Alpeev A.S.

DEPENDABILITY OF CONTROL SYSTEMS SOFTWARE AND SAFETY OF NUCLEAR POWER PLANTS

The paper considers the aspects of applicability of programmable control systems for nuclear power plants. The advantages and disadvantages of these systems have been identified. The main disadvantages of these systems have been singled out as follows: impossibility to prove the parameters of dependability of implemented control functions, susceptibility to potential cyber attacks. The paper offers the method of selecting automation means for implementing control systems using programmable and non-programmable automation means based on making a functional analysis of a nuclear power plant's control systems.

Keywords: *safety, control system, nuclear power plant, dependability, reliability, automation means, software, analysis, function, functional group, parameter.*

The problem of proof of SW dependability from the moment of its application in practical human activities has had one of the important places, since its use to reach required results has become necessary for solving various complex tasks practically in all areas of science and economy. Proof of its parameters becomes of special importance when constructing control systems for hazardous nuclear facilities such as nuclear power plants. The point is that failure-free operation of a nuclear power plant should be guaranteed for a long period of about 40-60 years. Such long failure-free operation requires implementing control systems with dependability parameters whose implementation and demonstration is practically infeasible at present.

That is why various teams of researchers have already been making researches in this field for about forty-fifty years, and a required result has not been achieved so far. Of course, to solve this problem is vital and necessary, though the problem of application of programmable automation means should be solved here and now based on those data that we have at present.

As mentioned above, the dependability of software used in control systems of nuclear power plants for executing control in operation modes and in case of accidents face high requirements, which in the context of existing programmable automation means and circuit engineering do not ensure proof of required time to failure of implemented functions equal to about 106 hour. Such situation regarding development of control systems is unsatisfactory and requires measures to be taken to ensure a due dependability of control systems operation. Also, emerging information about successful cyber attacks at hardware with control programmable systems related to nuclear installations [1] has increased interest in solving the problem of dependability of control systems used at nuclear power plants.

To start considering the topic, let us investigate the current situation regarding available information about automation means and systems. And it is worth to take into account that as stated in [2] cl. 2.9 "Quantative estimation of reliability of digital programmable means

due to a number of drawbacks is more difficult than for non-programmable means. It can cause some difficulties in demonstrating the expected safety of a system developed on the basis of a computer. Currently, the requirements of high program reliability are not provable. Consequently, projects based on a single system that is developed on the basis of a computer and has a failure rate as per requirement for the failure rate worse than 10^{-4} for software shall be implemented with caution". Further in [2] cl. 2.13 it is stated that "Quantitative definition of software reliability is an issue yet to be solved. Testing of software has some restrictions and thus quantative definition of software reliability for computer systems can be difficult or impossible to demonstrate".

For further consideration, all automation means are offered to be divided into two groups: (1) programmable automation means and (2) non-programmable automation means. Control systems can be implemented on the basis of the first category automation means as well as the second category automation means, and such experience in the practice of developing such systems is already available in the world. Let us consider the advantages and disadvantages of control systems developed with the help of automation means of the groups specified above.

First of all, it is worth to note that lately we witness the expanding application of control systems based on programmable automation means.

In particular it is related to the fact that such systems allow:

• ensuring a better control of parameters of a nuclear power plant, including those critical for safety;

• ensuring a better man-facility interface;

• ensuring ad-hoc testing;

• ensuring self-diagnostics of automation means and functional groups;

• ensuring better diagnostics;

• ensuring an enhanced precision of measurements;

• ensuring better resilience;

• reducing demand of cables owing to application of multiplex structures (common information buses);

• facilitating modification of control systems for emerging operational tasks.

The above advantages of programmable control systems do not rule out existing disadvantages of such systems. For example, such as:

• development and construction of software looks like a more complicated process and thus has a higher probability of generating mistakes, whose detection is rather a difficult task;

• difficulty in demonstrating reliability parameters;

• implementation of software generally represents discrete logical models of real world, thus leading to two types of consequences:

- software is more sensitive (i.e. less tolerable) to "small mistakes";

- interpolation and extrapolation methods are absolutely not applicable since they give unreliable results.

Therefore, the first group of automation means makes it possible to develop control systems with enhanced parameters of operation quality, however these systems do not have sufficient proof as regards dependability of execution of required functions and can be susceptible to cyber attacks [1].

The second group of automation means has bigger experience of industrial applications, however it is inferior to the first group in quality of implementation of required functions, it is more complex in terms of construction, commissioning and maintenance. Yet for control systems based on these automation means, dependability parameters are proved well enough and, as seen by the experience of longstanding operation, are not subject to cyber attacks.

When control systems based on automation means of different types are considered in such a way, their advantages and disadvantages are clearly seen. And in my opinion, it naturally leads to the necessity to consider possible symbiosis of systems based on automation means of two groups specified above, in order to use their positive sides in full and avoid negative effects of their applications.

To that end, we have to analyze functional groups of all control systems of a nuclear power plant to differentiate the functional groups for which the quality of implementation is sufficiently difficult and time consuming, and those whose failure causes an accident. According to [3], "Functional group is a part of a control system specified in the design that represents the aggregate of automation means implementing a specified function". According to [3] cl. 3.17, wherein it is stated that the design documents of safety related control systems shall specify functional groups and their classification as to safety categories. During the analysis it is necessary to take into account the classification of functional groups as to safety as well as a number of aspects vital for implementation of control systems.

For example, functional groups implementing protection as to one parameter generally represents quite a simple structure: meter of protection parameter, circuit comparing with a value of a specified protection parameter, device generating a command signal in case of a measured parameter exceeding the value of a specified parameter and a executive device. The algorithm of such system is quite simple and does not change in time. Operational mode is stationary and generally well troubleshot. The failure of a protection system can lead to substantial losses, i.e. the realization of a successful cyber attack has to be impossible. For such functional groups, in my opinion, its implementation should be done on the basis of automation means specified as the 2nd group.

In cases when a functional group implements rather a complex function, e.g. alignment of the field of a nuclear reactor's power density which has quite a complicated algorithm of implementation and depends on a lot of permanently changing technological parameters, such functional group, in my opinion, should be implemented on the basis of automation means of the 1st group. Since

the group will secure a better quality of implementation of a required task in automatic mode than in automated control mode. The application of the first group for automation purposes is reasonable in cases when we need control related to coordination of a large group of parameters and depending on technological parameters changing in time, for example, related to fuel burn-up or technological hardware failures when the continuity of a technological process has to be kept by putting backup hardware into operation without delay.

Therefore, the results of a functional analysis of a nuclear power plant's control systems is the basis for selecting automation means for developing respective control systems.

It should be noted that diagnostics systems, particularly those of safety related control systems, as a source of alarming signals should also be implemented on the basis of non-programmable automation means in order to be protected against cyber attacks and have a calculable dependability proof.

As stated in [4] cl. 4.1.12, "The report of NPP safety proof shall contain data on dependability parameters of normal operation systems critical for safety and their elements belonging to 1 and 2 safety classes as well as safety systems and elements. The analysis of dependability shall be made with common cause failures and staff mistakes taken into account".

Therefore, all functional groups of 1 and safety classes control systems will have dependability parameters justified by calculation, as they will be implemented on the basis of automation means of the 2nd group. Functional groups of 3 class implemented on the basis of programmable automation means will have a failure rate of up to 104 hour, which at present is an accepted value.

The author hopes that the offered method for selecting automation means and respective construction of control systems for nuclear power plants will be provided with more rationalized parameters of operation dependability.

References

1. Military bulletin as of 04.09.2012. «World cyber wars».

2. Software of safety critical systems implemented on the basis of computers for nuclear power plants. NS-G-1.1.

3. Requirements for control systems critical for nuclear power plants safety. NP-026-04.

4. General guidelines for safety of nuclear power plants. NP-001-97.