H. Schäbe

ABOUT THE PAPER BY A.F. KOLCHIN, N.V. MIKHEEV "ARCHITECTURE OF SAFETY RELATED SYSTEM SOFTWARE"

The paper by Kolchin A.F. and Mikheev N.V. [1] brought out bewilderment and a number of questions in me. First of all, judging by the title of the paper, the architecture of software should take into account the requirements of standard [2], in particular those specified in its second part as well as in cl. 7.4.3, B.1 and B.9 of the second part. These clauses of the standard make focus on development of redundant systems, ensuring a variety of methods for eliminating failures and, in particular, system fault-tolerance. However, paper in question [1] lacks the consideration of these substantial requirements. Instead of the requirements of standard [2] that is a key one in terms of functional safety, the authors offer to construct the structure and architecture of software (SW) based on SW quality sources that are not related to safety.

It is needed to be taken into account that we should secure SW stable behavior including SW behavior in time. It is required to ensure that SW could process all requests for one cycle or in time. For some structures and architectures proposed by the authors, this is not ensured – on the contrary, these structures are dangerous in this respect. If SW time problems occur, then methods of SW behavior probabilistic analysis (see, for example [3]) should be applied. And this is not mentioned by the authors.

Therefore, unfortunately, the paper facilitates choosing hazardous architectures that contradict the requirements of standard [2].

References

1. **Kolchin A.F., Mikheev N.V.** Architecture of safety related system software. Dependability, No. 1 (2015), pp. 75-81.

2. GOST R IEC 61508-2012 Functional safety of electrical, electronic and programmable electronic safety related systems. Parts 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.