Application of Petri Nets for Formalization of NPP I&C Functional Design

Alexey CHERNYAEV, Elena ALONTSEVA, and Alexey ANOKHIN

Design Division, JSC "Rusatom Automated Control Systems", 25 Pherganskaya str., Moscow, 109507, Russian Federation (AlNChernyaev@rasu.ru, ENAlontseva@rasu.ru, ANAnokhin@rasu.ru)

Abstract: The paper describes the experience gathered from functional modelling of the process system using the Petri net formalism. The Petri net modification used in this study combines multilevel prioritized Petri Net with inhibitory arcs allowing formalization of hierarchical function-oriented description of a process system, which is a part of I&C functional design process. The hierarchy contains four levels, namely goals, abstract functions, process functions and equipment. Simple process system was modelled in order to analyze an adequacy of the selected Petri net modification. The modelling process includes building of abstract / process functions and equipment hierarchy followed by building of Petri net and realization / testing of this net using special software. The reduced function and equipment state space assuming only two states (function is fulfilled / not fulfilled, equipment is switched on / off) was used for the purpose of the present study. The experience acquired during the study allows to conclude that application of Petri net provides development of strictly formalized structural functional model which can be a subject for farther analysis using full scope or engineering simulator.

Keyword: Process system, Model, Functional analysis, Petri nets

1 Introduction

The current approach to control of nuclear power plant (NPP) implies that operator concentrates on monitoring and control of process equipment state. Based on information about process parameters and equipment state the operator draws a conclusion regarding recent operational conditions followed by execution of appropriate operational procedure.

An alternative control philosophy has appeared and is developing during last two decades. It assumes that process equipment is just a tool providing fulfillment of a certain function, which in turn provides achievement of an industrial system goal. In many cases one function to be performed by one equipment or system only. However, there are situations when the same function can be fulfilled by various ways / equipment, which is a result of implementation of diversity and redundancy principles. Being concentrated on the status of equipment only the operator can miss information about fulfillment of the respective function. For example, shutdown of circulation loop pump may be interpreted by operator as a failure of heat removal from reactor. Meanwhile, an alternative equipment may be automatically activated (for example, pressurized emergency water reservoir), which provides fulfillment of the heat removal function. In order to recognize this fact, the operator has to make certain that this alternative equipment has been activated successfully as well as the temperature in reactor does not increase. Much shorter cut is to demonstrate to the operator that the function of heat removal is fulfilled or to advise how it can be restored in case of failure. Such information representation and control philosophy is known as function-based (or function-oriented) approach.

Relatively little number of publication covering a topic of formalization and application of the function-oriented control approach are known to date. Safety parameters display system intended to support operators in nuclear safety ensuring is one of the most successful and impressive example of application. This system provides operator with possibility to monitor state of safety functions which is evaluated basing on binary event trees. The other case of implementation of functional approach covers the normal (no safety related) operational functions [1].

However, application of function-oriented control approach does not mean simple redesign of human-machine interface and operational procedures. The function-based control is possible only in case when the functional philosophy is applied over the whole NPP lifecycle including function-oriented design of NPP and I&C system. The proposed procedure for I&C functional design includes [2]:

- description of the NPP structure in the form of four layer (four level) semantic net;
- description of cause-consequence relationships between process functions in the form of functional net;
- development of I&C system architecture including list of measurement points and actuators;
- mathematical modeling of process equipment and control algorithms.

Function-oriented description of NPP is a four-level (four-layer) hierarchy. The upper level of hierarchy is the *purpose* (one or several) of the system. The second level includes *abstract functions*, describing the purpose in terms of physical processes, such as conversion of nuclear energy into heat (heat generation), heat transfer, conversion of heat into mechanical energy. The third level includes *process functions*, by which abstract functions are performed. These functions are formulated in terms of specific physical processes in which some process mediums are involved, e.g. coolant heating, water demineralization, substance transportation, etc. Each process function is performed by specific *process equipment* (e.g., pumps, heat exchangers, pipelines, etc.), forming the lower (fourth) level of the functional hierarchy.

Two types of binary relations are defined for the set of goals, abstract functions, process functions and equipment. The *parent-child relationship* connects the components of different hierarchy levels. The relationship of this type defines how the function of upper level is implemented at lower level. The *functional relationships* are established between two functions and demonstrate that one function initiates performing the other one.

Hierarchy of functions demonstrates structural relationships and allows to answer the questions “How is the system goal achieved?” and “What does the system consist of?” However, this form of description does not reflect such a significant relation type as *causal-consequences* relationship. In order to describe them a semantic network (hierarchy) should be converted into a functional network which looks as a directed graph. Process functions are the nodes of this graph, while the arrows represent causal relationships, i.e. dependences of one function state on the other function state.

Functional network provides qualitative structural description of a process and visualize causal-consequences interrelationships between functions. This presentation clearly explains the process; however, much stricter model is required to develop control concept and control algorithms. The present paper is aimed to empirical evaluation of opportunity to apply Petri nets for development of such model. Use of the Petri net formalism is illustrated by the example of description of simple heat generating system [2]. The model has been tested using special software, which allows to make preliminary conclusions concerning of applicability of Petri nets for modelling of more complicated process systems.

2 Methodology

2.1 Classification of Petri nets

Petri net is an algebraic structure with two sets, one called *places* and the other called *transitions*, together with their associated relations and functions, and named after their inventor, Carl Adam Petri [3]. Elements of the same set can’t be connected with each other. State of system or process modelled by Petri net is described by marking of a net, which looks as a distribution of tokens among places.

Petri net is an extremely effective tool for validation of systems, description of their dynamics, designing of procedures for control of system under abnormal situations and multiple failures. There are many types and modifications of Petri nets which can be selected depending of specific features of process or system which is a subject to modelling. In a whole, Petri nets are categorized into two classes, namely *Original Petri nets* and *High-level Petri nets* [4]. *Extended Petri nets* and *Modified Petri nets* are located between these two categories.

The Original net doesn’t associate any conditions with transitions and places, i.e. all transitions and tokens are identical. The High-level net can contain colored tokens, prioritized transitions and transitions with associated delays. Moreover, such nets may have complex internal structure. *Colored Petri net* allows to use colored tokens and the places which are adapted to accept the tokens with certain color only. This allows to represent operation of the complex system where there are a few parallel flows of different materials. *Timed Petri net* contains transitions which fires with some delay. This allows not only to define a chain of events but also to map the events to the time scale. In *Petri net with priorities* a priority (for example, high, normal and low) should be assigned to each transition. The priorities allow to specify the sequence in which transitions should be fired. *In Hierarchical (nested, multilevel) Petri net* any token or transition can be decomposed into lower level net, which allows to describe structure of complex system. *Inhibitory Petri net* contains inhibitory arcs along with regular arcs. Inhibitory arc connects transition with place and prevents the firing of the transition when the place contains a token.

Various kinds of Petri nets and their modifications are extensively used for simulation of processes and verification of models [5, 6]. As a rule, in these applications the "place" is interpreted as a condition, data, signal, resource, buffer, conclusion, while the "transition" is an event, computation step, signal processor, task or job, cause of logic, processor [7].

There are not numerous publications describing the experience of application of Petri nets for simulation of technological process. For example, modified stochastic Petri net is used for detection of local deviations in turbogenerator stator windings [8]. Petri nets are also used as a tool for analysis of dynamical properties of the UML diagrams used for development of software for control of pumping plant [9]. The activity diagram is transformed into Petri net in order to reveal potentially incorrect states achieved by the system when operator switches on or stops the pumps. It is especially important when the developed model is used in farther software and I&C system development process.

2.2 The proposed Petri net notation

Modified multilevel Petri net with inhibitory arcs is used in the present study. In case of farther application of developed net for simulation and validation purposes the net should be supplemented (extended) by time delays and priorities.

Practically in all publications devoted to application of Petri nets for modeling of technological process, an equipment component or a technological system is considered as an object, and state or behavior of this equipment are considered as a subject of modeling. Commonly accepted that place is used for representation of state of equipment, while transition depicts some event, action or job intended to change state of equipment. As it was mentioned above, function-oriented NPP model focuses on description of the functions performed by the process equipment rather than on the equipment itself. Therefore, in the selected modification of Petri net the place is also used for representation of states of functions, while the transition indicates possible changes of these states (see Fig. 1). Each place of the net can contain no more than one token. Weight of arcs connecting places and transitions is one.

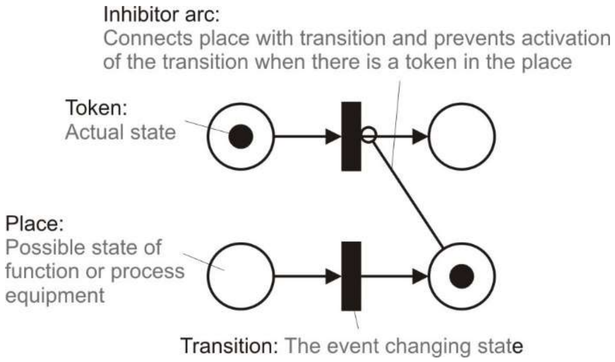

Fig. 1 The used Petri net notation.

Use of multilevel Petri net is explained by hierarchical nature and hierarchical structure of complex systems. In case of hierarchical net, any net can be decomposed to subnets, where each lower level subnet gives detailed description of certain transition of the higher level (parent) net. In other words, the lower level net can be considered as a complex transition in the parent net.

Components of complex system are always connected with each other by various kinds of relationships. The Original Petri net requires introduction of additional places and transitions for representation of such relationships between components of system, which essentially complicates the model. In order to avoid this complication, inhibitory arcs are used in the proposed notation.

As it was mentioned above, Petri net can be used not only for designing of control system, but also for simulation and validation of control algorithms. In this case the net must contain dynamical components. A priority assigned to transition is the first such component. Variation of priorities allows to manage sequence, in which transitions fire, and to test various

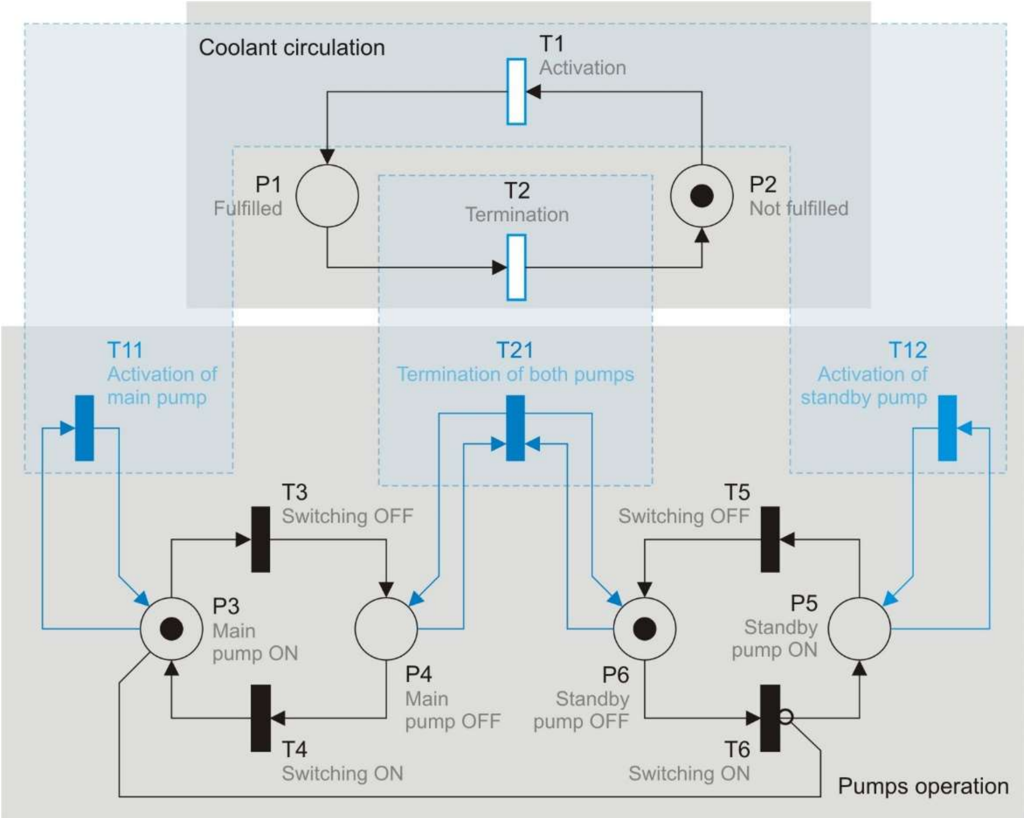

Fig. 2 Example of implementation of the proposed notation.

control scenarios. In real system some time is required for transition of equipment from one state to another. Different equipment requires different time. These delays can be introduced by using of time markers, which allows to evaluate time characteristics of the system.

Let's illustrate the proposed Petri net notation in application to description of behavior of the coolant circulation function. This function provides circulation of water within circulation loop using two pumps. One of the pumps is main while another one is standby. Each pump may be in two states: switched on (activated) or switched off (stopped). To simplify farther description, it is assumed that the function also may have two states: fulfilled or not fulfilled. The function is considered to be fulfilled, if at least one pump is activated. If both pumps are stopped then status of the function is "not fulfilled". The Petri net describing relationships and behavior of the functions and the pumps is shown in Fig. 2. The top level contains the subnet describing behavior of the functions. The states of equipment which have an influence on fulfillment of the function are represented at the lower level.

The coolant circulation function is fulfilled when the main pump is active and the standby pump is stopped. The inhibitory arc prevents activation of the standby pump if the main pump is switched on. In case of the main pump shutdown, the transition T_6 fires and the standby pump is activated, which ensures fulfillment of the coolant circulation function.

In Petri net a situation can occur when there are a few active transitions at the same moment. Transition becomes active (enabled) if each input place of this transition contains required number (at least one) of tokens. Any active transition can fire at next step. Priorities allow to manage the sequence of firing. In case of existence of two or more active competing transitions the higher priority ensures firing of the required one. The priorities of the transitions shown in Fig. 2 are specified in Table 1.

The only T_3 transition is active in initial marking of the net. After shutdown of the main pump the transition T_{21} becomes active with high priority. The transition T_{21} fires and the function switches to the state "no fulfilled". Then the transitions T_4 and T_6 are activated. The start of the standby pump activates the transition T_{12} and the function switches to the state "fulfilled".

The standby pump will stay switched on during all the period of repair of the main pump because of low priority of the transition T_5. After the main pump will have been repaired the transitions T_3 and T_5 will activate. Their fire initiates stopping of the main or standby pump. The reachability graph for the net is shown in Fig. 3.

Table 1 Petri net transitions

Transition	Priority	Description
T_1	Normal	Activation of coolant circulation
T_{11}	High	Activation of main pump
T_{12}	High	Activation of standby pump
T_2	Normal	Termination of coolant circulation
T_{21}	High	Termination of both pumps
T_3	Low	Switching off main pump
T_4	Normal	Switching on main pump
T_5	Low	Switching off standby pump
T_6	Normal	Switching on standby pump

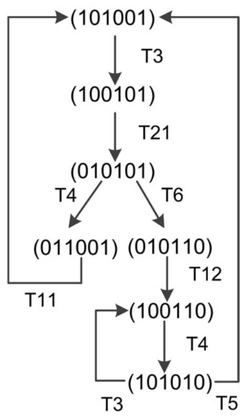

Fig. 3 The reachability graph for the net.

It should be noted that the transitions T_{11}, T_{12} and T_{21} provide "interface" between first and second levels of the net. The transitions T_{11} and T_{12} "explain" operation of the transition T_2.

3 Development of Petri net

This section illustrates the process of Petri net development as a part of function-oriented description for simple process system. The goal of the heat generating system is to provide consumers with heat. The upper level of the functional hierarchy is formed by two abstract functions: heat generation and heat consumption. In order to perform these two functions, it is necessary to transfer heat from the place of production to the place of its supply to consumer. Heat production is conversion of electrical energy into thermal power via tube-type electric heating element (TEHE), the main part of the electric boiler. A pump supplies coolant to the electric boiler where it is heated, washing the electric heater, then it goes further the circulation loop. The transfer of heat to the consumer takes place in the heat exchanger cooled down by some process cooling medium – water, gas or other substance, and then heat is supplied to the consumer (Fig. 4). It is necessary for safety purpose to consider an alternative way (alternative function) of consuming the produced heat if the heat transfer solution prove to be inefficient. A gas cooling blower is used to cool the electric heater. Hierarchy and relationships between functions and equipment are shown in Fig. 5 and 6.

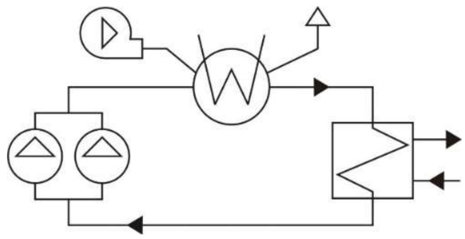
Fig. 4 Process flow chart (mimic diagram) of the system.

Three-level hierarchical Petri net is used for description of the system behavior (Table 2), where each lower level provides additional details for description of heat generating system operation.

Table 2 Petri net levels

Level	Described objects
1	Goal and abstract functions
2	Process functions
3	Subsystems and equipment

The free software CPN Tools supported and distributed by the AIS group (Eindhoven University of Technology, The Netherlands) [10] was used for computer-aided development and testing of the elaborated model.

First (top) level contains the goal and the abstract functions (Fig. 7). The top-level net includes the places depicting the goal and abstract functions and one generalized transition describing operation of the heat generating system. The structure of this transition is specified at the next (lower) level of the net. It should be mentioned that the abstract high-level net

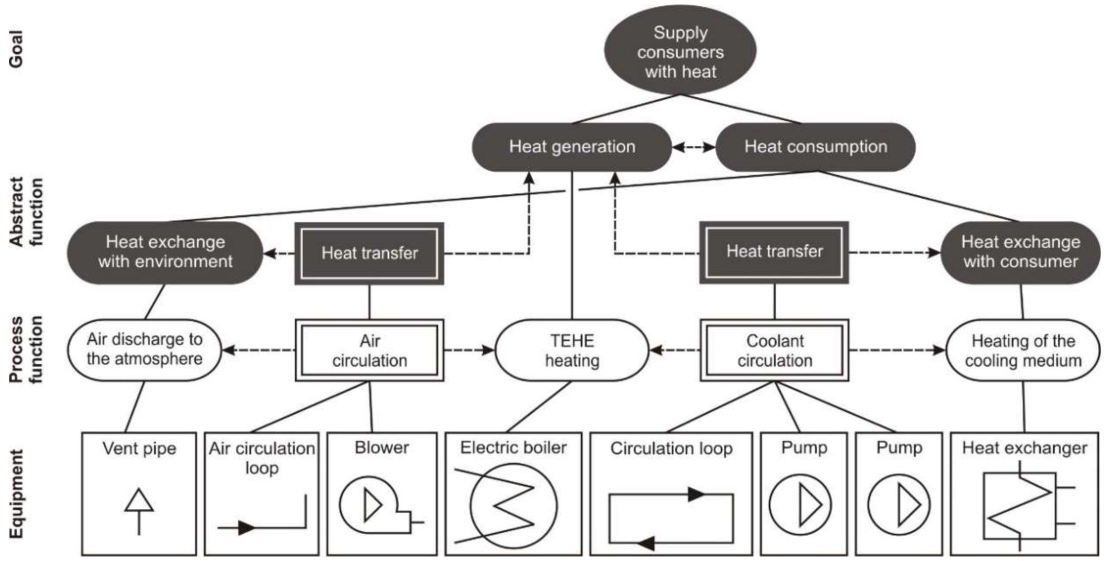

Fig.5 Hierarchy of functions and equipment.

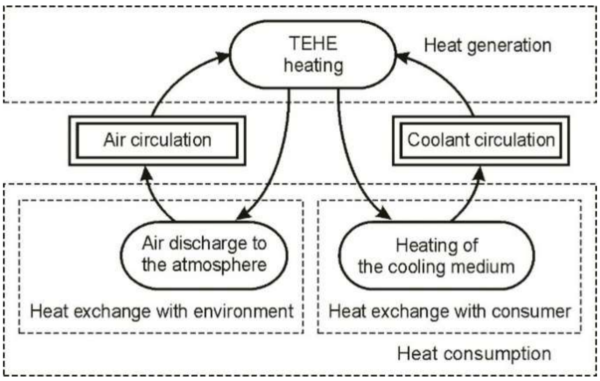

Fig. 6 Network of process functions.

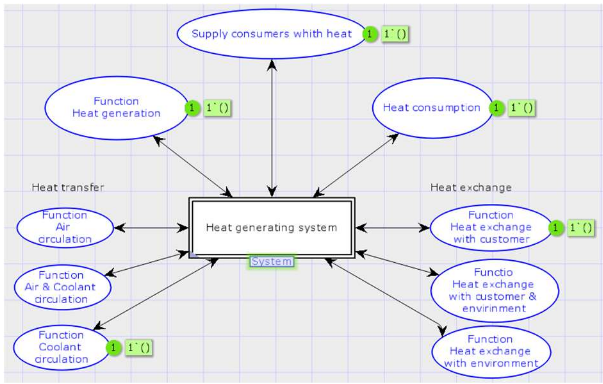

Fig. 7 The goals and abstract functions.

compiled by the used software does not look as a customary Petri net.

State of the net shown in Fig. 7 can be interpreted as followed: the goal “Supply consumer with heat” is achieved; the functions “Heat generation” and “Heat consumption” are fulfilled; the abstract function “Heat transfer” is fulfilled due to process function “Coolant circulation”, the abstract function “Heat exchange” is fulfilled due to process function “Heat exchange with consumer”.

The second level describes behavior of the process functions and their relationships with the abstract functions and goal (Fig. 8). Operation of the systems and equipment ensuring fulfillment of the process functions is simulated at the third level of the net. The example describing operation of the coolant circulation system and shown in Fig. 2 can be considered as a fragment of the third level net.

4 Conclusions

The present paper describes the experience gathered from functional modelling of the process system using the Petri net formalism. Petri net is a potentially power tool which formalizes representation of various information associated with structure, operation and behavior of process system including numerous complicated relationships within complex system. The broad variety of Petri net modifications allows us to select the most convenient type or to combine few types, which makes it possible to integrate various aspects of system operation into one model. The present paper demonstrates the experience in combination of multilevel and inhibitory nets. The review of the published research works revealed that the colored Petri net has the greatest potential for representation of complex algorithms and numerous of states of process system. The colored Petri net also

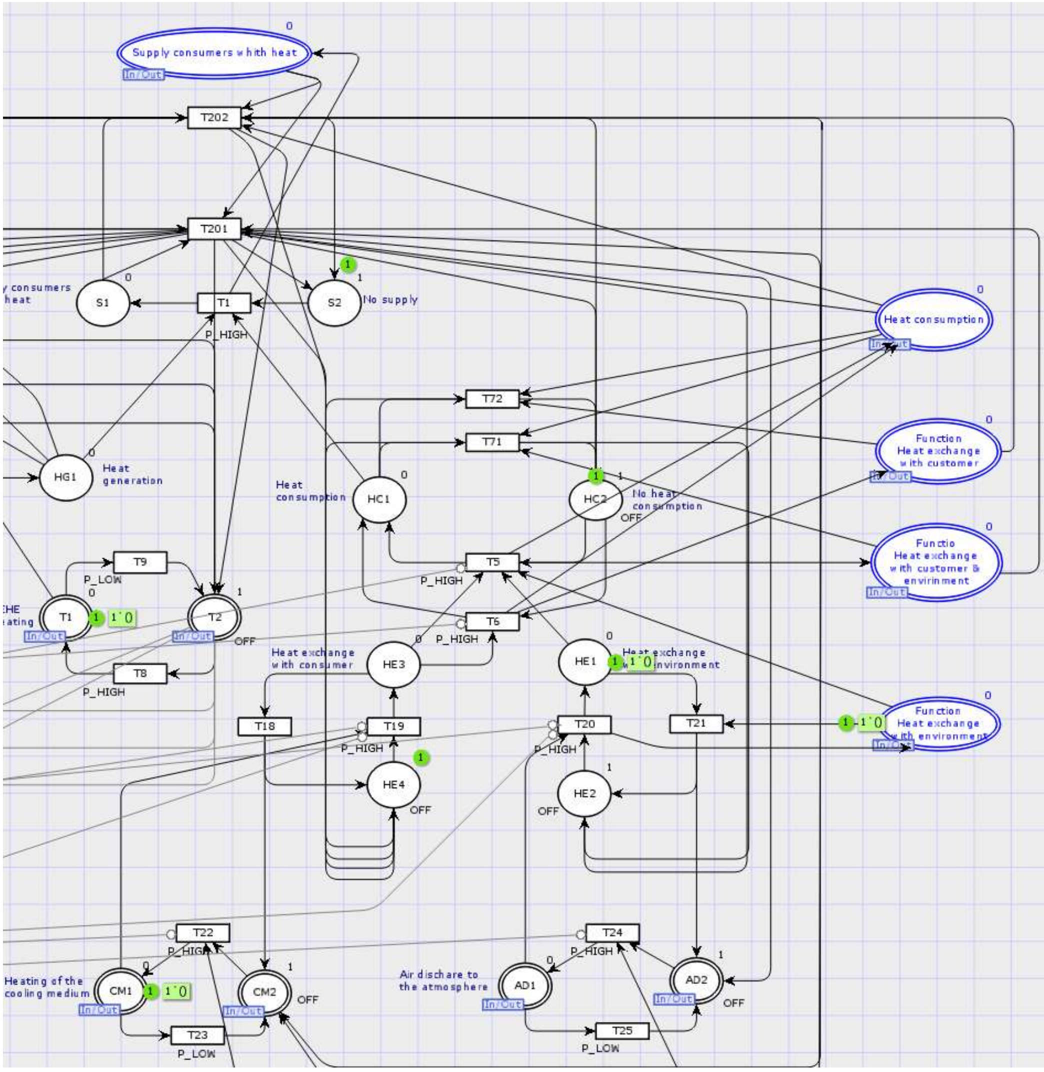

Fig. 8 Fragment of process functions description.

allows to associate certain conditions with transitions and places of net. The transition of component from one state to another when some process parameter overruns setpoint can serve as an example of such condition. Colored Petri nets can be easily integrated with hierarchical approach, which provides good perspectives for their application in functional analysis and design. On the other side, numerous logical conditions associated with colored net don't have graphical representation, which makes the net "non-transparent".

It is evidently, that modelling of real complex system requires much more complicated assumptions as compared with the assumptions accepted in the present paper. For example, only two possible state of function (fulfilled or not fulfilled) are permitted in the described study. More complicated and realistic assumption must take into consideration six states. Active and passive states are the main states of function. Being in passive state the function can be available (i.e. ready to be activated at any moment) or unavailable (unready). Being unavailable the function can be operable or degraded [11].

Nevertheless, the experience acquired during this study allows us to conclude that Petri nets can be used effectively for I&C functional design purpose including development of strictly formalized structural functional model and analysis of this model using full scope or engineering simulator.

References

[1] D. Pirus, "Functional Human-System Interaction for Computerized Operation," Proc. NPIC&HMIT 2004, Columbus, OH, September 19~22, 2004.

[2] A. N. Chernyaev and A. N. Anokhin, "Formalization of the Functional Analysis Methodology to Improve NPP I&C System Design

Process," Proc. NPIC&HMIT'2017, San Francisco, CA, June 11~15, 2017.

[3] ISO/IEC 15909-1:2004 Systems and Software Engineering. High-level Petri Nets. Part 1: Concepts, Definitions and Graphical Notation.

[4] I. A. Lomazova, Nested Petri Nets: Modeling and Analysis of Distributed Systems with Object Structure, Scientific Word, Moscow, 2004.

[5] Petri Nets - Manufacturing and Computer Science, Ed. P. Pawlewski, InTech, 2012; www.intechopen.com/books/petri-nets-manufacturing-and-computer-science.

[6] Petri Nets Applications, Ed. by P. Pawlewski, InTech, 2010; www.intechopen.com/books/petri-nets-application.

[7] T. Murata, "Petri nets: Properties, analysis and applications," Proceedings of the IEEE, Vol. 77, No. 4, pp. 541-580, 1989.

[8] S. A. Kachur and N. V. Shakhova, "Diagnostic system based on condition turbogenerator Petri nets," Izvestia Vysshikh Uchebnykh Zawedeniy. Yadernaya Energetika, No. 1, pp. 13-20, 2016.

[9] A. Voevoda, A. Markov and D. Romannikov, "Software development: software design using UML diagrams and Petri nets for example automated process control system of pumping station," SPIIRAS Proceedings, No. 3 (34), pp. 218-231, 2014.

[10] CPN Tools. AIS Group, Eindhoven University of Technology and the CPN Group, Aarhus University; www.cpntools.org.

[11] A. N. Anokhin, "Structural Approach to Functional Analysis and Design of Main Control Room," Proc. NPIC&HMIT'2009, Knoxville, TN, April 5~9, 2009.