УДК 621.3

ФУНКЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ СИСТЕМ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ И КОНТРОЛЯ

Л. Г. ЧЕРНАЯ, В. Н. АБАБУРКО
Государственное учреждение высшего профессионального образования
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»
Могилев, Беларусь

Системы противоаварийной защиты и контроля – системы электрические/электронные/программируемые электронные E/E/PE (electrical/ electronic/programmable electronic), связанные с безопасностью, должны выполнять функции, которые могут быть определены в спецификациях требований к функциям безопасности технологических установок EUC (equipment under control) и изменять последствия отказов в такой степени, что риск становится допустимым. Например, спецификация требований к функциям безопасности может содержать требование о том, что, когда температура достигает значения X, должен открываться клапан Y, который позволяет воде поступать в сосуд.

В свою очередь, системы, связанные с безопасностью, должны иметь степень надежности, достаточную для достижения в конкретной области применения допустимого риска, т.е. частота отказов систем, связанных с безопасностью, должна быть достаточно низкой, чтобы предотвратить превышение частоты опасных событий, соответствующей допустимому риску.

Допустимый риск зависит от многих факторов (например, от тяжести травм, числа людей, подвергающихся опасности, от того, насколько часто человек или люди подвергаются опасности, а также от периода времени, в течение которого люди подвергаются опасности).

Основываясь на рекомендациях МЭК 61508, разработана методика достижении допустимого риска для EUC, которая состоит из следующих этапов:

– определить числовое значение планируемого допустимого риска Ft, которое соответствует уровню полноты безопасности SIL (safety integrity level);

– определить риск EUC: $R_{пр}= F_{пр}\cdot C$. Для этого необходимо определить частотную составляющую риска EUC без учета каких-либо средств защиты $F_{пр}$; определить последствия опасного события С без учета каких-либо средств защиты. Частота, связанная с риском, создаваемым EUC, включая систему управления EUC и вопросы, связанные с человеческим фактором, но без учета каких-либо мер защиты, может быть определена с использованием количественных методов оценки риска. $F_{пр}$ может быть определена с помощью: анализа интенсивности отказов в схожих ситуациях; данных из соответствующих баз данных; расчетов с применением соответствующих

методов прогноза;

– определить, достигается ли для частоты $F_{пр}$ и последствия С допустимый уровень риска. Если получен I класс риска, то требуется дальнейшее снижение риска. Риски IV или III классов могут быть допустимыми рисками. Риск II класса требует дальнейших исследований;

– определить уменьшение риска ΔR, необходимое для того, чтобы сделать его допустимым. Для этого необходимо определить среднюю вероятность отказа PFD_{avg} (average probability of failure on demand) системы, связанной с безопасностью, при работе по запросу PFD_{avg}, состоящего в невозможности достичь требуемого снижения риска ΔR. Для постоянных последствий С:

$$PFD_{avg} = (F_t/F_{пр}) = \Delta R.$$

Например, для $PFD_{avg} = 10^{-2} – 10^{-3}$ уровень полноты безопасности SIL равен 2.

Системы, связанные с безопасностью, должны уменьшить интенсивность возникновения опасностей, как минимум, с $F_{пр}$ до F_t.

Главная цель состоит в обеспечении того, что оставшиеся отказы, соответствующие уровню полноты безопасности SIL, не приведут к отказу E/E/PE системы, связанной с безопасностью.

Для этих целей определяют среднюю вероятность отказа в обслуживании функции безопасности для E/E/PE системы, связанной с безопасностью. Средняя вероятность отказа по запросу для функции безопасности E/E/PE системы, связанной с безопасностью, PFD_{SYS} может быть вычислена по формуле: $PFD_{SYS} = PFD_S + PFD_L + PFD_{FE}$, где PFD_S – средняя вероятность отказа по запросу для подсистемы датчиков; PFD_L – средняя вероятность отказа по запросу для логической подсистемы; PFD_{FE} - средняя вероятность отказа по запросу для подсистемы оконечных элементов.

Компонентами подсистемы датчиков, например, могут быть датчики, защитные экраны, входные согласующие цепи; компонентами логической подсистемы – микропроцессоры и компьютерные с программным обеспечением; а компонентами подсистемы оконечных элементов – выходные согласующие цепи, экраны и исполнительные механизмы.

Для определения средней вероятности отказа каждой подсистемы должны быть известны следующие данные: архитектура построения, охват (покрытие) диагностикой каждого канала, интенсивность отказов для каждого канала в час; коэффициенты: β (dangerous undetected common-cause failure), β_D (dangerous detected common-cause failure) – влияния опасных необнаруживаемых и обнаруживаемых отказов соответственно.

Предложенная методика позволяет проектировать системы, противоаварийной защиты и контроля с требуемым уровнем полноты безопасности SIL.