FORMALIZATION OF THE FUNCTIONAL ANALYSIS METHODOLOGY TO IMPROVE NPP I&C SYSTEM DESIGN PROCESS

Alexey Chernyaev and Alexey Anokhin
JSC "Rusatom Automated Control Systems"
25, Ferganskaya street, Moscow, Russia, 109507
AlNChernyaev@rasu.ru; ANAnokhin@rasu.ru

ABSTRACT

Functional analysis is a universal methodology, which is able to support NPP and I&C design process. The paper proposes an approach to combining the functional analysis process and I&C design process into a single I&C functional design process. Operation of a system is considered as a set of functions providing not only the achievement of goal, but also keeping material and energy balances. A notation for graphical representation of semantic network (hierarchy of functions) describing a system is suggested. This network includes four levels, namely functional goals, abstract functions level, process functions level, and equipment level. The elements of the hierarchy are connected by three kinds of relationships, namely: parent-child, main-support, and cause-consequence. Then the semantic network (hierarchy) of functions is converted into a functional network which looks as a directed graph. This graph is used for development of control algorithm and for building of instrumentation and control functions hierarchy. Farther analysis of process functions reveals a set of criteria indicating real-time status and effectiveness of functions. The criteria are used for allocation of instruments and actuators. The process of functional analysis and design is illustrated in application to a simple heat generation system.

Key Words: Functional Analysis, Hierarchy of Functions, Functional Network, I&C Design

1 INTRODUCTION

Functional analysis is an established methodology which allows performing the system design of a complex process facility. In accordance with IEC 61839 the functional analysis is a starting point of NPP I&C system design process. The main task of functional analysis is to identify control functions and allocate them between human and automation. In order to accomplish identification of functions the standard recommends to formulate main functional goals of NPP and to break them into hierarchy of functions which ensure fulfillment of these goals. The lowest level of this hierarchy is constituted by control functions which should be assigned to human or automation.

The standard mentions three types of function when describing the procedure of identification of functions, namely: *goals* (sub-goals), *plant functions* and *control functions*. A control function is defined as a set of control actions performed by human or machines for the accomplishment of a functional goal including the related information acquisition and processing. The other terms (including a plant function) are not defined clearly in the standard, however there are two remarks clarifying their meaning: 1) the terms "goal" and "function" are interchangeable, 2) higher levels of the hierarchy reflect a plant design concept and are better expressed in terms of goals while at lower levels it is more appropriate to refer to a function as an activity performed by a human or automated system.

In accordance with IEC 61513 I&C functions and functional requirements identified during functional analysis constitute a basis for designing I&C architecture. Thus it can be affirmed that functional analysis is a universal methodology ensuring implementation of systematic (functional) approach when designing of an NPP and its components, including I&C and control rooms. Firstly, the

functional analysis allows making sure that the NPP design has taken into account everything to achieve the goal of NPP operation, i.e. safe power generation. Secondly, a huge amount of data is collected and analyzed during functional analysis to solve all subsequent tasks during design of control algorithms, human-machine interface, procedures etc. Thirdly, functional analysis may contribute to building an adequate control system using a functional approach to control process, i.e. to control of the status of functions instead of control of the status equipment.

However, these capabilities are not yet completely implemented during NPP I&C design and functional analysis itself is not clearly and formally described, so an actual benefit of functional analysis is often disproportionate to an effort and time spent to perform it.

As of today, some experience in implementation of functional analysis during I&C design has been already accumulated in the Russian NPP projects. The first experience was obtained in design of Tianwan NPP in cooperation with Siemens [1]. The subsequent projects contributed to development and improvement of functional analysis methodology according to which the power generation process shall be divided into seven functional domains, namely: K – Power and fluid supply, B – Waste treatment and disposal, ٧ – Heat removal to ultimate heat sink, D – Secondary circuit, E – Reactor cooling system, F – Turbine-generator unit, G – Balance-of-plant and off-site systems. Then each domain shall be divided into functional sub-domains. For example, Domain E shall be divided into the following sub-domains: E1 – safety systems that provide Level 3a safety functions; E2 – safety related normal operation systems; E3 – reactor cooling system; E4 – safety systems and safety related normal operation systems that provide severe accident management. The functional groups of equipment shall be defined on the next level of functional division. Then each functional group of equipment is considered as an object of 'functional group control'. For example, the functional sub-domain E4 shall be divided into a passive heat removal system through steam generators, a passive heat removal system from the containment and a molten core catcher [2], each is a functional group control object. Then the functional group control level shall be decomposed to individual control functions.

Thus the functional division of NPP process as well as division of the control functions in the Russian projects includes four levels: functional domains, functional sub-domains, functional groups, and control functions. However, the main drawback of this approach and other approaches described in standards and publications is a lack of formalized technique of functional analysis. The above mentioned approach is not able to fully answer the questions such as "Why is the process and control process divided into seven domains?", "How is the goal of control achieved", "How to develop a control algorithm?"

We consider the potential of functional analysis is huge and is not limited to assignment of control functions to human and automation. Functional analysis is a universal methodology, which is able to support in building of NPP process structure, to define the scope of equipment, to ensure observability and controllability of the process, to develop control algorithms and much more. The paper proposes an approach to combining the functional analysis process and I&C design process into a single I&C functional design process. To achieve this, the main concepts of the functional analysis shall be formalized, structured and illustrated by an example of I&C functional design process implementation in a relatively simple process object.

2 I&C FUNCTIONAL DESIGN METHODOLOGY

2.1 Hierarchy of Functions

Hierarchy of functions described in IEC standard is rather simple but weakly structured that prevents from strict formalization of functional analysis procedure.

More complex approach to building a hierarchy of functions (i.e. a multi-layered network) is developed by K. Vicente [3] within the methodology called Cognitive Work Analysis. This methodology establishes the structure of complex system study to ensure effective interaction with the user. The

foundation of CWA was laid by J. Rasmussen [4], who suggested describing the work domain in a form of abstraction hierarchy. Abstraction hierarchy forms the basis for the method of Work Domain Analysis, which serves as a starting point of the CWA methodology.

The Abstraction Hierarchy is a derivative of an engineering technique called Functional Decomposition of a system [5]. The hierarchy starts from definition of *functional purposes* which have to be achieved by the system under consideration. Next level consists of *abstract functions* providing accomplishment of the purposes and describing the causal relationships underlying the work domain. Usually abstract functions are described in terms of the laws of physics, such as mass and energy transformation. At the third level an analyst should identify device-independent *generalized functions* explaining how the abstract functions can be accomplished. Then, at the fourth level, *physical functions* (in other words, process mediums (e.g., gas, steam, water), equipment (tank, heat exchanger, etc.) and its capabilities) providing fulfillment of generalized functions should be identified. The Bottom, lowest level of the hierarchy represents description of *physical form* of that equipment in terms of size, shape, color, location and conditions.

Various authors use several types of abstraction hierarchy. T. Xiao et al. [6] suggested describing a system at the following five levels: 1) domain purposes, 2) domain priorities, 3) domain functions, 4) physical functions, 5) physical object and configurations. Similar structure is described by G. Lintern in [7] where the following levels of hierarchy are suggested: 1) system purposes, 2) domain values, 3) domain functions, 4) technical functions, 5) physical resources and material configurations. The main peculiarity of this hierarchy is that the second level contains domain values, i.e. constraints that encapsulate human and social values (e.g., safety-productivity) and thereby constrain the space of acceptable action.

In addition to abstraction hierarchy G. Jamieson and K. Vicente described in [8] six types of process functions: *source*, *sink*, *store*, *balance*, *transport*, and *barrier*. Typification of process functions facilitates transfer from abstract level of system description to physical objects and to the specific equipment. Comparison of various methods of functional decomposition is given in [9].

We suggest using the simplified (in comparison with [5]) 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 next 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. In fact NPP operation is interaction of process functions.

Process and abstract functions are divided into two classes: *main* and *support* functions. Main function is a function aimed at achieving the goal and/or ensuring material and energy balance. Support function is a function which is not directly connected with the goal and intended for creating conditions of the main functions implementation. The example of abstract support function is heat transfer from a generator to a consumer. In other words, this function connects the functions of heat generation and heat consumption. Each process function is performed by specific *process equipment* (e.g., pumps, heat exchangers, pipelines, etc.), forming the lower level of functional hierarchy. Selection and design of this equipment is the final step of functional design of system. Functions requiring enhanced reliability shall be performed by redundant equipment, including redundant equipment based on other physical principles (diversity principle).

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 higher level is implemented as well as the means

providing its implementation. The *functional relationships* are established between two functions and demonstrate that one function initiates performing the other one.

Goals, abstract functions, process functions, main-support, parent-child and functional relationships form a four-layer semantic network. Graphic notation of this network is given in Fig. 1.

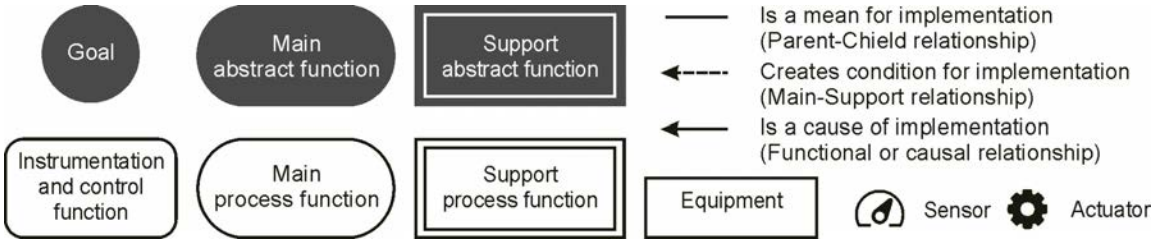

Figure 1. Elements of graphic notation of semantic network describing a system.

2.2 Functional Network and Control Algorithm

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. Unaware of such connections we cannot say anything about how these functions affect each other and in which sequence they are implemented. It is impossible to proceed from functional description of a plant to functional description of a control system, as well as to specification of tasks, algorithms and control criteria without this knowledge.

Let's convert a semantic network (hierarchy) of functions 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 (Fig. 1). Process functions can be visually combined in groups corresponding to functions of higher level. The list of possible states and the set of parameters based on which the state can be assessed should be defined for each function. In the simplest case a function state can be based on a combination of two indicators: activity of function (activated, not activated) and fulfillment of (fulfilled, not fulfilled) [9]. If a function state is defined by its fulfillment, these fulfillment criteria shall be established.

Arrows (causal relationship) can be described in two ways: 1) in terms of dependencies of function discrete states (e.g., function A shall be fulfilled for function B actuation, or function A shall be in state A_j for transfer of function B to state B_i); 2) in terms of a balance ratio (in a form of dependence of parameter x_B characterizing the state of function B on parameter x_A characterizing the state of function A: $x_B=f(x_A)$).

The graph includes cycles; each cycle forms a closed loop of operation. Such presentation allows developing an algorithm of a process object control. Control includes sequential actuation of functions forming the loop and finally activation of the whole loop (cycle) of graph. Selection of control loop can be based on weight coefficients. Detailed description of control algorithm can be performed by means of Petri nets [10], but it is beyond the scope of this article. Functional approach to control process described in [11] can be implemented by using such algorithm.

2.3 Instrumentation and Control Functions and Facilities

Process control system must ensure observability and controllability of the process, which is provided by sensors, actuators and equipment allowing configuring the process. At the first stage Instrumentation and Control Functions (I&C function) are defined, after that they are assigned to human and automation.

I&C functions shall be provided for all the process and abstract functions which shall be observed (monitored) and controlled. I&C functions are interconnected by cause-consequences relations while the functional network of process functions is used as the basis for generating the network of I&C functions. I&C functions of the lower level are connected with process equipment and form control loops. Each of the lower level loops consists of instrumentation tools (sensors and data transmission channels), control facility performing this I&C function (for instance, automatic controller, computers, operator, human-machine interface), and actuators implementing control actions. Similar to the process functions network, cycles forming control loops are also presented in the I&C functions network.

The generated I&C functions network allows proceeding to I&C functional structure, assigning I&C functions to human and automation and designing control algorithms.

The basis of control algorithms design is the necessity of closing the control loop by its maximum length. Thus closed loop with maximum length corresponds to achieving the goal of control.

Generally each I&C function has two inputs and two outputs. A control task arrives to I&C function input from the upper level while feedback comes from the lower level. The function outputs are feedback on function execution result, received at the upper level of control, and the control action (or control task) transferred to the function of the lower level of control. Thus, it is fair to say that one I&C function can only participate simultaneously in two control loops. One control loop shall connect the I&C function with the lower level, and the other loop – with the upper level of control.

In some particular cases a I&C function can participate in many more control loops. Weights can be assigned for competing control loops for the purpose of making choice when implementing the control algorithm. Due to these weights two loops by which control will be performed are selected. It is important to emphasize that in case of such an approach the lower loop will always be the regulation loop while the upper level will be the control loop. For the regulation loop the goal of control is to reduce the controlled parameter deviation to zero while for the control loop the goal of control is to generate a control task.

In some cases an I&C function may have only one input and one output. This means that during I&C design these functions can be integrated with upper level functions towards to optimization of I&C system.

2.4 Methodology of I&C Functional Design

As a result of generalizing the actions described above the following process of designing process object and control system can be suggested.

1. The goal hierarchy is built, main and auxiliary abstract and process functions ensuring the achievement of these goals are defined.
2. For performing each process function particular process equipment is selected (or designed). A four-layer (four-level) semantic network is generated.
3. Functional redundancy and diversity are implemented, after which this semantic network is corrected.
4. A functional network defining the cause-consequence relations between process functions is generated.
5. Indexes and criteria of process functions state are defined; cause-consequence relationships (dependencies) between them are described.
6. Sensors and actuators as well as equipment allowing process configuration are defined on the basis of the list of criteria and process functions state indicators.
7. I&C functions network comprising closed control loops is generated.
8. Mathematical models of process equipment and control processes are developed.
9. Further on I&C design including human factor engineering is performed.

3 CASE STUDY

3.1 Building the Functions Hierarchy and Functional Design of the Technological System

Let us consider the functional design process of the technological system and I&C using a simple example. The heat generating system that supplies consumers with heat is considered as a designed system. So, the goal of the 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 successfully it is necessary to transfer heat from the place of production to the place of its transfer to the consumer. Further, we shall describe the process functions ensuring the technology implementing these abstract functions.

The use of a closed-loop coolant is a conventional technology of building such systems. Heat production, in this case, is conversion of electrical energy into thermal power via tube-type electric heating element (TEHE), the main part of the electric boiler. K 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. 2). The process equipment selected to perform the process functions is integrated into the process flow chart (Fig. 3, on the left).

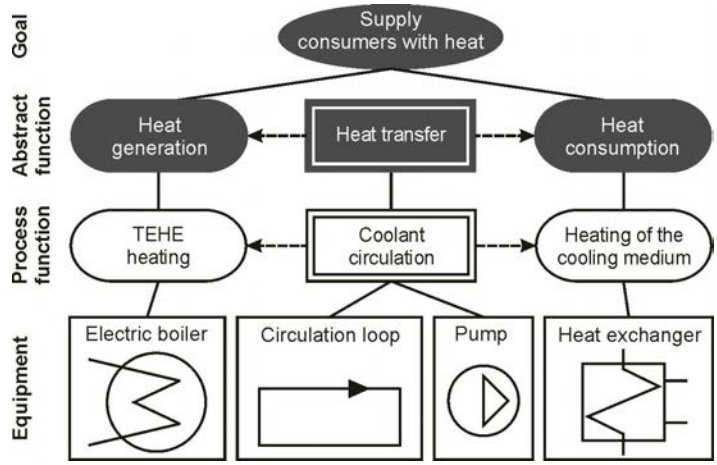

Figure 2. Hierarchy of functions.

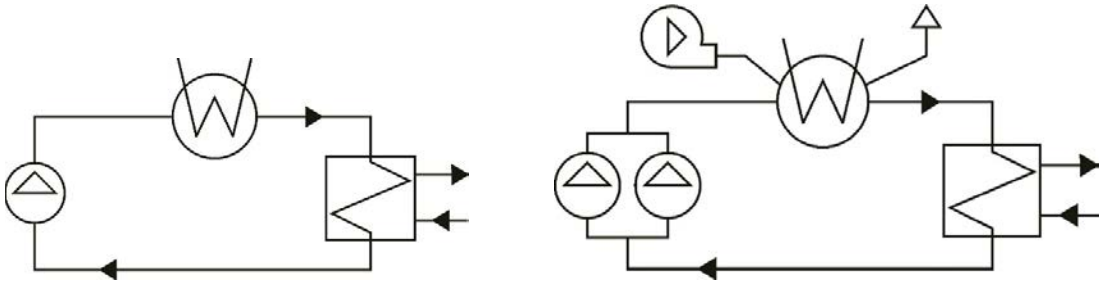

Figure 3. Process flow chart (mimic diagram) of the system.

The electric boiler is the most vulnerable element in this system. The impairment of a heat transfer function and, as a consequence, a heat consumption function breaks the thermal balance in the system and results in overheating and damage of the boiler's heating element. Prevention of this event is essential to the safe operation of the designed system. A pump failure can be a cause of the heat transfer disorder. The problem can be prevented by adding a redundant pump.

It is necessary to consider an alternative way (alternative function) of consuming the produced heat if the heat transfer solution prove to be inefficient. For example, a gas cooling blower can be used to cool the electric heater. Bringing this process function into operation increases the system reliability and ensures the implementation of the diversity principle as well.

The function hierarchy formed by implementing redundancy and ensuring the safety is given in upper part of Fig. 5, and the equipment process flow chart is given on the right of Fig. 3.

3.2 Building the Functional Network

Upper level functional network consists of abstract functions that form the cycle (closed loop) implementation of which ensures energy balance between heat production and consumption (Fig. 4). Taking into account redundancy and diversity implemented, heat consumption can be performed in two ways: as the result of heat exchange with the consumer and heat exchange with the environment. Heat production can be performed by actuation any of these loops, however the right loop is more preferable and has a higher weight. There is no need of heat consumption when the heat production is stopped.

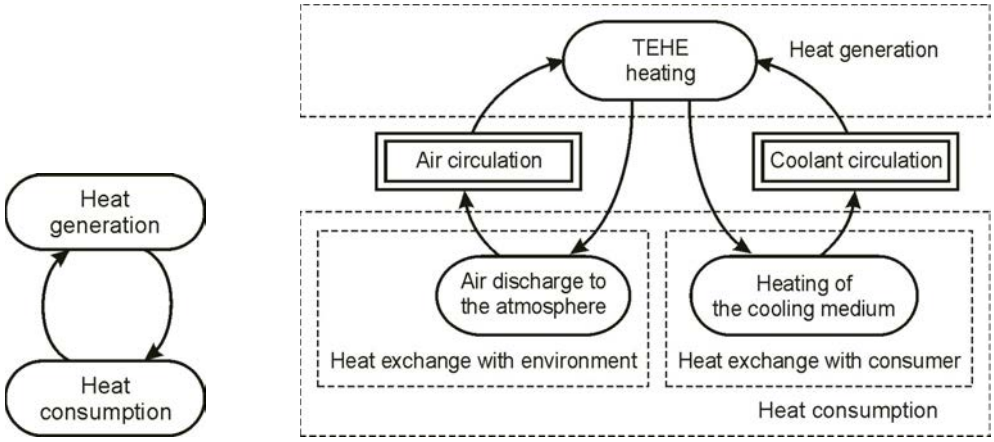

Figure 4. Upper level (on the left) and full (on the right) network of process functions.

The process functions network is built on the basis of the following assumptions:

- heating of the electric heater makes it necessary to remove heat by heating the cooling medium through the heat exchanger or dumping heat to the atmosphere;
- the coolant circulation shall be started for heat exchange, and air circulation shall be started for dumping heat to the environment;
- coolant or air circulation is a required condition for heating the electric heater (TEHE).

Performance criteria of the functions implementation are the following (the given values are used only as an example and are not based on any thermohydraulic calculation):

- the function of TEHE heating is fulfilled when electric current is from 10 to 80 A;
- the function of coolant circulation is effective when the coolant pressure before the electric boiler ensures that the boiling point is at least 15 °C more than the coolant temperature after the electric boiler (for example, pressure shall not be lower than 1.8 MPa when the coolant temperature is 180 °C), the coolant flow at the inlet of the electric boiler is at least 20 kg/s, the coolant flow is proportional to the TEHE electric current, the coolant temperature after the electric boiler does not exceed 180 °C, TEHE temperature does not exceed 240 °C;

- the function of cooling medium heating is fulfilled when the medium temperature at the outlet of the heat exchanger is not more than 20 °C lower than the coolant temperature at the outlet of the electric boiler, the coolant temperature at the outlet of the heat exchanger is 60–80 °C lower than TEHE temperature;

Certain additional conditions can be used along with the effectiveness criteria to estimate the status of functions. For example, the status of the coolant circulation function is identified based on the following additional conditions:

- the function is active when one pump is on and another one is in standby mode;
- the function is fulfilled when a boiling margin is maintained at the level of 30 °C;
- reliability of the function is threatened when the second pump is under repair (i.e. the standby pump is out of service).

3.3 Building Control System Elements

The network of I&C functions is shown in Fig. 5. The network of I&C functions practically mirrors the network of process functions. It should be noted that air dump into the atmosphere is carried out through a ventilation pipe which is not equipped with instrumentation and control facilities. Nonetheless, the process function of air vent into the atmosphere corresponds to a fictitious I&C function shown in the diagram by a dashed line.

Performance of each lower level I&C function starts from monitoring process parameters. These parameters should ensure observability of performance indexes (criteria) and conditions that characterize the state of a controlled process (or abstract) function. Considering the above criteria and conditions the following list of the monitored parameters can be made for the example discussed (Fig. 6): the current through the tube-type electric heater (A), the temperature of the tube-type electric heater (T1), the coolant temperature at the outlet of the boiler (T2), the coolant temperature at the outlet of the heat exchanger (T3), the temperature of the process medium at the outlet of the heat exchanger (Ǒ4), the coolant pressure before the boiler (P2), the coolant flow at the inlet to the boiler (G), the state of each pump (on / off, ready / not ready), the state of gas blower (on / off, ready / not ready).

As equipment to ensure the controllability of the system and implementation of control actions, in addition to actuators (such as potentiometers for controlling the current through the TEHE, switches for activation of pump and gas blowers, etc.) the following shall be provided:

- to control the coolant circulation – flow regulating valve at the inlet of the boiler,
- to control heat removal – flow regulating valve at the process medium supply line into the heat exchanger from the consumer side.

Considering the additional process equipment the list of parameters prepared earlier shall be supplemented with information on the position of each of the two regulating valve (0–100 %).

4 DISCUSSION

The main idea of this paper was to develop an algorithm formalizing functional design of both I&C and a technological system. Functional design consists in transition from the goal to a hierarchy of functions providing accomplishment of this goal. Being applied to designing of a system, functional design consists in building of a hierarchy of process functions followed by specification of equipment. In terms of I&C, functional design consists in identification of I&C functions, their allocation between human and automatics, developing I&C architecture and implementing its elements, including HMI, control stations, automatic controls and so on.

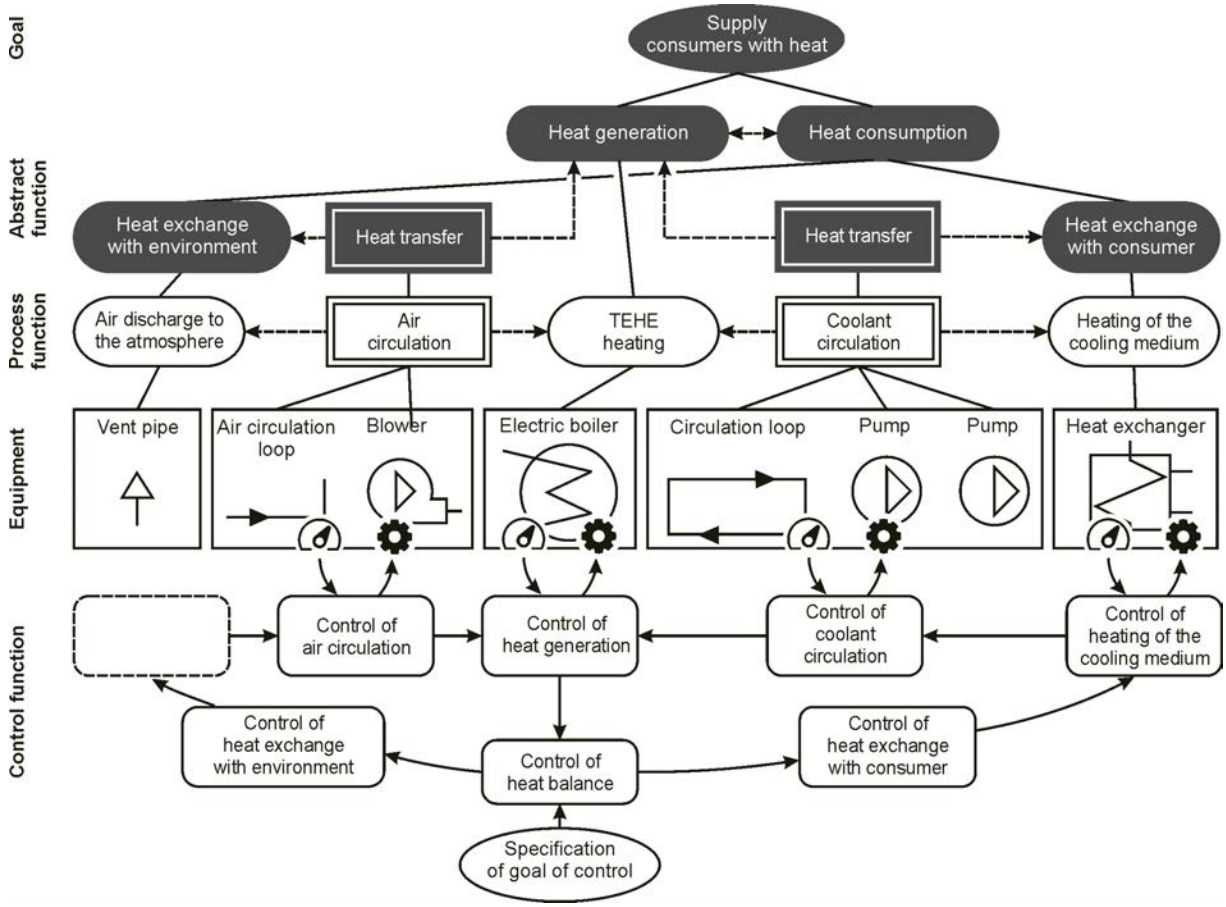

Figure 5. Hierarchy of process and control functions.

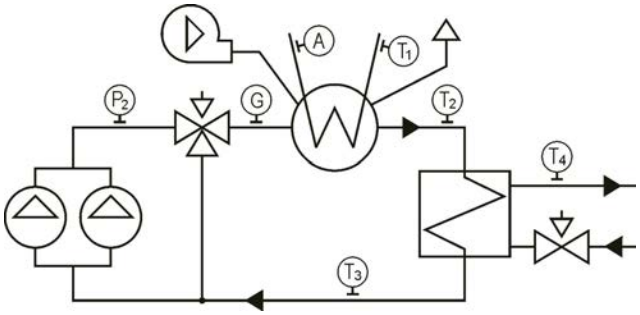

Figure 6. Instruments allocation.

All those stages are well known. Nonetheless, the vast majority of design solutions are developed either based on the experience accumulated from the previous projects, or using heuristics, formulated by the designer. The problem is that, for proper step-by-step implementing of functional design procedures we shall have to clearly define what data shall be accumulated at each preceding stage, in what form that data should be represented and stored and how they will be used and converted at a later stage. In addition, we shall have criteria of completion and quality of each stage.

To increase the rigor of this process, we propose to consider operation of a system as a set of functions providing not only the achievement of goal, but also keeping material and energy balances, such as “heat production – heat consumption”, “loss of coolant – make up of coolant”. In this case, appearance

of some function disrupting balance requires implementation of another counter-function restoring disrupted balance. Ensuring balance can be a quality criterion (and a completion criterion) of a transition from the goal to abstract functions and from abstract functions to process ones.

However, the only criterion of ensuring balance does not allow to completely get rid of functional design heuristics. The proposed procedure and notation for formalization of functional analysis and design result presentation partially solves the problem of a more rigorous transition from a stage to a stage. However, this does not eliminate the large variability of possible solutions. Using the same logic it is possible to build many variants of a semantic network. In addition, for a more detailed description it is necessary to develop a detailed classification of functions (as is done in [8]), and learn to combine description of discrete control processes and regulation processes.

In the end, any methodology of structural modeling similar to the one proposed in this paper works well on simple examples. All the same, with scale growth and transition from tens of functions to hundreds and even thousands a description stops being conceivable and hence, heuristic analysis and validation become impossible. To make that possible mathematical formalization of a structural model and its analysis procedures are needed. Application of Petri nets is just one of approaches to solving this task.

REFERENCES

1. V. N. Osetskij, "Osobennosti i opyt proektirovaniya ASU TP na AES Tianwan (Specific Features and Experience Gathered from Designing of I&C System for NPP Tianwan)," *Materials of the ASE workshop on Designing of I&C for Abroad Constructed Russian Design NPPs*, Moscow, Russia, March 2006, URL: http://www.proatom.ru/modules.php?file=article&name=News&sid=958 (2006) (in Russian).

2. A. M. Kazarin, A. V. Molchanov, G. A. Ershov, "Today's Nuclear Power Plants – Requirements and Implementation Options," *Trans. 9th Conf. on Safety Assurance of NPP with VVER*, Podolsk, Russia, May 19–22, 2015, OKB "Gidropress" (2015) (in Russian).

3. K. J. Vicente, *Cognitive Work Analysis: Towards Safe, Productive, and Healthy Computer-Based Work*, Lawrence Erlbaum Associates, Inc., Mahwah, NJ (1999).

4. J. Rasmussen, "The role of hierarchical knowledge representation in decision making and system management," *IEEE Trans. on Systems, Man and Cybernetics*, **15**, pp. 234–243 (1985).

5. C. M. Burns, J. R. Hajdukiewicz, *Ecological Interface Design*, CRC Press, Boca Raton, FL (2004).

6. T. Xiao, P. M. Sanderson, M. Mooij, S. Fothergill, "Work Domain Analysis for Assessing Simulated Worlds for ATC Studies," *Proc. HFES 52nd Annual Meeting*, New York, September 22–26, 2008, pp. 277–281 (2008).

7. G. Lintern, "Work Domain Analysis," http://www.cognitivesystemsdesign.net/Tutorials/Work%20Domain%20Analysis%20Brief%20(wildfires).pdf (2017).

8. G. A. Jamieson, K. J. Vicente, "Modeling Techniques to Support Abnormal Situation Management in the Petrochemical Processing Industry," *Proc. CSME Symp. on Industrial Engineering and Management*, Toronto, Ontario, Canada, May 19–22, 1998, pp. 249–256, CSME (1998).

9. A. N. Anokhin, "Structural Approach to Functional Analysis and Design of Main Control Room," *Proc. NPIC&HMIT'2009*, Knoxville, TN, April 5–9, 2009, pp. 2484–2495, American Nuclear Society (2009) (CD ROM).

10. V. E. Kotov, *Seti Petri* (Petri Nets), Nauka, Moscow (1984) (in Russian).

11. D. Pirus, "Functional Human-System Interaction for Computerized Operation," *Proc. NPIC& HMIT 2004*, Columbus, OH, September 19–22, 2004, American Nuclear Society (2004) (CD ROM).