УДК 621.3

ОБЕСПЕЧЕНИЕ ФУНКЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ И ЗАЩИТЫ ДЛЯ ВЗРЫВООПАСНЫХ СРЕД

Л. Г.ЧЕРНАЯ, В. Н. АБАБУРКО, П. Ф. НИКИТИН
[*]В. Ч. КАНТОР, [*]А. Е. САЗОНКО, [*]А. В. КОХАН
Государственное учреждение высшего профессионального образования
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»
[*]ДЕПАРТАМЕНТ ПО НАДЗОРУ ЗА БЕЗОПАСНЫМ ВЕДЕНИЕМ РАБОТ В ПРОМЫШЛЕННОСТИ (ГОСПРОМНАДЗОР)
Могилев, Минск, Беларусь

В настоящее время на мировом рынке широко предлагаются безопасные системы управления и противоаварийной защиты для взрывоопасных производств. Для их правильной эксплуатации необходимы хорошие знания и правильное применение, положенных в основу работы этих систем, технических нормативных и правовых актов в области функциональной безопасности. В Республике Беларусь введен в действие германизированный с международными нормами комплекс стандартов СТБ IEC 61508-1-2014… СТБ IEC 61508- 4-2014 «Функциональная безопасность электрических, электронных, программируемых электронных систем, относящихся к безопасности…», описывающих классификацию, аппаратное и программное обеспечение безопасных электрических / электронных / программируемых электронных систем (electrical/electronic/programmable electronic system) E/E/PES. Системы служат для управления, защиты или мониторинга, основанные на использовании одного или нескольких электрических/электронных/ программируемых электронных (electrical/electronic/programmable electronic) E/E/PE устройств, включая все элементы системы, такие как: источники питания; датчики и другие устройства ввода; магистрали данных и другие коммуникационные магистрали; устройства привода и другие устройства вывода.

На различных стадиях жизненного цикла управляемого оборудования (equipment under control) EUC возможно возникновение отказов, которые приводят к опасным ситуациям и, в зависимости от стечения обстоятельств, способны создать существенную угрозу для человеческих жизней. Эти отказы делятся на опасные обнаруживаемые и опасные необнаруживаемые.

При опасных обнаруживаемых отказах система обеспечения безопасности может, при соответствующей настройке, перевести весь агрегат или установку в безопасное состояние. Весьма критичную ситуацию представляют собой необнаруживаемые опасные отказы. Они могут сохраняться в системе до ее выключения, или, в худшем случае, до аварийной ситуации, при полном неведении пользователя об их наличии.

Системы, связанные с безопасностью, предназначены для того, чтобы уменьшить частоту (или вероятность) опасных событий и/или последствий опасных событий, достигнуть требуемого уменьшения риска, делающего его допустимым. Системы, связанные с безопасностью:

– реализуют функции безопасности, необходимые для достижения или поддержания безопасного состояния управляемого оборудования, например, когда температура достигает значения *x*, должен открываться клапан *y*, который позволяет воде поступать в сосуд;

– используя собственные средства, или в совокупности с другими E/E/PE системами, связанными с безопасностью; с системами, связанными с безопасностью, основанными на других технологиях; или с внешними средствами уменьшения риска – достигают необходимой полноты безопасности для требуемых функций.

Полнота безопасности определяется как вероятность того, что система, связанная с безопасностью, будет удовлетворительно выполнять требуемые функции безопасности.

Чем выше уровень полноты безопасности (safety integrity level) SIL системы, связанной с безопасностью, тем ниже вероятность того, что система, связанная с безопасностью, не сможет выполнить требуемые функции безопасности. Имеется четыре уровня полноты безопасности, для систем уровень полноты безопасности, равный 4, характеризует наибольшую полноту безопасности, уровень, равный 1, отвечает наименьшей полноте безопасности. Например, для уровня полноты безопасности SIL 4 (средняя вероятность отказов, равная 10^{-5} при выполнении назначенной функции по запросу, или как вероятность опасного отказа, равная 10^{-9} в час).

При определении полноты безопасности должны учитываться все причины отказов, которые ведут к небезопасному состоянию, например, отказы аппаратуры, отказы, вызванные программным обеспечением, и отказы, имеющие причину в электрическом интерфейсе.

Необходимо обеспечивать системный подход к проблеме функциональной безопасности систем управления EUC для взрывоопасных сред, который состоит из трех составных частей:

– определение требований к безопасности с учетом уровня полноты безопасности SIL;

– реализация системы или устройства, обеспечивающих безопасность;

– ввод в эксплуатацию, проверка эффективности всех функций безопасности, эксплуатация, техническое обслуживание и вывод из эксплуатации.