Раздел 3. БЕЗОПАСНОСТЬ

УДК: 621.396:519.853+504.75

С. М. Аполлонский
ОАО «Ленгипротранс»

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ В ЭЛЕКТРОЭНЕРГЕТИЧЕСКОЙ ЖЕЛЕЗНОДОРОЖНОЙ СИСТЕМЕ

Дата поступления 19.06.2015
Решение о публикации 03.07.2015
Дата публикации 28.03.2016

Аннотация: Рассмотрены вопросы функциональной безопасности и нормативно-технического регулирования в области электромагнитной совместимости технических средств в электроэнергетической железнодорожной системе.

Ключевые слова: электромагнитное поле, электромагнитная совместимость электрооборудования, электромагнитная среда, электромагнитная обстановка, электромагнитная безопасность технических средств, функциональная безопасность.

Stanislav M. Apollonskiy
Open Joint Stock Company “LENGIPROTRANS”
FUNCTIONAL SAFETY ELECTRIFIED RAILWAYS

Abstract: The study of functional safety includes identification of specific hazards that may cause serious consequences (e.g., human sacrifices), and establishing for each of them maximum frequency of occurrence. Reveals equipment, failure of which may contribute to the occurrence of such situations. Such equipment is usually referred to as "security-related". Examples include process of control systems, process shutdown systems, equipment alarm systems, centralization and blocking on the railway, controls the movement of the vehicle, medical equipment, etc. In other words, any equipment (software or not), failure of which may affect the occurrence of an emergency, should be regarded as "security-related".

It should be noted that at present the world's leading corporations seek not just to provide EMC electrical systems that they produce, and make them functional safety.

Functional safety is called security, which is associated with inadvertently cause failure in the performance of certain functions of the system. The reasons for failure may be defective programs, data, hardware, environmental effects and unintentionally incorrect of staff actions.

Functional safety should be distinguished from the information security (generally deliberate action on the system); from electrical safety (protection of people from electrical shock) and from the explosion and fire (to prevent ignition of flammable gases and dust).

Functional safety is also characterized by very close to the concept of reliability in that it takes into account not only the frequency of failures of the system but also the likelihood of a dangerous situation during a failure. The term "functional" with respect to the safety means automation security, which is dependent on the correct functioning of the system, i.e. the correct implementation of the system of its functions. In contrast, describes a failure rate of reliability regardless of the destination system and consequences caused by failures. However, reliability is used in the quantitative description of functional safety.

The issues of functional safety and regulatory technical regulation in the field of electromagnetic compatibility technical equipment in electrified railways are considered.

Keywords: electromagnetic field, electromagnetic compatibility of electrical equipment, the electromagnetic environment, electromagnetic safety of technical equipment, functional safety.

1. Введение

Изучение функциональной безопасности включает в себя выявление таких специфических опасных ситуаций, которые могут повлечь за собой серьезные последствия (например, человеческие жертвы), и установление для каждой из них максимально допустимой частоты возникновения. Выявляется оборудование, отказ которого может внести вклад в возникновение подобных ситуаций. Такое оборудование обычно называют «связанным с безопасностью». Примерами могут служить системы управления производственными процессами, системы останова технологического процесса, оборудование систем сигнализации, централизации и блокировки (СЦБ) на железной дороге, средства управления движением автомобиля, медицинское оборудование и т.д. Иными словами, любое оборудование (с программным обеспечением или без него), отказ которого может повлиять на возникновение аварийной ситуации, следует считать «связанным с безопасностью».

Следует отметить, что в настоящее время ведущие мировые концерны стремятся не просто обеспечить ЭМС электротехнических комплексов, которые они производят, а сделать их функционально безопасными.

Функциональной безопасностью называют безопасность, которая связана с непреднамеренно вызванными отказами в выполнении отдельных функций системы [1]. Причинами отказов могут быть дефекты программ, данных, аппаратуры, влияние внешней среды и непреднамеренно неправильные действия обслуживающего персонала.

Функциональную безопасность следует отличать от информационной безопасности (в основном, умышленное воздействие на

систему); от электробезопасности (защита человека от поражения электрическим током) и от взрывопожаробезопасности (предотвращение воспламенения горючих газов и пыли).

Функциональная безопасность отличается также от очень близкого понятия надежности тем, что она учитывает не только частоту отказов системы, но и вероятность возникновения опасной ситуации во время отказа. Термин "*функциональная*" применительно к безопасности систем автоматизации означает безопасность, которая зависит от корректного функционирования системы, т.е. от правильного выполнения системой своих *функций.* В отличие от этого, надежность описывает частоту отказов независимо от назначения системы и тяжести последствий, вызванных отказами. Тем не менее, показатели надежности используются при количественном описании функциональной безопасности.

В представленном докладе рассмотрены вопросы функциональной безопасности и нормативно-технического регулирования в области ЭМС технических средств в ЭЭЖС.

2. Преднамеренные электромагнитные воздействия в ЭЭЖС

Отличие такого рода воздействий от коммутационных помех или наводок, вызванных протеканием тока молнии, заключается в том, что при мощности, соизмеримой с мощностью разряда молнии, эти воздействия могут находиться так же близко к чувствительной аппаратуре, как и источники относительно слабых коммутационных помех.

Основными каналами преднамеренного воздействия на электронную аппаратуру являются сети электропитания всех классов напряжения, контрольные кабели и проводные линии связи, эфир. Поскольку микропроцессорные устройства релейной защиты (МУРЗ) в ЭЭЖС связаны и с внешней сетью электропитания, и с разветвленной сетью контрольных кабелей, и с проводами-антеннами ЛЭП (через трансформаторы напряжения и тока), и с компьютерной сетью, то оказываемое на них деструктивное воздействие может быть очень сильным и одновременно скрытным. Существенно повышает скрытность электромагнитного воздействия то обстоятельство, что анализ повреждений в уничтоженном оборудовании не позволяет однозначно идентифицировать причину возникновения повреждения, так как причиной одних и тех же повреждений может быть силовое деструктивное воздействие как преднамеренное (нападение), так и непреднамеренное (например, индукция от молнии). Это обстоятельство позволяет злоумышленникам успешно использовать эту технологию неоднократно.

Микроволновые источники излучения высокой мощности, работающие в сантиметровом и миллиметровом диапазонах, имеют дополнительный механизм проникновения энергии в оборудование даже через небольшие отверстия, вырезы, окна и щели в металлических корпусах, через плохо экранированные интерфейсы. Любое отверстие, ведущее внутрь оборудования, ведет себя как щель в микроволновой полости, позволяя микроволновой радиации формировать пространственную стоячую волну внутри оборудования [2]. Компоненты, расположенные в противоположных узлах стоячей волны, будут подвергаться воздействию электромагнитных полей (ЭМП) и перенапряжений. Особо чувствительны к воздействиям такого рода элементы памяти и современные микропроцессоры с очень высокой степенью интеграции внутренних компонентов. Отсюда становится понятным, что защититься от всех этих «напастей» не так-то просто. И даже такие известные помехоустойчивые технологии, как оптоволоконные, оказываются подверженными, как это не покажется странным, воздействию мощных ЭМ импульсов. Во-первых, оптоволоконные линии имеют концевые устройства, выполненные на микроэлектронных компонентах и даже на микропроцессорах, которые предназначены для преобразования электрического сигнала в световой сигнал и обратно. Во-вторых, известно, что вектор поляризации света в оптическом волокне может изменяться под действием внешнего магнитного поля. Это приводит к тому, что сигналы систем релейной защиты и связи, передаваемые по оптическому волокну, встроенному в провода высоковольтной ЛЭП (весьма распространенная сегодня технология), будут подвергаться искажениям при протекании по этим проводам больших импульсных токов, создающих импульсные магнитные поля. Уже сегодня фиксируются сбои в работе этих систем при растекании по проводам ЛЭП токов молнии.

Очевидно, что не возможно полностью защитить электронное оборудование современных СЦБ в ЭЭЖС от естественных и, особенно, от преднамеренных электромагнитных воздействий. Однако существующие сегодня способы защиты (специальные шкафы, электропроводные прокладки и смазки, фильтры и т. п.) могут существенно ослабить влияние внешних ЭМП и излучений в широком спектре частот на высокочувствительные устройства.

Понятно, что использование специальных технологий для защиты микропроцессорных устройств приводит к дополнительному удорожанию релейной защиты. Но с этим приходится мириться. Если этого не сделать сейчас, то может наступить момент, когда делать это будет уже поздно, ибо зависимость нашей цивилизации от электроники, компьютеров,

микропроцессоров стала столь значительной, что беспечность в сфере защиты этих систем от преднамеренного воздействия на них направленного электромагнитного излучения может обернуться непредсказуемыми последствиями.

Существующая в электроэнергетике тенденция все расширяющегося применения микропроцессорных устройств релейной защиты, непосредственно управляющих энергетическим оборудованием - с одной стороны, и тенденция увеличения плотности элементов в микрочипах (сопровождающаяся снижением их устойчивости к внешним электромагнитным воздействиям) - с другой, на фоне прогресса в области создания средств дистанционного деструктивного воздействия создают весьма опасный прецедент [3].

3. Проблемы электромагнитных воздействий на микропроцессорные устройства релейной защиты

Проблема ЭМС электронной аппаратуры возникла вместе с самой этой аппаратурой, поскольку одни ее узлы функционально построены таким образом, что являются приемниками электромагнитного излучения, тогда как другие - источниками излучения. Проблемы возникали как из-за взаимного влияния одних узлов на другие внутри аппаратуры, так и при воздействии на электронную аппаратуру внешних излучений различного происхождения. Десятилетиями проблемы ЭМС были прерогативой специалистов в области электроники, радиотехники и связи. В последние десятилетия эта проблема стала весьма актуальной и в электроэнергетике. Конечно, довольно значительные ЭМП на объектах электроэнергетики существовали всегда. Однако применявшиеся десятилетиями устройства автоматики, управления и релейной защиты электромеханического типа были мало подвержены этим полям, и никаких особых проблем с ЭМС не возникало. Последние два десятилетия характеризуются интенсивным переходом от электромеханических к микропроцессорным устройствам релейной защиты (МУРЗ) в электроэнергетике. Причем этот переход осуществляется не только по мере строительства новых подстанций и электростанций, но и путем замены старых электромеханических реле защиты на подстанциях, построенных еще в те времена, когда никто даже не предполагал использование в них микропроцессорной техники. Суперсовременные МУРЗ оказались весьма чувствительны к электромагнитным помехам, поступающим из окружающей среды, по цепям оперативного тока, цепям напряжения и от трансформаторов тока. Отмечались случаи ложного срабатывания МУРЗ даже от мобильного

телефона [4]. В качестве других примеров можно привести случаи ложного срабатывания микропроцессорных устройств на действующих объектах «Мосэнерго» - Очаковской и Зубовской подстанциях. Алгоритм работы защит нарушался из-за молнии, работающего поблизости экскаватора, электросварки и некоторых других помех. Во время ввода в действие Липецкой подстанции, руководство которой потратило около полутора миллионов долларов на приобретение МУРЗ, проблемы с микропроцессорными устройствами полгода не позволяли запустить этот энергообъект. В итоге подстанцию запустили, используя комплект традиционных защит [5].

На практике приходилось сталкиваться со случаями, когда короткие замыкания по стороне 110 кВ вызывали ложную работу защит на стороне 330 кВ, а помехи при коммутациях по одному классу напряжения проникали (через общие цепи оперативного тока) на входы аппаратуры РЗА, работающей по другому классу напряжения [6].

Неправильная работа релейной защиты по причине недостаточной ЭМС, по данным «Мосэнерго», составляет до 10% от всех случаев ложной работы и касается, в основном, только реле на микроэлектронной и микропроцессорной элементной базе [5]. Столь высокий процент случаев неправильной работы по причине недостаточной ЭМС вызван тем, что чувствительность к электромагнитным помехам МУРЗ на несколько порядков выше, чем у традиционных электромеханических защит. Например, по данным [6], если для нарушения работы электромеханического реле требуется энергия 10^{-3} Дж, то для нарушения работы интегральных микросхем – всего 10^{-7} Дж. Разница составляет 4 порядка.

Степень повреждения зависит от устойчивости как каждого из компонентов схемы, так и от энергии мощной помехи в целом, которая может быть поглощена схемой без появления дефекта или отказа. Например, для электромагнитного реле с катушкой на напряжение 230 В переменного тока коммутационная помеха от индуктивной нагрузки с амплитудой 500 В хотя и является более чем двукратным перенапряжением, но вряд ли приведет к отказу реле из-за стойкости электромеханики к такого рода помехам и малой длительности самой помехи (в течение микросекунд). Иначе обстоит дело с микросхемой, питающейся от источника 5 В постоянного тока. Импульсная помеха с амплитудой 500 В в 100 раз превышает напряжение питания этого электронного компонента и приводит к неизбежному отказу и последующему разрушению устройства. Стойкость микросхем к перенапряжениям на несколько порядков ниже, чем стойкость электромагнитного реле [7].

Импульсные перенапряжения, возникающие при разрядах молний и при коммутации в силовых электроустановках, способны повреждать и разрушать как электронные устройства, так и целые системы. Многолетняя статистика подтверждает, что число таких повреждений удваивается каждые три-четыре года [7]. Эта статистика хорошо согласовывается с законом Мура [6], еще в 1965 году показавшим, что количество полупроводниковых компонентов в микрочипах удваивается примерно каждые два года. И такая тенденция сохраняется уже много лет. Если каких-то десять лет тому назад микросхемы так называемой транзисторно-транзисторной логики (TTL) содержали 10-20 элементов на квадратный миллиметр и имели типичное напряжение питания 5 В, то сегодня популярные микросхемы могут содержать почти сто CMOS (Complementary Metal-Oxide Semiconductor) транзисторов на каждом квадратном миллиметре поверхности и имеют напряжение питания только 1,2 В. Новейшие технологии твердого тела, например, SOS (Silicon-On-Sapphire), поднимают плотность элементов до 500 на одном квадратном миллиметре поверхности [8]. Ясно, что для таких микросхем потребуется еще более низкое напряжение питания. При этом совершенно очевидно, что с повышением степени интеграции в микроэлектронике уменьшается устойчивость ее компонентов к высоковольтным импульсным перенапряжениям по причине уменьшения толщины изоляционных слоев и уменьшения рабочих напряжений полупроводниковых элементов.

Поскольку помехи, имеющие меньшую энергию, возникают чаще помех, имеющих большую энергию, наиболее частой реакцией МУРЗ на воздействие электромагнитных помех будет не разрушение устройства, а нарушение его работы или кратковременный сбой в работе с последующим восстановлением нарушенной функции. Это означает, что сработавшее неправильно на подстанции МУРЗ покажет полностью исправную работу при его исследовании в лаборатории, и установить причину его ложного срабатывания на подстанции будет невозможно.

В практике ОАО «Мосэнерго» накопилось уже достаточно фактов негативного влияния электромагнитных помех на работу МУРЗ. Наиболее наглядно это показывает опыт включения магнитного поля защит фирмы Siemens на ТЭЦ-12 ОАО «Мосэнерго» по проекту, выполненному институтом «Атомэнергопроект». При проектировании никак не были учтены требования ЭМС. Вследствие помех только за период с августа по декабрь 1999 года было зарегистрировано более 400 ложных информационных сигналов по дискретным и аналоговым входам МУРЗ [9]. При этом следует иметь в виду, что цена каждого отказа МУРЗ раз в 10 выше, чем цена отказа одного электромеханического реле, вследствие концентрации большого количества функций в каждом МУРЗ.

4. Функциональная безопасность в ЭЭЖС

Проблемы ЭМС современной ЭЭЖС значительно усложнены из-за применения современных высокочувствительных средств, обеспечивающих СЦБ, надёжность которых может оказаться ниже, чем при применении электромеханических релейных систем.

Справедливости ради следует отметить, что в России, активно занимающейся разработкой средств поражения электронной аппаратуры, находятся отдельные специалисты в области электроэнергетики и релейной защиты, понимающие нависшую опасность и принимающие соответствующие меры. Например в одном из базовых центров по внедрению передовых компьютерных (интеллектуальных) технологий в электроэнергетике России, созданном на базе Великоустюгских электрических сетей «Вологдаэнерго» и охватывающей 35 подстанций, с самого начала реконструкции приняли модель, согласно которой электромеханические защиты не были выброшены на свалку, а, наоборот, на базе новых электромеханических реле защиты разработаны и созданы новые панели релейной защиты, специально предназначенные для ввода в эксплуатацию в критической ситуации, когда вся компьютерная техника может быть выведена из строя. Кроме того, и сама интеллектуальная система автоматического управления специально разрабатывается для этого опытного полигона российской энергетики предприятиями оборонной промышленности по технологиям, используемым для производства космических аппаратов.

Изучение функциональной безопасности ЭЭЖС включает в себя выявление таких специфических опасных ситуаций, которые могут повлечь за собой серьезные последствия, и установление для каждой из них максимально допустимой частоты возникновения. Выявляется также оборудование, отказ которого может внести свой вклад в возникновение подобных ситуаций. Такое оборудование обычно называют «связанным с безопасностью». Например, системы сигнализации, централизации и блокировки на железной дороге. Их отказ может повлиять на возникновение аварийной ситуации, а поэтому их следует считать «связанным с безопасностью».

Следует отметить, что в настоящее время ведущие мировые концерны стремятся не просто обеспечить ЭМС электротехнических комплексов, которые они производят, а сделать их функционально безопасными.

Функциональной безопасности программируемых электронных систем посвящен международный стандарт IEC 61508, а также серия связанных с ним стандартов [10].

Стандарт IEC 61508 устанавливает общий подход к вопросам обеспечения безопасности для всего жизненного цикла систем, состоящих из электрических / электронных / программируемых электронных систем (E / E / PES), которые используются для выполнения функций безопасности. Этот унифицированный подход принят для того, чтобы разработать рациональную и последовательную техническую концепцию для всех электрических систем, связанных с безопасностью. Основной целью при этом является содействие разработке стандартов.

В большинстве ситуаций безопасность достигается за счет использования нескольких систем защиты, в которых используются различные технологии (например, механические, гидравлические, пневматические, электрические, электронные, программируемые электронные). Любая стратегия безопасности должна, следовательно, учитывать не только все элементы, входящие в состав отдельных систем (например, датчики, управляющие устройства и исполнительные механизмы), но также и все подсистемы, связанные с безопасностью, входящие в состав комбинированной системы, связанной с безопасностью. Таким образом, хотя стандарт посвящен в основном (E / E / PE) системам, связанным с безопасностью, он может также предоставлять общую структуру, в рамках которой рассматриваются системы, связанные с безопасностью, основанные на других технологиях.

Признанным фактом является существование огромного разнообразия использования (E / E / PES) в различных областях, отличающихся различной степенью сложности, опасностями и возможными рисками. В каждом конкретном применении необходимые меры безопасности будут зависеть от многочисленных факторов, которые являются специфичными для этого применения. Настоящий стандарт, являясь базовым стандартом, позволяет формулировать такие меры в будущих международных стандартах для областей применения.

По существу стандарт:

- рассматривает все этапы жизненного цикла систем безопасности в целом, а также подсистем E / E / PES и программного обеспечения (например, начиная с исходной концепции, включая проектирование, разработку, эксплуатацию, сопровождение и вывод из эксплуатации), в ходе которых E / E / PES используются для выполнения функций безопасности;
- был задуман с учетом быстрого развития технологий; его структура является достаточно устойчивой и полной для того, чтобы удовлетворять потребностям разработок, которые могут появиться в будущем;

- делает возможной разработку стандартов областей применения, где используются системы E / E / PES; разработка стандартов для областей применения в рамках общей структуры, вводимой настоящим стандартом, должна приводить к более высокому уровню согласованности (например, основных принципов, терминологии и т. п.) как для отдельных областей применения, так и для их совокупности; это приносит преимущества как в плане безопасности, так и в плане экономики;
- предоставляет метод разработки спецификаций для требований к безопасности, необходимых для достижения требуемой функциональной безопасности E / E / PE систем, связанных с безопасностью;
- использует уровни полноты безопасности для задания планируемого уровня полноты безопасности для функций, которые должны быть реализованы E / E / PE системами, связанными с безопасностью;
- использует для определения уровней полноты безопасности подход, основанный на оценке рисков;
- устанавливает количественные величины отказов E / E / PE систем, связанных с безопасностью, которые связаны с уровнями полноты безопасности;
- устанавливает нижний предел для планируемой величины отказов в режиме опасных отказов, который может быть задан для отдельной E / E / PE системы, связанной с безопасностью; для E / E / PE систем, связанных с безопасностью, работающих в:
- режиме с низкой интенсивностью запросов нижний предел для выполнения планируемой функции по запросу устанавливается на средней вероятности отказов 10^{-5};
- в режиме с высокой интенсивностью запросов нижний предел устанавливается на вероятности опасных отказов 10^{-9} в час.

Стандарт IEC 61508 выделяет четыре «уровня полноты безопасности» (Safety Integrity Level, SIL), которые выбираются в зависимости от тяжести последствий, которые могут наступить при неправильном функционировании системы.

Уровни SIL определяют величину допустимого риска для системы. Они являются мерой вероятности того, что система будет правильно выполнять свои функции, влияющие на безопасность.

Уровень SIL4 является самым высоким, наиболее труднодостижимым. Для его обеспечения требуется чрезвычайно высокая квалификация и работа «на грани искусства». Поэтому следует избегать необходимости его применения.

Уровень SIL3 ниже, чем SIL4, но также требует высокой квалификации и высокого уровня организации процесса проектирования. Немногие исполнители способны обеспечить этот уровень безопасности.

Уровень SIL2 требует управления работами в соответствии со стандартом ISO 9001. Достижение этого уровня требует большего числа испытаний, чем SIL1, что приводит к удорожанию проекта.

Уровень SIL1 является самым низким, для его выполнения достаточно наличия хорошего опыта разработок.

На основе стандарта IEC 61508 и серии связанных с ним стандартов в РФ опубликованы аутентичные ГОСТы по функциональной безопасности с с десятилетним отставанием от международных. В 2012 г. они частично переработаны [13-19]. К сожалению, эти ГОСТы носят лишь рекомендательный характер.

Необходимо заметить, что проблемы функциональной безопасности в ЭЭЖС ещё не стали предметом пристального внимания как разработчиков систем автоматического регулирования на железной дороге, так и эксплуатационников.

5. Проблемы в сфере нормативно-технического регулирования в ЭЭЖС

Прежде чем заняться проблемами функциональной безопасности на электрифицированной железной дороге, необходимо навести порядок в сфере нормативно-технической документации в ЭЭЖС:

- развить систему стандартизации и нормативно-технического обеспечения в отрасли электроэнергетики;
- разработать и гармонизировать комплекты стандартов и других нормативно-технических документов, которые бы объединяли множество интеллектуальных цифровых вычислительных и коммуникационных технологий и электрических архитектур, а также связанных с ними установленных норм и процедур, процессов и услуг, которые функционально и информационно должны быть совместимы и обеспечивать необходимые показатели надежности, безопасности и качества.

Чтобы разрешить проблемы развития нормативно-технического регулирования в области ЭМС и энергоэффективности электрооборудования в ЭЭЖС, необходимо осуществить следующие мероприятия:

- обеспечить однозначное понимание объектов технического регулирования и стандартизации оборудования, работ, процессов и услуг на основе разработанных справочников-словарей унифицированных терминов и определений;
- гармонизировать необходимые национальные стандарты с международными и европейскими, являющимися доказательной базой

нормативно-технического обеспечения в процессах управления и реализации проектов, и внедрить их;

- разработать и ввести единый классификатор электрооборудования, позволяющий разработать стандартизованные показатели энергоэффективно-сти и методов расчетов, учитывая географические и климатические условия;

- разработать эффективные унифицированные методы испытаний оборудования в соответствии с вышеописанными пунктами, а также реестр контрольно-измерительной аппаратуры в системах управления железнодорожным транспортом;

- регулярно проводить мониторинг устройств управления в ЭЭЖС и разрабатывать планы по совершенствованию её энергоэффективности и энергоресурсосбережению;

- создать хранилище данных нормативно-справочной информации, в том числе результатов мониторинга, анализа, статистики и инновационных инженерных решений в процессах изыскания, проектирования, строительства и эксплуатации объектов и сооружений железной дороги, т.е. по всему жизненному циклу.

Проблемы надёжности, живучести и безопасности в ЭЭЖС и связанные с ними проблемы ЭМС должны решаться комплексно. К сожалению, до последнего времени эти проблемы рассматривались либо независимо, либо с недостаточной полнотой. К сожалению, их решение в настоящее время находится в том же состоянии, как и решение аналогичных проблем в российской электроэнергетике [11].

До сих пор в электроэнергетике применяются устаревшие нормативно-технические документы и стандарты органов власти СССР и РСФСР, отраслевых институтов, а также документы РАО «ЕЭС России», разработанные много лет назад. Статус таких документов неоднозначен, поскольку часть из них носит рекомендательный характер, другие не прошли установленных процедур инкорпорирования в законодательство Российской Федерации. Федеральная служба по экологическому, технологическому и атомному надзору в своей деятельности руководствуется нормативно-техническими документами, перечень которых она сама утверждает ежегодно, что также не может быть признано правомерной практикой. Связано это с отсутствием процедуры принятия общеотраслевых стандартов и финансирования их разработки. Нет нормативных документов, регулирующих вопросы надежности, живучести и безопасности электроэнергетической системы и объектов электроэнергетики в условиях рыночных отношений, вступления России в ВТО, участия в Таможенном союзе и др.

Всё отмеченное является чрезвычайно актуальным для отдельных элементов, подсистем и в целом ЭЭЖС. Часть из рассмотренных вопросов отражены в протоколе совместного заседания научно-технической коллегии НП «НТС ЕЭС» и научного совета РАН по проблемам надежности и безопасности больших систем [12].

Федеральные законы «О техническом регулировании», «Об электроэнергетике», «О промышленной безопасности опасных производственных объектов», «О безопасности объектов ТЭК», а также постановление правительства «О мерах по совершенствованию подготовки нормативных правовых актов федеральных органов исполнительной власти, устанавливающих не относящиеся к сфере технического регулирования обязательные требования», а также изменения к ним, упорядочивают отдельные сферы регулирования, функционирования, безопасности, надежности и качества единой энергосистемы России и объектов электроэнергетики. Но они не устраняют системных проблем электроэнергетики в целом, дублирования и прямого противоречия правовых норм, пересечения полномочий и сфер ответственности федеральных органов исполнительной власти и т.д. Проблемы усугубляются значительным отставанием от Европейского союза и США в сфере стандартизации.

Естественно, что и разработка стандартов для электроэнергетики железных дорог находится в зачаточном состоянии.

Анализ, проведенный специалистами ФГБУ «РЭА» и «ВНИИНМАШ» Росстандарта, показал, что уровень гармонизации с международными и европейскими стандартами составляет, в среднем, лишь 23% (в Германии – 91%; в ЕС – 72%). Поэтому в отрасли неэффективно действует система технического регулирования, в которой стандарты должны играть основную доказательную базу в нормативно-правовых отношениях, как это происходит в Европейском союзе и США. В Штатах действуют более 600 организаций по стандартизации, в том числе в области электроэнергетики, отдельно – комитет по надежности электроэнергетики с полномочиями установления обязательных требований в стандартах. У нас практически не функционируют многие технические комитеты по стандартизации, созданные более 10 лет назад по различным направлениям электроэнергетики.

Проблема надежности и безопасности электроэнергетических объектов стала особенно актуальной после аварии на Саяно-Шушенской ГЭС и взрыва на Баксанской ГЭС. Эти и другие тяжелые аварии на электростанциях, происшедшие ранее, показали, что в нашей стране не только технические причины приводят к катастрофам. Предпосылкой зачастую является отсутствие обязательных требований и государственных

ограничений, соответствующих стандартов в эксплуатации опасных промышленных объектов, в связи с этим нет и персональной ответственности должностных лиц за нарушение технических нормативов.

Стоит отметить, что в нашей стране научными работниками «Научно-исследовательского и конструкторского института энергетики им. Н.А. Доллежаля» разработана современная управляющая система безопасности для объектов электроэнергетики с эффективной нормативной базой, составляющей основу технологической платформы безопасности и с соответствующей надёжностью в эксплуатации.

Такую технологию целесообразно использовать и при управлении ЭЭЖС. Система предполагает реализацию комплекса организационных и технических мер защиты на всех этапах жизненного цикла: разработка, изготовление, внедрение, эксплуатация, модернизация.

Из всего многообразия направлений обеспечения функциональной безопасности в области управляющих систем энергетических установок внимание уделяется, прежде всего, двум важнейшим взаимосвязанным аспектам:

- использованию при проектировании «директивных» принципов обеспечения функциональной безопасности;
- обеспечению качества на всех этапах жизненного цикла.

За последнее время был утвержден ряд нормативных документов. Однако принятые к 2011 г. меры нельзя считать достаточными для обеспечения надежности электроэнергетической системы и энергооборудования по следующим причинам:

- надежность, как важнейшая нормативно-техническая характеристика, не является обязательной;
- отсутствуют система стандартизации в отрасли и соответствующий организационно-методический институт, проведение работ по созданию нормативно-технических документов не скоординировано;
- нет отраслевой нормативно-технической базы и даже концепции и программы работ по стандартизации в отрасли;
- отсутствует регламентация отраслевых нормативно-технических документов и правил их утверждения, в том числе обязательных по проектированию и закупке энергооборудования, необходимого для обеспечения надежности и энергобезопасности.

6. Заключение

В докладе проанализировано состояние дел по обеспечению функциональной безопасности в ЭЭЖС. Установлено, что до настоящего времени работа по обеспечению функциональной безопасности

высокочувствительного электрооборудования в системах СЦБ железной дороги проводится недостаточно. Формально на базе стандарта IEC 61508 в Российской Федерации выпущены гармонизированные с ним ГОСТы [13-19], но они носят лишь рекомендательный характер к использованию. Кроме того, они не адаптированы к ЭЭЖС, имеющей существенную специфику по сравнению с устройствами стационарной энергетики. И, конечно, в них должны быть отражены ЭЭЖС, предполагающие использование магнитолевитационных технологий при организации электродвижения.

Библиографический список

1. Дэвид Дж. Смит. Функциональная безопасность. Простое руководство по применению стандарта МЭК 61508 и связанных с ним стандартов / Дэвид Дж. Смит, Кеннет Дж. Л. Симпсон - М.: Издательский Дом «Технологии», 2004. – 208 с.

2. Apollonskiy S. M., Starkhov V. G. Calculation of the penetration of EMF through a rectangular slot in a plane screen in the resonant frequency region //Telecommun., Radio Eng., 1991, vol. 46, no. 4, pp. 2–6. .

3. Гуревич В. И. Уязвимости микропроцессорных реле защиты: проблемы и решения. – М., 2014. – 256 с.

4. Theriault G., Goldberg E. T. & so on. Cancer Risks Associated with Occupational Exposure to Magnetic Fields among Electric Utility Workers in Ontario and Quebec, Canada and France: 1970 – 1989 //American Journal of Epidemiology 1994, v. 139, n. 6, pp. 550-571.

5. Плакс А. В. Электрические железные дороги /А.В. Плакс, В.П. Феоктистов, А.Н. Савоськин и др. – М.: Транспорт, 1993. – 278 с.

6. Марквардт Г. Г. Вычислительная и микропроцессорная техника в устройствах электрических железных дорог. – М.: Транспорт, 1989. – 286 с.

7. Косарев А. Б. Основы теории электромагнитной совместимости систем тягового электроснабжения переменного тока. – М.: ИНТЕКСТ, 2004. – 272 с.

8. Кузнецов М. Входные цепи устройств РЗА. Проблемы защиты от мощных импульсных перенапряжений / М. Кузнецов, Д. Кунгуров, М. Матвеев, В. Тарасов // Новости электротехники, 2006, № 6 (42).

9. Чижма С. Н. Совершенствование методов и средств контроля качества электроэнергии и составляющих мощности в электроэнергетических системах с тяговой нагрузкой. Дисс. докт. техн. наук. – Омск, 2014. – 368 с.

10. A Summary of the IEC 61508 Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Programmable Electronic Safety-Related Systems. – Sellersville, PA 18960, USA. – 29 pp.

11. Карякин А. М. Энергетическая безопасность России в условиях рыночных отношений в электроэнергетике. – М., 2012. – 224 с.

12.Чмель А.В., Шкрабляк Н.С. Проблемы структурной модернизации системы управления предприятиями электроэнергетики России. – М.: НИЭБ, 2012. – 108 с.

13. ГОСТ Р МЭК 61508-1-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования.

14. ГОСТ Р МЭК 61508-2-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам.

15. ГОСТ Р МЭК 61508-3-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению.

16. ГОСТ Р МЭК 61508-4-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных связанных с безопасностью. Часть 4. Термины и определения.

17. ГОСТ Р МЭК 61508-5-2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности.

18. ГОСТ Р МЭК 61508-6-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2-2012 и ГОСТ Р МЭК 61508-3-2012.

19. ГОСТ Р МЭК 61508-7-2012. Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства.

References

1. Smith D. J. & Simpson K. J. L. *Funktcionalnaya bezopasnost. Prostoye rykovodstvo po primeneniu standarta MEK 61508 i svazanix s nim standartov* [Functional safety. A simple guide on the use of IEC 61508 and related standards]. Moskow, 2004. 208 p.

2. Apollonskiy S. M. & Starkhov V. G. Calculation of the penetration of EMF through a rectangular slot in a plane screen in the resonant frequency region. Telecommun., Radio Eng., 1991, vol. 46, no. 4, pp. 2-6.

3. Gurevich V. I. *Uyazvimosti mikroprocessornyx rele zashhity: problemy i resheniya* [Vulnerabilities microprocessor relay protection: problems and solutions]. Moskow, 2014. 256 p.

4. Theriault G. & Goldberg E. T. *American Journal of Epidemiology*, 1994, vol. 139, n. 6, pp. 550-571.

5. Crybaby A. V., Feoktistov V. P. & Savoskin A. N. *Elektricheskie zheleznye dorogi.* [Electric Railways]. Moskow, 1993. 278 p.

6. G. Marquardt. *Vychislitelnaya i mikroprocessornaya texnika v ustrojstvax elektricheskix zheleznyx dorog vychislitelnaya i mikroprocessornaya texnika v ustrojstvax elektricheskix zheleznyx dorog* [The computing and microprocessor technology devices electric railways]. Moskow, 1989. 286 p.

7. Kosarev A. B. *Osnovy teorii elektromagnitnoj sovmestimosti sistem tyagovogo elektrosnabzheniya peremennogo toka* [Fundamentals of the theory of the electromagnetic compatibility of traction power supply AC]. Moskow, 2004. 272 p.

8. Kuznetsov M., Kungur D., Matveev M. & Tarasov V. *Novosti elektrotexniki – News of Electrical Engineering*, 2006, vol.42, no 6.

9. Chizhma S. N. *Sovershenstvovanie metodov i sredstv kontrolya kachestva elektroenergii i sostavlyayushhix moshhnosti v elektroenergeticheskix sistemax s tyagovoj nagruzkoj* [Improvement of methods for monitoring power quality and power components in power systems with traction load]. Diss. Doctor. tehn. Sciences. Omsk, 2014. 368 p.

10. A Summary of the IEC 61508 Standard for Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Programmable Electronic Safety-Related Systems. Sellersville, PA 18960, USA. 29 pp.

11. Karjakin A. M. *Energeticheskaya bezopasnost rossii v usloviyax rynochnyx otnoshenij v elektroenergetike* [Energy security of Russia in the conditions of market relations in the power sector]. Moskow, 2012. 224 p.

12. Chmel A. & Shkrablyak N. S. *Problemy strukturnoj modernizacii sistemy upravleniya predpriyatiyami elektroenergetiki Rossii* [The problems of structural modernization of the enterprise management system of Russian power]. Moskow, 2012. 108 p

13. GOST R IEC 61508-1-2012. Functional safety systems, electrical, electronic, programmable electronic safety-related. Part 1: General requirements. elektricheskie zheleznye dorogi

14. GOST R IEC 61508-2-2012. Functional safety systems, electrical, electronic, programmable electronic safety-related. Part 2: Requirements for systems.

15. GOST R IEC 61508-3-2012. Functional safety systems, electrical, electronic, programmable electronic safety-related. Part 3: Software requirements.

16. GOST R IEC 61508-4-2012. Functional safety systems, electrical, electronic, programmable electronic safety-related. Part 4. Definitions.

17. GOST R IEC 61508-5-2012 Functional safety systems, electrical, electronic, programmable electronic safety-related. Part 5. Application methods for determining the safety integrity levels.

18. GOST R IEC 61508-6-2012. Functional safety systems, electrical, electronic, programmable electronic safety-related. Part 6: Guidance on the application of IEC 61508-2-2012 GOST R and GOST R IEC 6150819. GOST R IEC 61508-7-2012. Functional safety systems, electrical, electronic, programmable electronic safety-related. Part 7: Methods and tools.-3-2012.

Сведения об авторе:

АПОЛЛОНСКИЙ Станислав Михайлович, доктор техн. наук, профессор, засл. деятель науки РФ, ведущий специалист по ТПС ОАО «Ленгипротранс»

E-mail: smapollon@yahoo.com

Information about author:

APOLLONSKIY Stanislav, Dr. Sci. Sciences, Professor, Honored Worker of Science, a leading expert on traction substations of Open Joint Stock Company "LENGIPROTRANS"

E-mail: smapollon@yahoo.com