Х. Шебе

ПО ПОВОДУ СТАТЬИ А.Ф. КОЛЧИНА, Н.В. МИХЕЕВА «АРХИТЕКТУРА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ, СВЯЗАННОЙ С БЕЗОПАСНОСТЬЮ»

Статья Колчина А.Ф. и Михеева Н.В. [1] вызвала у меня недоумение и ряд вопросов. Прежде всего, судя по названию статьи, архитектура программного обеспечения должна учесть требования стандарта [2], особенно те, которые изложены во второй его части, а также в п.п.7.4.3, В.1 и В.9 третьей части. В этих статьях стандарта акцентируется внимание на построении избыточных систем, обеспечении разнообразия методов исключения отказов, и, особенно, отказоустойчивости систем. Однако в рассматриваемой статье [1] отсутствует учет указанных существенных требований. Вместо требований базового по функциональной безопасности стандарта [2] авторами предложено строить структуру и архитектуру программного обеспечения (ПО) на основании источников по качеству ПО, которые не связаны с безопасностью.

Надо учесть, что следует обеспечивать стабильное поведение ПО, включая поведение ПО во времени. Надо обеспечить, чтобы ПО смогло в одном цикле или во времени обработать все запросы. С некоторыми структурами и архитектурами предложенными авторами это не обеспечивается – наоборот, эти структуры опасны в этом отношении. Если возникают временные проблемы ПО, то надо привлечь методы вероятностного анализа поведения ПО (смотри, например [3]). И это не упоминается авторами.

Поэтому, к сожалению, статья поощряет выбор опасных архитектур, которые противоречат требованиям стандарта [2].

Литература

1. **Колчин А.Ф., Михеев Н.В.,** Архитектура программного обеспечения системы, связанной с безопасностью, Надежность, № 1 (2015), стр. 75-81.

2. ГОСТ Р МЭК 61508–2012 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Части 1 – 7.

3. **Altmeyer S., Davis R.A.,** On the Correctness, Optimality and Precision of Static Probabilistic Timing Analysis, University of York, report no. YCS-2013-487.