо закрывать срочно, вручную, чтобы остановить воду. Вручную, потому что напряжения-то нет, никакие защиты не сработали…»

Фонтан из шахты разрушил перекрытие машинного зала и поддерживающие его конструкции над тремя агрегатами. Фрагменты перекрытия при разрушении разлетались по всему машинному залу до ГА-5.

Вот как вспоминают эти события другие свидетели аварии [2] – ведущий инженер производственно-технической службы Ильдар Багаутдинов:

«В это время у нас в отделе проходила планерка. Мы услышали сильный грохот, потом погас свет, потом еще один грохот и начался сильный шум. Когда выскочили на крыльцо, то увидели фонтан, который бил со стороны второго гидроагрегата. Поначалу подумали, что порвало водовод (труба, по которой вода доставляется к агрегату) и поняли, что надо бросать затворы (то есть перекрывать воду на верху плотины).

Перекрыть воду, поступающую в машинный зал, можно тремя способами. Во-первых, с помощью ключей из самого машинного зала, но он уже находился под водой. Во-вторых, за счет автоматической системы управления, но ее смыло водой и она не успела сработать. И последний способ – вручную на гребне плотины.

Гидроэнергетические сооружения очень сложные, и здесь нельзя пренебрегать правилами. Конечно, можно было опустить заслонки быстрее, но это могло привести к гидравлическому удару (когда в водоводе на короткое время образуется вакуум) и к еще большим разрушениям внизу. Поэтому пытались затворы опустить в щадящем режиме. Мы добились своего и остановили дальнейшее развитие аварийной ситуации.

Следующей задачей было открыть водосброс (это когда вода вхолостую проходит через тело плотины), чтобы не допустить перелива воды из водохранилища. Не сделай мы этого, затопленными оказались бы населенные пункты ниже по течению Енисея, а также из строя вышла бы еще одна ГЭС – Майнская. Но для этого нужно было найти дизель-генератор, потому что вся станция была обесточена. Его привезли рабочие, которые сейчас строят обводной тоннель. Они первыми приехали на гребень плотины и привезли генераторы и механизмы, чтобы можно было открывать крышки водостоков.

Электропитание запустили к 11 часам (через 2 часа 45 мин.) и сразу же начали поднимать затворы. Стали медленно поднимать все 11 секций. Быстрее нельзя. У нас до этого уже были проблемы с тем, что разбивало водобойный колодец. Появилась определенная методика – затворы открывали попарно, от центра к краю. Чтобы потоки били не в одну точку, а постепенно расширялись и заполняли полностью весь колодец».

Разрушение второго гидроагрегата Саяно-Шушенской ГЭС произошло в момент срыва крышки турбины вследствие излома шпилек крепления. Автоматика на ГЭС в момент аварии вышла из строя и не управляла станцией. При этом ГА-2, с которого началась авария, был модернизирован в 2009 году, на него была поставлена новая система управления, но не были продублированы системы защиты и электропитания на ГЭС [3].

В результате сильнейшего повреждения ГА-2 произошел выброс воды из кратера турбины, что привело к частичному обрушению строительных конструкций на участке от 1-го до 5-го ГА и перекрытия обслуживания машинного зала (отметка 327); были повреждены и местами разрушены несущие колонны здания и расположенное оборудование систем регулирования, управления и защит гидроагрегатов; получили механические повреждения различной степени фазы силовых трансформаторов; были повреждены строительные конструкции трансформаторной площадки в зоне 1-го и 2-го ГА.

В результате попадания воды электрические и механические повреждения различной степени тяжести получили все гидроагрегаты ГЭС. Все общестанционные технологические системы, расположенные на отметке 327 и нижележащих отметках, были затоплены и получили повреждения различной степени тяжести. Произошел выброс турбинного масла (до 50 т.) в реку Енисей. Короткое замыкание в системах управления генераторов привело к полному прекращению работы ГЭС.

Вот так великолепное творение человека обернулось серьезной техногенной катастрофой. Экономический ущерб от аварии на Саяно-Шушенской ГЭС составил:

• потери, связанные с повреждением основных производственных фондов, – 7 млрд руб.;

• стоимость контракта на поставку нового оборудования – 11,7 млрд руб.;

• финансирование работ по восстановлению станции – на 2009 год в объёме 5,1 млрд руб. и на 2010 год в объёме 16,1 млрд руб.;

• материальная помощь семьям погибших выплачена компанией «РусГидро» в размере 1 млн руб. семье каждого погибшего;

• дополнительная материальная помощь семьям погибших из федерального бюджета в размере 1,1 млн руб. семье каждого погибшего;

• единовременные выплаты выжившим, но пострадавшим при аварии, в размере от 50 до 150 тыс. руб. каждому пострадавшему;

• в общей сложности на социальные программы помощи – 185 млн руб.;

• затраты на локализацию и ликвидацию причин аварии – 192, 51 млн руб.;

• затраты МЧС России – 83,2 млн руб.;

• экологический ущерб – 63,134 млн руб.;

• доставка пострадавшему населению бутилированной питьевой воды за счет финансирования Еврокомиссии – 10,5 тыс. евро.

4. Анализ причин аварии

Анализ причин аварии, произошедшей 17 августа 2009 года на СШГЭС, показывает, что это была комплексная системная авария, явившаяся сочетанием технических, организационных, управленческих причин [4].

Технические:

• повышенные вибрации в ГА-2, в том числе при прохождении запрещенной для работы зоны при пуско-остановочных операциях и регулировании нагрузки;

• продолжительная эксплуатация ГА-2 с недопустимо сильной вибрацией;

• недопустимый усталостный износ шпилек крепления фланцевого соединения крышки турбины ГА-2 к статорному кольцу;

• отсутствие на гидроагрегатах защит, адекватных уровню опасности и уникальности СШГЭС;

• отсутствие резервирования собственных нужд в электроэнергии;

• при модернизации ГА-2 в 2009 году не были продублированы системы защиты и электропитания.

Организационные:

• ослабление технологической дисциплины и ответственности;

• отсутствие полноценного контроля технического состояния оборудования;

• выполнение ремонтно-восстановительных работ неквалифицированными организациями без контроля со стороны производителей оборудования;

• отсутствие в нормативной документации положений о систематическом контроле и дефектоскопии наиболее нагруженных и сложных узлов и креплений;

• отсутствие научно-технического сопровождения процесса эксплуатации уникальных гидроэнергетических комплексов.

Управленческие:

• неоправданная передача со стороны Системного оператора функций частотного регулирования с Братской ГЭС на Саяно-Шушенскую ГЭС, приведшая к частому переходу агрегатов (в том числе и ГА-2) через запрещенную зону нагрузки;

• неправильное перераспределение нагрузки между агрегатами при внутристанционной оптимизации из-за отсутствия полноценной системы диагностики оборудования и мониторинга его состояния.

Более детально можно сформулировать технические причины, выявленные в результате расследования аварии, а именно:

1. Отказ датчика частоты вращения. В результате этого произошел разгон ротора гидроагрегата и отказ систем регулирования и управления.

2. Отказ систем управления. В результате короткого замыкания в гидрогенераторе после разрушения крепления крышки турбины и попадания воды на обмотки сигнал на сброс аварийного затвора в связи с отказом систем управления не поступил (рис. 4), именно его во время аварии пришлось закрывать вручную.

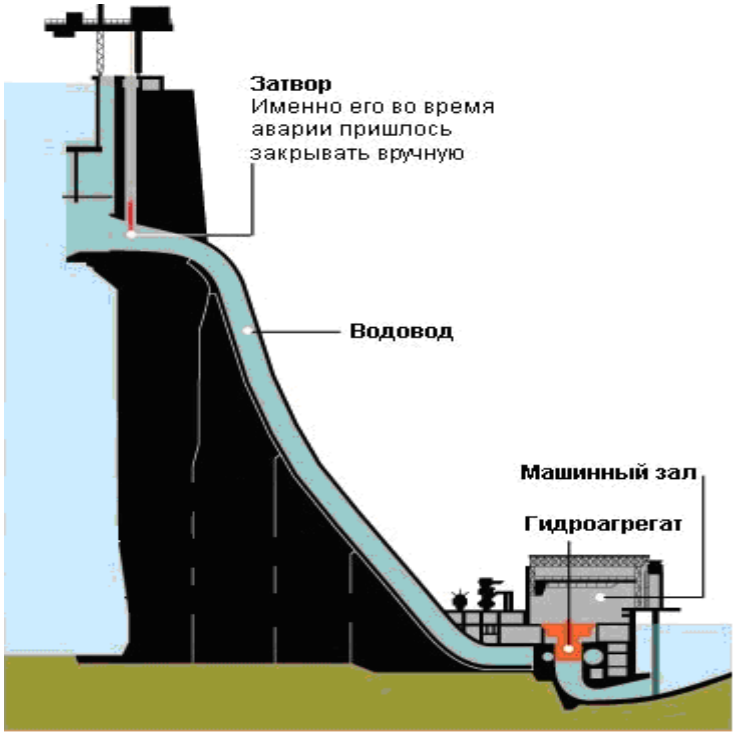

Рис. 4. Расположение аварийного затвора на водопроводящем тракте ГЭС

3. Отсутствие системы непрерывного виброконтроля. Система непрерывного виброконтроля, установленная на ГА-2 в 2009 году (рис. 5), не была введена в эксплуатацию и не учитывалась оперативным персоналом и руководством станции при принятии решений.

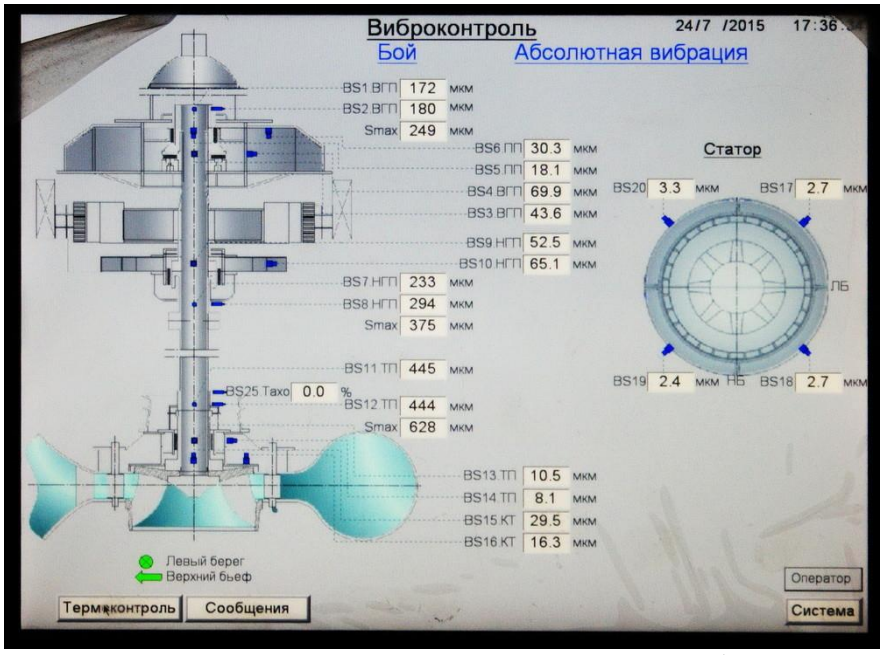

Рис. 5. Пример экрана монитора системы непрерывного виброконтроля ГА

4. Обрыв шпилек крышки турбины. При входе гидроагрегата в зону параметров, не рекомендованную к работе, произошел отрыв ротора в местах крепления крышки турбины (разрушено 80 шпилек вследствие усталостных явлений, на шести шпильках (из 41 обследованной) к моменту аварии отсутствовали гайки, вероятно, вследствие самораскручивания в результате вибрации (их стопорение не было предусмотрено конструкцией турбины).

5. Отказ автоматической системы управления вследствие прекращения энергоснабжения. Автоматические системы управления гидроагрегатов, останавливающие их в случае нештатных ситуаций, могли функционировать лишь при наличии электропитания, но в условиях затопления машинного зала и массового замыкания электрооборудования энергоснабжение самой станции было потеряно очень быстро и автоматика успела остановить только один гидроагрегат – ГА-5.

Анализ причин аварии показал, что проектирование инфраструктуры ГЭС и ее систем управления, контроля и защиты производились без комплексного решения вопросов обеспечения гарантоспособности данного объекта критического использования. Мало того, при восстановлении СШГЭС, на наш взгляд, также не были полностью решены основные вопросы отказоустойчивости, безопасности и живучести, являющиеся базовыми принципами в обеспечении гарантоспособности объектов повышенной опасности, что оставляет достаточно большие риски при дальнейшей эксплуатации данной ГЭС и других станций, аналогичных ей.

Напомним, что включает в себя понятие гарантоспособность. Базовой платформой гарантоспособности систем является отказоустойчивость, а атрибутами - безотказность, готовность, живучесть, обслуживаемость, достоверность, информационная безопасность (целостность, конфиденциальность) и функциональная безопасность.

Гарантоспособная система (ГС) – это система, обладающая полным или частичным (исходя из условий функционирования) набором первичных свойств (атрибутов), составляющих гарантоспособность.

Иными словами, ГС – это отказоустойчивая, высоконадежная, безопасная и живучая система с гарантированно достоверными вычислениями и управляющими воздействиями.

Вопросы отказоустойчивости, безопасности и живучести, являющиеся основополагающими в создании ГС, остаются на сегодняшний день очень актуальными. Только комплексный подход к решению данной проблемы на всех этапах жизненного цикла КСА (от формирования концепции до утилизации) позволит создавать системы с высоким уровнем гарантоспособности.

В результате проведенного анализа еще раз попытаемся сформулировать несколько наиболее важных причин аварии на СШГЭС. С позиций обеспечения гарантоспособности, одной из важных причин аварии явилось отсутствие свойства отказоустойчивости системы электроснабжения станции, а именно, ошибочное решение, заключающееся в организации электроснабжения систем управления, контроля и защиты, связанного с собственными мощностями, вырабатываемыми станцией. Это привело к массовому выходу из строя систем, обеспечивающих безопасность станции, в результате короткого замыкания в общей системе электроснабжения из-за затопления водой электротехнического оборудования одного из ГА.

Другой важной причиной таких серьезных последствий аварии стало недостаточное решение проблемы живучести станции. Грубейшей ошибкой было размещение жизненно важных систем безопасности станции практически в одном уровне с машинным залом (который, кстати, находится ниже минимального уровня нижнего бьефа (УНБ)), при котором любое затопление машинного зала автоматически приводит к одновременному затоплению систем управления, контроля и защиты станции. Расположение всех генераторов станции в одном машинном зале привело к массовой гибели сотрудников станции, рабо-

тающих в данную смену, и выходу из строя большинства генераторов при аварии на одном из них.

Третьей, не менее важной причиной аварии на станции, являлся низкий уровень решения проблемы обслуживаемости агрегатов и систем станции. На станции была плохо организована система планово-предупредительного технического обслуживания, не позволившая вовремя обнаружить усталостные разрушения шпилек крепления ГА-2. Кроме того, на ряде шпилек вовремя не были обнаружены гайки, открутившиеся вследствие повышенной вибрации агрегата. Ошибочным решением было отсутствие средств фиксации гаек от самораскручивания в результате вибрации. Слабость системы технического обслуживания не позволила также вовремя обнаружить отказ датчика частоты вращения ГА-2 в условиях полного отсутствия системы непрерывного виброконтроля агрегатов.

Четвертой важной причиной аварии на станции явился низкий уровень решения проблемы функциональной безопасности станции, а именно, не была решена фундаментальная задача обеспечения внутренней безопасности систем критического использования, заключающаяся в обеспечении гарантированного срабатывания технических средств системы противоаварийной автоматики (СПА) станции (аварийных затворов и заслонок) в условиях аварийного отключения электроэнергии.

Рассмотрим более подробно некоторые, на наш взгляд, наиболее эффективные способы решения описанных выше проблем обеспечения гарантоспособности ГЭС путем внедрения:

- гравитационной автоматики в СПА;
- капсульной структуры технологических помещений;
- декомпозиции электронных систем;
- независимости энергоснабжения.

5. Гравитационная автоматика как средство обеспечения отказобезопасности

5.1. Гравитационный принцип обеспечения гарантированного выключения

Основным видом энергии, используемым при работе элементов, устройств и систем автоматики, является электрическая энергия. При построении гарантоспособных систем автоматики, работающих в критических областях народного хозяйства, включая экологически опасные области, приходится решать сложную задачу обеспечения надежного электроснабжения систем.

Сбои в электроснабжении систем часто приводят к катастрофическим отказам, имеющим тяжелые экономические, экологические и нравственные последствия. Наиболее чувствительными к безотказности электроснабжения являются защитные подсистемы контроля и обеспечения безопасности – СПА, отказ которых, как правило, имеет самые тяжелые последствия.

Одним из стабильных, бесплатных и постоянно присутствующих источников энергии на Земле является сила гравитации, которая является неисчерпаемой и никогда не исчезает. Рассмотрим более подробно вопросы построения СПА на основе специально разработанных элементов, конструкция которых основана на гравитационном принципе обеспечения гарантированного выключения. Системы, использующие данные элементы, назовем системами гравитационной автоматики – системами автоматического управления и контроля, исполнительные элементы которых, ответственные за их функциональную безопасность, используют гравитационный принцип обеспечения гарантированного выключения.

Методы синтеза безопасных схем зависят от свойств элементов схемы. С точки зрения надежности, можно выделить два класса элементов:

• элементы с несимметричными отказами, у которых вероятность возникновения отказа одного вида (0→1 или 1→0) настолько мала, что ею можно пренебречь;

• элементы с симметричными отказами, у которых отказы обоих видов примерно равновероятны и ими нельзя пренебречь (все полупроводниковые элементы, интегральные схемы и электромагнитные реле с пружинным возвратом якоря).

Элементы с несимметричными отказами созданы специально для решения проблемы безопасности. Элементы, у которых вероятность отказов типа 0→1 мала, были названы h_1-надежными [5], а их интенсивность отказов $\lambda_{0\to1}$ очень мала и находится в пределах $10^{-12} – 10^{-14}$1/ч.

5.2. Элементы гравитационной автоматики с несимметричными отказами

5.2.1. Электромагнитные реле высокого уровня гарантии

Рассмотрим реализацию парадигмы «неизбежного срабатывания» на примере специально разработанного электромагнитного реле с гравитационным принципом обеспечения гарантированного выключения, нашедшего широкое применение в системах железнодорожной автоматики, ответственных за безопасность движения поездов [6].

По уровню гарантии выключения нейтральные электромагнитные реле делятся на:

• реле высокого уровня гарантии (ВУГ) с гравитационным принципом обеспечения выключения (h_1-надежные);

• реле низкого уровня гарантии (НУГ) с пружинным и др. принципами обеспечения выключения.

5.2.2. Электромагнитные реле постоянного тока ВУГ типа НМШ

Реле типа НМШ (нейтральное малогабаритное штепсельное) – это электромагнитное реле, не реагирующее на полярность управляющего воздействия (напряжения в обмотке).

Главным элементом электромагнитного реле НМШ (рис. 6) является электрический магнит, посредством которого происходит преобразование электрической энергии в механическое движение. Он состоит из основания (1), обмотки (2) с сердечником (3), ярма (10) и подвижной части, называемой якорем (4), с гравитационным противовесом и антимагнитным бронзовым штифтом. Обмотки нормальнодействующих реле НМШ состоят из двух катушек, намотанных на фенопластовые шпули, а у медленнодействующих реле НМШМ – на медные.

Когда электрический ток проходит по обмотке, якорь притягивается к сердечнику и осуществляет воздействие с помощью тяги на контактные пружины. При этом фронтовой контакт (Ф) замыкается с общим контактом (О), а тыловой контакт (Т) размыкается с ним. Этот процесс называется срабатыванием реле.

Поскольку реле ВУГ используются в системах автоматики, обеспечивающих безопасность, то к ним предъявляются особые эксплуатационно-технические требования [7]:

1. Реле должно обладать такой функциональной надежностью, которая не требует схемного контроля выключения реле (отпускания якоря).

2. При выключении питания отпускание якоря должно происходить под действием собственного веса якоря и связанных с ним подвижных частей (гравитационный принцип отключения), а не под действием упругих пружин.

3. Конструкция реле должна исключать возможность магнитного прилипания якоря к сердечнику после выключения тока в обмотке реле (обеспечивается с помощью антимагнитного бронзового штифта).

4. Положение контактных пружин, принудительно соединенных между собой, должно управляться с помощью тяги, прикрепленной к якорю реле.

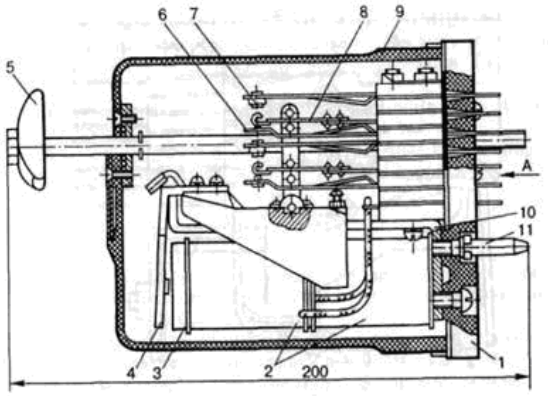

Рис. 6. Схема нейтрального реле ВУГ типа НМШ: 1 – основание, 2 – катушки, 3 – сердечник, 4 – якорь, 5 – ручка, 6 – тыловой контакт (Т), 7 – фронтовой контакт (Ф), 8 – общий контакт (О), 9 – колпак, 10 – ярмо, 11 – направляющий штырь

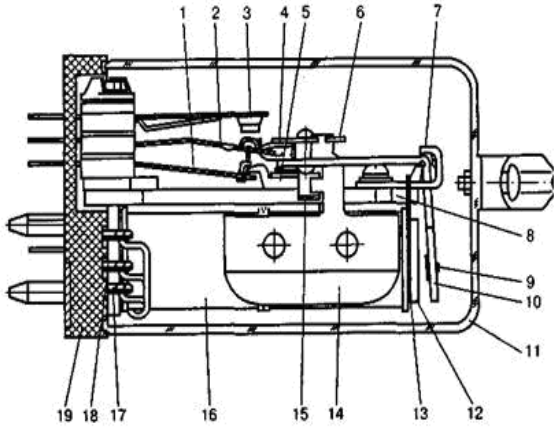

Рис. 7. Схема нейтрального реле ВУГ типа РЭЛ: 1 – тыловой контакт (Т), 2 – общий контакт (О), 3 – фронтовой контакт (Ф), 4 – пластмассовый поводок, 5 – упор, 6 – планка, 7 – скоба, 8 – ярмо, 9 – бронзовая пластина, 10 – якорь, 11 – колпак, 12 – сердечник, 13 – фиксатор, 14 – груз, 15 – ограничитель, 16 – катушка, 17 – вывод, 18 – клемма, 19 – основание

5. Конструкция контактов реле должна обеспечивать:

– надежное размыкание всех тыловых контактов при замыкании хотя бы одного фронтового контакта и размыкание всех фронтовых контактов при замыкании хотя бы одного тылового контакта реле;

– при сваривании тылового контакта с общим контактом в группе должна полностью исключаться возможность замыкания сварившихся контактов с фронтовым контактом из своей группы (мостового соединения фронтового и тылового контактов посредством подвижного общего контакта);

– продукты износа материала фронтового контакта не должны накапливаться на поверхности общего контакта.

6. Фронтовые и общие контакты не должны свариваться в результате электрической искры при любых условиях (разнородные материалы: контакт Ф – графито-серебряная смесь (однородность и качество смеси контролируется рентгеновской установкой), контакты О и Т – серебро).

7. Замкнутые контакты должны выдерживать длительное прохождение тока 3 А без изменения их электрических и механических параметров, а при токах в диапазоне свыше 3 А до 6 А не должно возникать опасных отказов контактов:

– сваривания фронтового контакта с общим контактом:

– выкрашивания графито-серебряной смеси из чашечки фронтового контакта, приводящего к его замыканию с общим контактом.

8. Магнитная система реле должна изготавливаться из материалов, обладающих высокой магнитной проницаемостью и малой коэрцитивной силой (способностью к остаточному намагничиванию), не подверженных заметному старению.

9. Все подверженные коррозии металлические детали должны иметь антикоррозионное покрытие (оцинкованы, никелированы), а неметаллические части должны быть негорючими.

10. Для исключения попадания пыли и влаги конструкция реле должна быть закрыта прочным прозрачным влагозащитным и пломбируемым колпаком, что обеспечивает работоспособность реле в условиях брызг или кратковременного затопления водой.

11. Штепсельные разъемы реле должны исключать возможность ошибочной установки реле в розетку другого типа и возможность его переворачивания с целью принудительного воздействия на якорь реле.

12. Срок службы реле составляет порядка 20 лет и определяется режимом и интенсивностью его работы. Условия эксплуатации: температура окружающего воздуха от – 45°С до + 50°С, влажность до 100% при температуре + 25°С.

5.2.3. Электромагнитные реле постоянного тока ВУГ типа РЭЛ

Реле РЭЛ предназначены для работы в непрерывном режиме в устройствах автоматики и телемеханики, обеспечивающих безопасность. Реле обладает функциональной надежностью, не требующей схемного контроля выключения реле (отпускания якоря). Реле РЭЛ является базовой конструкцией электромагнитных реле IV поколения [8]. Конструкция реле РЭЛ подобна конструкции реле НМШ, однако имеет ряд особенностей, улучшающих ее технические характеристики.

Реле РЭЛ изображено на рис. 7. В отличие от реле НМШ, магнитная система реле РЭЛ – разветвленная, содержит якорь 10, ярмо 8 и два сердечника 12, на каждом из которых размещены по две катушки 16. Реле имеет две независимые обмотки, каждая из которых размещена на двух катушках, расположенных на разных сердечниках. Обмотки нормальных реле РЭЛ намотаны на пластмассовые шпули, а медленнодействующих реле РЭЛМ – на медные.

Вместо одного бронзового антимагнитного штифта у реле НМШ, который подвергается расклепу при интенсивной работе реле, на якоре реле РЭЛ установлена бронзовая пластина 9, устойчивая к расклепу и обеспечивающая зазор не менее 0,15 мм между якорем и обоими сердечниками, которая исключает магнитное залипание якоря.

Возврат якоря в начальное положение обеспечивается действием гравитационного противовеса, состоящего из двух специальных грузов 14. Свободное размещение грузов на якоре обеспечивает повышенную виброустойчивость реле, а также малое время вибрации (дребезг) тыловых контактов при работе.

Каждая группа контактов состоит из фронтового (Ф) 3, подвижного общего (О) 2 и тылового (Т) 1 контактов. Используемые контактирующие материалы контактов у реле РЭЛ такие же, как у реле НМШ.

Реле РЭЛ также закрыто прозрачным герметичным колпаком 11, который пломбируется, что обеспечивает работоспособность реле в условиях брызг или кратковременного затопления водой. Конструкция реле исключает ошибочную установку одного типа реле вместо другого.

Установленный ресурс реле не менее $1{,}5 \cdot 10^6$ циклов включения-выключения для нормальных реле. Условия эксплуатации: температура окружающего воздуха от - 45°С до + 50°С, влажность до 100% при температуре + 25°С.

5.2.4. Электромагнитные реле переменного тока ВУГ типа АР

Аварийные реле переменного тока типа АР (АРП, АРУ) применяются в специальных устройствах автоматики, обеспечивающих безопасность (рис. 8). Реле служат для переключения электрических цепей на резервное питание при аварии в сети основного питания. Реле обладает функциональной надежностью, не требующей схемного контроля выключения реле (отпускания якоря).

Рис. 8. Схема аварийного реле ВУГ типа АР

Аварийные реле типа АР (АРП, АРУ) являются электромагнитными механизмами с расщепленными полюсами и утяжеленными якорями (с гравитационным принципом обеспечения выключения) [9].

При прохождении переменного тока через катушку якорь реле притягивается к сердечнику и при помощи установленных на нем подвижных контактов включает замыкающие контакты. Если в катушках отсутствует ток, якорь под действием гравитации опускается, и подвижные контакты замыкаются с размыкающими контактами.

Основными частями реле являются электромагнитная и контактная системы, укрепленные на пластмассовой плате. Электромагнитная система состоит из якоря, П-образного сердечника и катушки. Сердечник набирается из П-образных пластин, соединенных заклепками. В полюс сердечника вложено два короткозамкнутых медных витка, обхватывающих часть сечения сердечника. На сердечник установлена катушка, закрепляемая направляющей скобой.

Якорь реле состоит из трех секций, соединенных между собой. Средняя секция выступает над боковыми. Сердечник реле укреплен на плате двумя стойками. Его можно перемещать в пазах стоек и этим регулировать необходимый зазор между ним и якорем. Якорь свободно вращается на оси, укрепленной в правой и левой стойках. С нижней стороны к якорю двумя винтами привернута планка из пластмассы, на которой установлены две подвижные контактные пружины.

Контактная система реле АР, АРП состоит из двух контактных групп тройников, а каждый из них – из неподвижного замыкающего (Ф), неподвижного размыкающего (Т) и подвижного общего (О) контактов. Замыкающие контакты представляют собой жесткие стойки с наклепками из серебра. Размыкающие контакты изготовляются в виде стоек, к которым прикреплены плоские пружины с серебряными контактами. Подвижные контактные пружины состоят из плоской пружины с серебряным контактом цилиндрической формы.

Механизм реле закрывается герметичным стеклянным или металлическим остекленным кожухом, опломбированным заводской печатью, что обеспечивает работоспособность реле в условиях брызг или кратковременного затопления водой (на низких напряжениях питания).

Примечание 2. Малогабаритные штепсельные аварийные реле переменного тока ВУГ типов АШ2, АПШ, АСШ2 (ОМШ2, АОШ2, ОМШМ1) имеют конструкцию, аналогичную конструкции реле ВУГ типов НМШ и РЭЛ с гравитационными противовесами.

5.2.5. Гидротехнические заслонки ВУГ

Заслонки аварийного закрытия (ЗАЗ) с управляемым запиранием фирмы ADAMS обеспечивают полную надежность систем напорных трубопроводов (ремонтных, аварийных, основных, предтурбинных и др. затворов) гидроэлектростанций [10] (рис. 7). ЗАЗ обладают функциональной надежностью, не требующей схемного контроля выключения заслонки (перехода диска заслонки в закрытое положение).

Арматура GZA может использоваться в качестве заслонки аварийного запирания на входе турбины для защиты турбины или же в качестве обратной заслонки для защиты насоса. Арматура приводится в действие с помощью гравитационного противовеса (закрывающего груза) и гидравлического сервопривода (рис. 9). Эта защищенная от неправильного использования система надежна в критических ситуациях (ВУГ) даже при полном

отключении электропитания. Сервопривод открывает диск заслонки и действует в качестве мощного гидравлического демпфера во время закрытия. Для предотвращения гидроудара внутри напорной трубопроводной системы могут поставляться регулируемые многоступенчатые демпфирующие устройства.

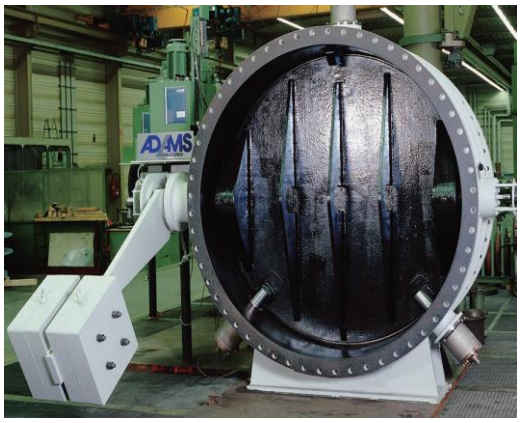

Рис. 9. Заслонки аварийного закрытия ВУГ с управляемым запиранием

Регулируемая заслонка аварийного закрытия с функцией запорной и обратной заслонки имеет:

- диск с хорошими гидродинамическими параметрами;
- двойной эксцентрический вал;
- двойное управление: расположенный снаружи гравитационный противовес (закрывающий груз) и гидравлический сервопривод;
- высокий уровень гарантирования аварийного закрытия;
- электронную систему управления;
- детектор превышения скорости закрытия;
- измерительную диафрагму;
- устройство блокировки диска;
- номинальные диаметры: от 500 мм до 4000 мм;
- широкий температурный диапазон: от – 20^{o}C до + 150^{o}C.

5.3. Отказобезопасность как синтез отказоустойчивости и функциональной безопасности

Наиболее важным свойством гарантоспособных систем противоаварийной автоматики (ГСПА) является свойство отказоустойчивости. Без этого свойства невозможно создать систему с высоким уровнем гарантоспособности. Отказоустойчивость напрямую или косвенно влияет на такие атрибуты, как безотказность, готовность, живучесть и функциональная безопасность. Кроме того, отказоустойчивость, основанная, как известно, на структурной избыточности и методах многоверсийного проектирования, определяет уровень гарантоспособности вычислений, выполняемых программными средствами ГСПА.

Отказоустойчивость ГСПА – дорогое удовольствие, которое может себе позволить не каждый заказчик.

Примечание 3. Например, истребитель Миг-35 поколения 4^{++} имеет 3-канальную электронную систему управления и контроля с 4-кратным резервированием каждого канала. Стоимость Миг-35 составляет порядка $45 млн.

В большинстве случаев применения ГСПА экономически обоснованным является замена полной отказоустойчивости на частичную отказоустойчивость, названную нами отказобезопасностью [11].

Использование подхода, при котором стратегия полной отказоустойчивости заменяется стратегией отказобезопасности с использованием h_1-надежных элементов гравитационной автоматики, позволяет строить экономически эффективные ГСПА с меньшими техническими затратами.

Особенностью стратегии отказобезопасности является то, что она допускает наличие отказов системы, но только таких, при которых последняя переходит в защитное безопасное состояние и полностью исключает появление таких отказов, при которых система переходит в опасное состояние, чреватое катастрофическими последствиями. Алгоритм работы ГСПА в рамках данной стратегии должен исключать опасные ситуации не только при исправном, но и при неисправном состоянии самой системы. Внутренние отказы системы не должны приводить к опасным искажениям алгоритма ее работы.

Для рассмотрения данного направления в проектировании ГСПА введем следующие понятия и определения.

Защитное состояние (Protective State) – неработоспособное состояние системы, при котором значения всех параметров, характеризующих способность выполнять заданные функции по обеспечению безопасности, соответствуют требованиям нормативно-технической и (или) конструкторской документации (НТД, КД).

Опасное состояние (Hazardous State) – неработоспособное состояние системы, при котором значение хотя бы одного параметра, характеризующего способность выполнять заданные функции по обеспечению безопасности, не соответствует требованиям НТД и (или) КД.

Таким образом, понятие безопасность ГСПА можно уточнить как свойство системы непрерывно сохранять исправное, работоспособное или защитное состояние в течение некоторого времени или наработки.

Защитный отказ (Protective Failure) – событие, заключающееся в нарушении работоспособного состояния системы при сохранении защитного состояния.

Опасный отказ (Hazardous Failure) – событие, заключающееся в нарушении работоспособного и защитного состояний системы.

При оценке безопасности в работе [12] исходят из понятия безопасного состояния, которое может принять система или ее компонент. В этом состоянии исключена опасность со стороны системы. В работе [13] безопасность технического устройства рассматривается как его свойство находиться в штатном или нештатном неопасном состоянии.

Штатное состояние (Staffing Condition) – работоспособное состояние, при котором технологический процесс развивается в соответствии с заданным алгоритмом, определяющим адекватную реакцию системы управления на внешние факторы.

Безопасное состояние (Safe state) – состояние некоторой системы, в котором при определенных допущениях и заданных условиях отсутствует угроза для жизни людей, экономики и окружающей среды.

Конструктивность этого подхода состоит в том, что он дает способ решения основного вопроса, который возникает при анализе и синтезе безопасных систем. Для этого сформулируем понятие – критерий опасного отказа.

Критерий опасного отказа (Hazardous Failure Criterion) – признак или совокупность признаков опасного состояния системы, установленные в НТД и (или) КД [14].

Внутренняя безопасность (Internal Security) – свойство системы сохранять исправное, работоспособное и защитное состояния.

На основании вышеизложенного сформулируем вводимый нами новый термин отказобезопасность [11].

Отказобезопасность (Failsafe) – свойство технической системы при отказе ее некоторых составных частей переходить в режим работы, не представляющий опасности для людей, окружающей среды или материальных ценностей.

Примечание 4. Если бы СПА СШГЭС разрабатывались с учетом комплексных требований по гарантоспособности, то использование элементов гравитационной автоматики в наиболее ответственных узлах, обеспечивающих безопасность и живучесть станции, скорее всего, позволило бы в первые секунды возникновения аварии осуществить сброс аварийных затворов даже при условии внезапного исчезновения электропитания систем управления, контроля и защиты.

6. Заключение

В результате ревизии уровня безопасности СПА по результатам аварии на СШГЭС были сформулированы следующие предложения по повышению безопасности ГЭС:

– использование базовых принципов инжиниринга сложных КИ гидроэнергетического назначения и методов оценки надежности, безопасности и живучести ее элементов с учетом безопасных проектных решений инфраструктуры, безопасных и независимых систем управления, контроля и защиты.

– построение инфраструктуры и систем ГЭС с учетом требований по гарантоспособности к системам КИ;

– построение СПА на принципах гравитационной автоматики;

– внедрение новых систем управления и диагностики гидроагрегатов;

– внедрение методов предупредительной профилактики управляемых объектов и устройств СПА;

– внедрение мероприятий по сокращению времени принятия решений в аварийных ситуациях;

– применение новых методов обоснования продления срока службы гидроэнергетического оборудования.

В следующих публикациях по данной теме будут рассмотрены вопросы проектирования отказобезопасных СПА с использованием элементов гравитационной автоматики, а также методы повышения живучести систем управления, контроля и защиты ГЭС путем использования капсульной структуры технологических помещений, декомпозиции электронного оборудования и построения отказоустойчивого энергоснабжения.

СПИСОК ЛИТЕРАТУРЫ

1. Саяно-Шушенская ГЭС, 9 августа. Как это было [Электронный ресурс]. – Режим доступа: http://www.proatom.ru/modules.php?file=article&name=News&sid=5516.

2. Саяно-Шушенскую ГЭС спас инженер [Электронный ресурс]. – Режим доступа: http://www.krsk.kp.ru/daily/24354.4/541385/.

3. Структура полного ущерба от аварий на техническом объекте на примере катастрофы Саяно-Шушенской ГЭС [Электронный ресурс]. – Режим доступа: http://www.refbzd.ru/viewreferat-2570-1.html.

4. Авария на Саяно-Шушенской ГЭС [Электронный ресурс]. – Режим доступа: http://900igr.net/prezentatsii/obg/Avarii/006-Na-skopost-pasppostpanenija-i-vysotu-volny-ppopyva-okazyvaet.html.

5. Методы построения безопасных микроэлектронных систем железнодорожной автоматики / В.В. Сапожников, Вл.В. Сапожников, Х.А. Христов [и др.]; под ред. Вл.В. Сапожникова. – М.: Транспорт, 1995. – 272 с.

6. Теоретические основы железнодорожной автоматики и телемеханики / А.С. Переборов, А.М. Брылеев, А.В. Смирнова [и др.]. – М.: Транспорт, 1984. – 384 с.

7. Эксплуатационно-технические требования к реле [Электронный ресурс]. – Режим доступа http://chiplist.ru/article/jekspluatacionno-tehnicheskie_trebovanija_k_rele/.

8. Реле электромагнитные РЭЛ IV поколения [Электронный ресурс]. – Режим доступа http://scbist.com/spravochnik/rel1.htm.

9. Реле релейной защиты и противоаварийной автоматики [Электронный ресурс]. – Режим доступа: http://museumrza.ru/jeksponaty/a-83.html.
10. Заслонки аварийного закрытия с управляемым запиранием фирмы ADAMS [Электронный ресурс]. – Режим доступа: http://ites.com.ua/produkciya/zaporno-reguliruyushchaya-armatura/adams-1/kombinirovannye-obratnye-i-zapornye-zaslonki/gza.
11. Федухин А.В. Стратегия отказобезопасности как альтернатива полной отказоустойчивости при проектировании гарантоспособных компьютерных систем. Ч. 1 / А.В. Федухин, Ар.А. Муха // Молодий вчений. – 2016. – № 8 (35). – С. 169 – 173.
12. Graband M. Sichereits philosophie und Prufung / M. Graband, H. Gunther // Signal und Draht. – 1988. – N 9. – P. 199 – 204.
13. Лисенков В.М. Безопасность ответственных технологических процессов и технических средств на транспорте / В.М. Лисенков // Автоматика, телемеханика и связь. – 1992. – № 1. – С. 8 – 11.
14. Христов Х.А. Електронизация на осигурителната техника / Христов Х.А. – София: Техника, 1984. – 355 с.

Стаття надійшла до редакції 13.02.2017