The Equipment Qualification Testing Framework: Model Driven Development for Design and Model-Based Testing for Verification

VLADIMIR SKLYAR[1], VYACHESLAV KHARCHENKO[1,2]
[1]National Aerospace University "KhAI"
Computer Systems and Networks Department
Kharkiv, UKRAINE
[2]Centre for Safety Infrastructure Oriented Research and Analysis
RPC Radiy, Kropyvnytskyi
UKRAINE

Abstract: Computer control systems (CCS) are an important for operation and maintenance of safety- critical infrastructures. A challenge in such systems implementation is certification and licensing against national and international regulatory requirements. Environmental tests are applied to check that equipment of the CCS can withstand the rigors of harsh environments, for example high and low temperature and humidity, water drops and dust, seismic vibration and acceleration, electromagnetic interference, radiation, etc. It can happen that environmental tests emphasis is methods, level and types of environmental impacts, but there is a question about functions which shall perform a system under test before, during and after test impact application. Equipment Qualification Testing Framework is proposed. The requirements to system operation under test is described in view of a model. Model Driven Development methodology is applied for design and Model-based Testing methodology is applied for verification.

Key-Words: - Computer Control Systems, safety critical infrastructures, qualification testing framework, system verification

Received: May 4, 2020. Revised: October 15, 2020, Accepted: November 5, 2020. Published: November 20, 2020.

1. Introduction

Computer-based Control Systems (CCS) play an important role in safety-and security assurance of critical applications and infrastructures. At the present time there some types of CCS such as Embedded Systems (ES), Industrial Control Systems (ICS), Internet of Things (IoT) taking into account Device Layer, as well as Industrial Internet of Things (IIoT) which can be considered as some specific architecture different from typical IoT [1,2].

There are rigorous requirement to safety and security of CCSs performing critical functions. Such requirements are documented in national and international standards [3,4]. The most part of CCS safety and security related standards contain requirements to safety and security life cycle (SSLC) with comprehensive review, analysis and testing at each of the life cycle stage. The final stage of typical SSLC is validation testing of integrated product against requirements of the specification. Validation includes the following two types of tests: functional tests and environmental tests. During functional testing a product (integrated CCS or some separated its parts) operates in accordance with functional specification. 100% of functional tests coverage shall be achieved [5].

Environmental tests are applied to check that equipment of the CCS can withstand the rigors of harsh environments, for example high and low temperature and humidity, water drops and dust, seismic vibration and acceleration, electromagnetic interference, radiation, etc. Environmental tests are often named as Equipment Qualification (EQ) tests, so will use this term in the paper [6,7]. Usually test team is focused on methods, level and types of environmental impacts but is still a question: which functions shall perform a System under Test (SUT) before, during and after test impact application? To answer the above question we propose EQ Testing Framework (see Fig. 1).

To be more specific we will consider a Programmable Logic Controller (PLC) as a SUT. We make this assumption because PLCs are the most complicated hardware-software parts of CCS, for example FPGA-based Instrumentation and Control System of NPP [4,5]. The same approach can be

applied for other types of CCS and their parts. Also we consider PLCs as generic platforms for design of applications. It is needed to note the Qualification Test Specimen (QTS) shall contain a representative set of parts of the developed system and shall perform some representative set of functions.

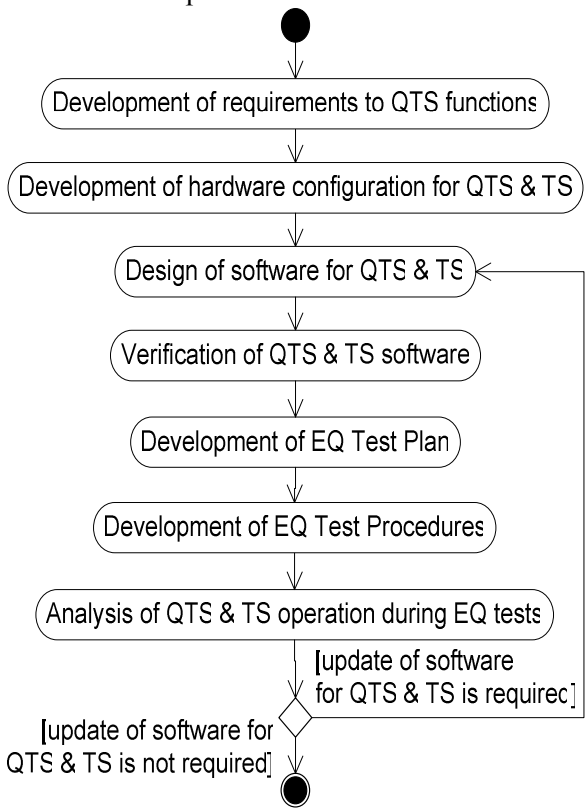

Fig. 1. Sequence of actions in the EQ Testing Framework (UML activity diagram).

To develop the EQ Testing Framework we attack the following issues in this paper:

- Firstly, an approach to check functionality of the QTS is proposed. For that, choice and development of requirements to the QTS functions should be performed. Since some EQ tests are destructive, the QTS is a separated product which cannot be supplied to clients. We suggest to develop these requirements in a view of model to implement below Model Driven Development (MDD) [9].
- Development of hardware configuration for the QTS and for the Test System (TS).
- Design of software (as named control logic) for the QTS and the TS. It should be noted that once developed software can be used in different projects and for various types of environmental tests.
- Verification of the QTS & TS software. Below we discuss an approach to use of Model-based Testing (MBT) for verification [10].
- Development of EQ Test Plan (EQTP), which is a general plan for environmental testing.
- Development of EQ Test (EQT) Procedures for specific types of testing such us temperature, humidity, vibration, electromagnetic and other tests. Thus, the development of plans and procedures for EQ testing is carried out in conjunction with the design of the QTS and the TS.
- Analysis of QTS & TS operation during EQ tests performance. Depending on the type of testing, the requirements to the functioning of the QTS and the TS may be updated. In some cases that may lead to some software correction. In this case a return to the previous activity (Design of software for QTS & TS) should be performed.

So the main objective of the paper is to develop EQ Testing Framework, which can be applied as a generic methodology for any type of CCSs or their hardware.

2. Parts and Control Logic of the Qualification Test Specimen and the Test System

2.1 Development of requirements to functions of the Qualification Test Specimen

What are not clearly defined in the standards are the requirements for the functioning of the SUT and the QTS before, during and after of the delivery of extreme test impacts. At the same time, customers expect a detailed description for the functions performed by the equipment. In addition, it is necessary to identify a normative document that can be referred concerned sufficient functionality of the QTS.

We propose to refer the document of the U.S. Electrical Power Research Institute (EPRI) called EPRI TR-107330 “General Specification of Requirements for the Qualification of Commercial PLCs for Safety-Related Applications at Nuclear Power Plants”. The EPRI TR-107330 was used for certification purposes by such leading manufacturers of CCS equipment as Siemens, Rolls-Royce, Toshiba, Mitsubishi, Schneider Electric (formerly Invensys), ABB, Westinghouse, Doosan. As it is known, nuclear industry demands high requirements to the CCSs. Also the EPRI TR-107330 is only one reference in the field of requirements to PLCs functionality during EQ testing. We will discuss details of the EPRI TR-107330 below considering software design of the QTS and the TS.

2.2 Methodologies of Model Driven Development and Model-based Testing

We describe requirements to the QTS operation in view of a model, so MBD methodology can be applied for design and MBT methodology can be applied for verification. MDD is an approach to design software and computer systems when core documented

artefacts, requirements or architecture are described with formal (for example, VDM, Z, B, etc.) or semi-formal diagrammatic (for example, UML, SysML, etc.) [9].

At the same time, it is possible to extract test cases from the model to validate conformance of intermediate and final products with this model. For safety- and security-critical systems we often meet the requirements to produce test plan after requirement specification.

MBT can support this issue since test cases and scenarios are extracted from a model before a CCS is integrated and all hardware and software components are produced. Also early functional test design is able to reveal inconsistency in the requirement specification as well as to evaluate requirements testability. One more MBT benefit is a potential to improve test efficiency from the point of view of time and human resources consuming [10]. Both MDD and MBT propose a good base for test automation.

For PLC it is possible to use a graphical Functional Block Diagram (FBD) language, which can support both MDD and MBT methodologies.

2.3 Development of hardware configuration for the Qualification Test Specimen and the Test System

Let's consider a minimal configuration of the PLC-based QTS, which performs functions of receiving, logic processing and generation of analog and discrete signals (see Fig. 2). We assume that the conversion of AC voltage to DC is carried out outside the PLC, and the PLC has two redundant 24 VDC inputs.

The discussed QTS includes the following parts [8]:

- The chassis that performs the functions of module disposal, providing power and communications to the modules, and also connecting the signal cables through a backplane.
- The Logic Control Module (LCM), which performs all the computational and logic functions. The LCM has an unidirectional Ethernet port for transmission of plant and monitoring data to the workstation.
- The Analog Input Module (AIM) performs processing of 16 analog input signals. Each of the 16 input port can be configured to receive 0-5 V voltage signal or 4-20 mA current signal.
- The Discrete Input Module (DIM) performs processing of 16 discrete input signals with ON state at a voltage value of 24 V.
- The Analog Output Module (AOM) generates 16 analog output signals. Each of the 16 output ports can be configured to provide 0-5 V voltage signal or 4-20 mA current signal.
- The Discrete Output Module (DOM) generates 16 discrete output signals with ON state at a voltage value of 24 V.

The TS includes a PLC that is able to generate input signals for the QTS and process output signals for the QTS like "mirror" (TS outputs – QTS inputs and TS inputs – QTS outputs). National Instruments company equipment operating under LabView software can be used as a core of the TS. The PLC of the TS is connected to the QTS using signal cables and terminal blocks. The TS also includes Data Acquisition System (DAS) which is a workstation that receives plant and diagnostics data through the Ethernet network, both from the QTS and from the PLC of the TS.

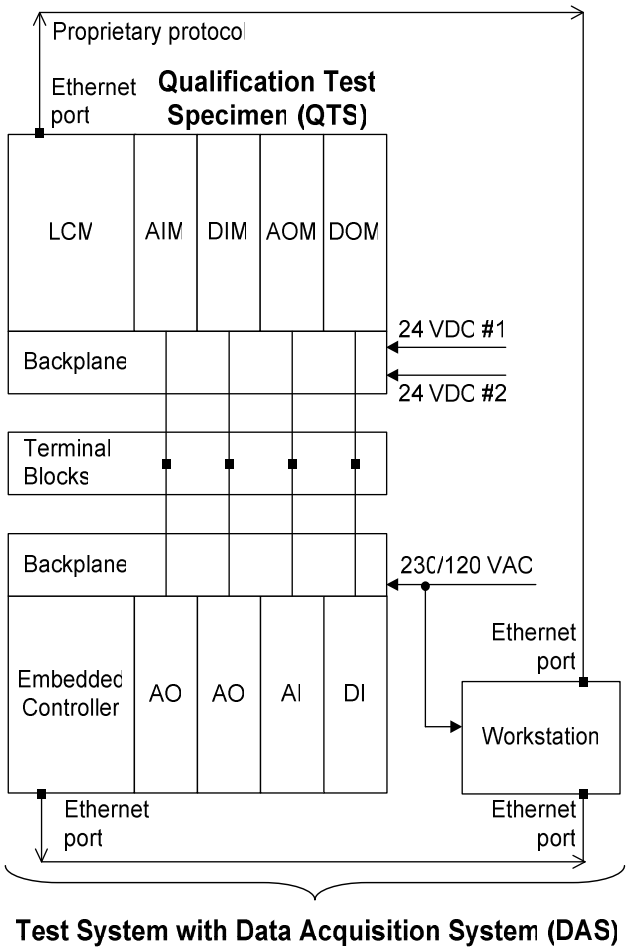

Fig. 2. A configuration and connection diagram for the PLC-based Qualification test Specimen connected with the Test System.

2.4 Design of software for the Qualification Test Specimen and the Test System

To develop the software of the QTS we first consider the requirements of EPRI TR-107330 for the

operation of the PLC when conducting qualification tests (see Table 1).

Table 1. EPRI TR-107330 requirements for PLC functions.

Test name	Implementation in the QTS	MDD inputs
Analog input/output accuracy test	For each type of input and output analog signal, the accuracy of the linear measurement must be checked at least five points	For AI: the functional block "Data Transmission" . For AO: the functional block "Stair steps" (5 reference values for signals in the measured range)
Response time test	The response time of the system (changing the output value) must be measured to change the input for the circuits	For AO – DO loops: the functional block "Comparator" with set-points in the middle of the range
Discrete input operability test	Measurement of electrical parameters at which the logic value of a digital input changes (ON to OFF and OFF to ON)	No additional inputs (is covered by measurement)
Discrete output operability test	Measurement of electrical parameters at which the logic value of a discrete output changes (ON to OFF and OFF to ON)	No additional inputs (is covered by measurement)
Timer test	Testing the accuracy of performing temporary functions	For DI – DO loops: the functional block "Delay"
Failover operability tests	Testing of functioning in the conditions of failures of redundant equipment	No additional inputs ((is covered by switching off one from two redundant 24 VDC)
Power interruption test	Not applicable for the considered PLC configuration	No additional inputs (is covered by switching off / on the power)
Burst of Events Test	Testing the response to fast switching of input signals	No additional inputs (is covered by configuration of AI – AO and DI – DO loops)

Thus, the tests described in Table 1 define the minimum set of PLC functions and allows checking the main performance functions such as processing and generation input and output signals, accuracy, response time, timers, communications, operation in fault conditions and fast switching of input signals. All these functions can be implemented by developing a simple control logic (see Fig. 3).

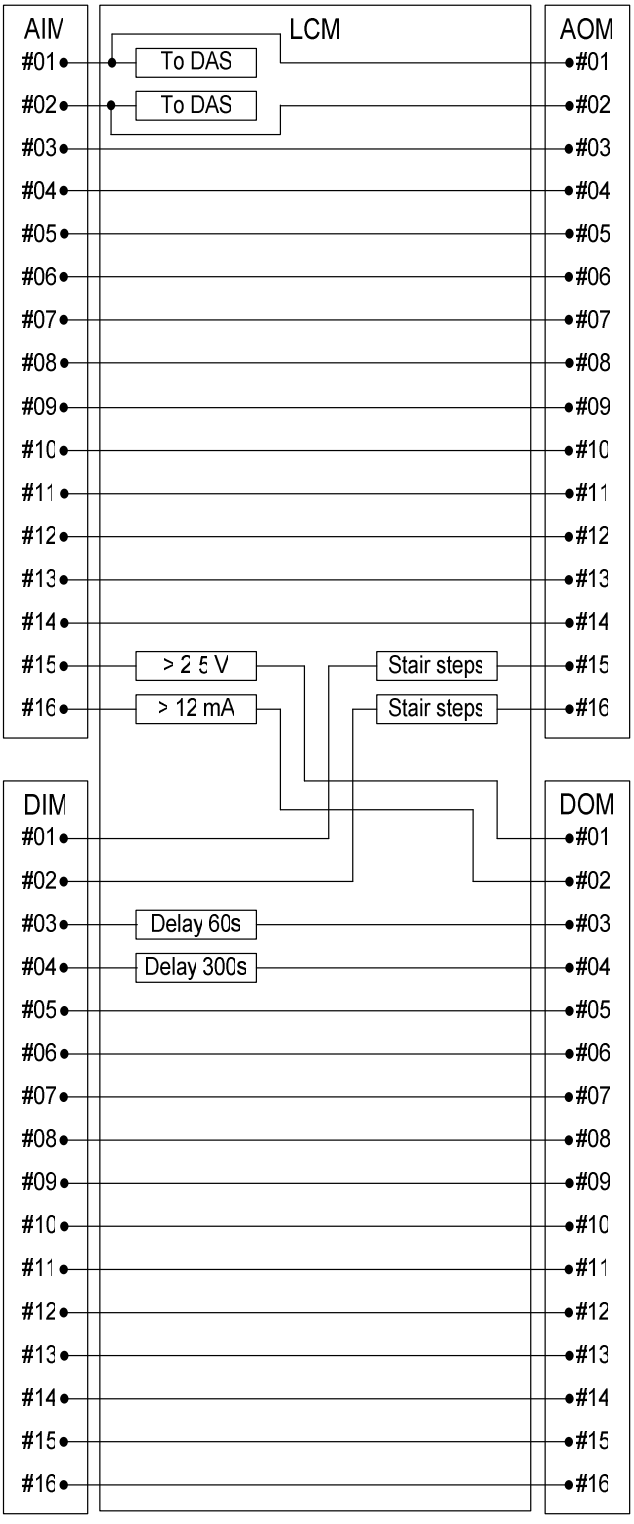

Fig. 3. Control logic of the PLC-based Qualification Test Specimen implementing basic functions.

The control logic (software) of the QTS represents a set of control algorithms, for which the input is connected to the output, and the LCM implements the control function, most of which is the direct conversion of the input signal to the output one.
The values of the discrete output signals are equal to the values of the input signals. For the analog signals a linear transformation is realized in accordance with the following equation:

$$y(x) = y1 + (y2 - y1) / (x2 - x1) \cdot (x2 - x1),$$

where x1, x2 are the lower value and the upper value of the range of the input signal, y1, y2 – are the lower value and the upper value of the range of the output signal.
For the functional blocks used, the following notations are introduced:
- "To DAS" – transmission of the measured value of the analog signal via Ethernet to the DAS for comparison with the reference value (accuracy test).
- "> 2.5 V", "> 12 mA" – comparators for exceeding the setpoint, the value of which are set in the middle of the range of the measured physical value of the signal (response time test for the circuit analog input - digital output).
- "Stair steps" – generation of a step changeable analog signal, in this case for 0%, 25%, 50%, 75% and 100% of the upper value of the measured range (accuracy test);
- "Delay 60s", "Delay 300s" – delays of 60 and 300 seconds (timer test).
Fig. 3 should be supplemented with ranges of measured analog signals, as well as with the distribution of control loops between the tests conducted. To clarity these issues we represent below an additional table (see Table 2) which can be a part of both the QTS and the TS software design as well as software verification.
Control loops connected input and output analog ports are configured in such manner to provide all the possible loops combinations, such as:
- 0-5 V (input) – 0-5 V (output).
- 0-5 V (input) – 4-20 mA (output).
- 4-20 mA (input) – 4-20 mA (output).
- 4-20 mA (input) – 0-5 V (output).

3. Verification of Software for the Qualification Test Specimen and the Test System

We represent the QTS functional model in a table view (see Table 2 for analog inputs and outputs and Table 3 for discrete inputs and outputs) that includes descriptions of input and output signals and the dependence of output values from input values. This model covers both MDD and MBT.

The following fields are included in Table 2 and Table 3:
- TS Out – a signal value at the output of the TS connected with the associated input of the QTS. For addressing of the TS inputs and outputs we use the same numeration as for the QTS inputs and outputs (see Fig. 3).
- QTS In – an address of the input in the format "AI.01" (first analog input of the AIM) or "DO.16" (16th discrete output of the DOM).
- In Range – the operating range of the input signal.
- In Signal Value – is determined for the inputs by the physical value of the field signal (all initial values are listed in the table, but the same table can be used for stimuli modelling).
- Purpose for Test – a name of a supported functional test (see Table 1).
- Control Logic – a brief description of the corresponding algorithm ("Scaling 1:1" – a linear conversion of analog signals; "Data Transmission" – a transfer of a value of a signal to the DAS; "Comparator" - comparator; "Stair-steps" – a step change in the analog signal; "Delay" – time delay; "=" – the value of the output digital signal is equal to the value of the associated in the loop input discrete signal. For output modules dependences between output value and input value are described in the fielf "Signal Value".
- Related QTS Out – an address of the output connected to the input.
- QTS Out - an address of the output. Please note, it is similar but not the same with the field "Related QTS Out". An order outputs addresses is numerological, but is does not always related with connection order and control loops configuration.
- Out Range – the operating range of the output signal.
- Out Signal Value - is determined by the software of the LCM. Mathematical dependencies of outputs values from inputs values are given in the format of Microsoft Excel equations.
- TS In – a signal value at the input of the TS connected with the associated output of the QTS.

To verify the design of the software of the QTS and the TS, it is beneficial to combine in one table the models of the input and output modules. For this, the description of signals with the same adresses (for example, AI.01 and AO.01) is placed in Table 2 and Table 3 in a single line. In addition, the integrated model of the QTS and the TS must be supplemented with input and output signals of the test system.

The complete dependence of the signals of the model can be described by the following expression:
TS Input i = QTS Output i = f QTS [QTS Input i = = TS Output i = f TS (TS Setup j)].

Table 2. A functional model of the QTS (analog inputs and outputs).

Out	TS In	Range	ignal Value	ose for Test	ntrol Logic	ed QTS Out	S Out	Range	Out Signal Value	S In
0	AI.01	-5 V	0	Accuracy	Scaling 1:1 Transmission	AO.01 DAS	O.01	-5 V	=AI.01	0
4	AI.02	20 mA	4	Accuracy	Scaling 1:1 Transmission	AO.02 DAS	O.02	20 mA	=AI.02	4
0	AI.03	-5 V	0	ponse Time	Scaling 1:1	AO.03	O.03	-5 V	=AI.03	0
4	AI.04	20 mA	4	ponse Time	Scaling 1:1	AO.04	O.04	-5 V	=5/16*(AI.04-4)	0
0	AI.05	-5 V	0	ponse Time	Scaling 1:1	AO.05	O.05	20 mA	=4+16/5* AI.05	4
4	AI.06	20 mA	4	ponse Time	Scaling 1:1	AO.06	O.06	20 mA	= AI.06	4
0	AI.07	-5 V	0	st of Event	Scaling 1:1	AO.07	O.07	-5 V	= AI.07	0
4	AI.08	20 mA	4	st of Event	Scaling 1:1	AO.08	O.08	-5 V	=5/16*(AI.08-4)	0
0	AI.09	-5 V	0	st of Event	Scaling 1:1	AO.09	O.09	20 mA	=4+16/5* AI.09	4
4	AI.10	20 mA	4	st of Event	Scaling 1:1	AO.10	O.10	20 mA	= AI.10	4
0	AI.11	-5 V	0	st of Event	Scaling 1:1	AO.11	O.11	-5 V	= AI.11	0
4	AI.12	20 mA	4	st of Event	Scaling 1:1	AO.12	O.12	-5 V	=5/16*(AI.12-4)	0
0	AI.13	-5 V	0	st of Event	Scaling 1:1	AO.13	O.13	20 mA	=4+16/5* AI.13	4
4	AI.14	20 mA	4	st of Event	Scaling 1:1	AO.14	O.14	20 mA	= AI.14	4
0	AI.15	-5 V	0	ponse Time	mparator >2,5	DO.01	O.15	-5 V	IF(DI.01=1;"Stair-stepping";0)	0
4	AI.16	20 mA	4	ponse Time	mparator >12	DO.02	O.16	20 mA	IF(DI.02=1;"Stair-stepping";0)	4

Table 3. A functional model of the QTS (discrete inputs and outputs).

Out	TS In	Range	ignal Value	ose for Test	ntrol Logic	ed QTS Out	S Out	Range	Out Signal Value	S In
0	DI.1	4 VDC	0	Accuracy	air-stepping	AO.15	DO.1	4 VDC	=IF(AI.15>2,5;1;0)	0
0	DI.2	4 VDC	0	Accuracy	air-stepping	AO.16	DO.2	4 VDC	=IF(AI.16>12;1;0)	0
0	DI.3	4 VDC	0	Timer	Delay 60s	DO.03	DO.3	4 VDC	AND(DI.03=1;T>=60);1;0)	0
0	DI.4	4 VDC	0	Timer	Delay 300s	DO.04	DO.4	4 VDC	AND(DI.04=1;T>=300);1;0)	0
0	DI.5	4 VDC	0	ponse Time	=	DO.05	DO.5	4 VDC	= DI.05	0
0	DI.6	4 VDC	0	st of Event	=	DO.06	DO.6	4 VDC	= DI.06	0

0	DI.7	4 VDC	0	st of Event	=	DO.07	DO.7	4 VDC	= DI.07	0
0	DI.8	4 VDC	0	st of Event	=	DO.08	DO.8	4 VDC	= DI.08	0
0	DI.9	4 VDC	0	st of Event	=	DO.09	DO.9	4 VDC	= DI.09	0
0	DI.10	4 VDC	0	st of Event	=	DO.10	O.10	4 VDC	= DI.10	0
0	DI.11	4 VDC	0	st of Event	=	DO.11	O.11	4 VDC	= DI.11	0
0	DI.12	4 VDC	0	st of Event	=	DO.12	O.12	4 VDC	=C DI.12	0
0	DI.13	4 VDC	0	st of Event	=	DO.13	O.13	4 VDC	= DI.13	0
0	DI.14	4 VDC	0	st of Event	=	DO.14	O.14	4 VDC	= DI.14	0
0	DI.15	4 VDC	0	st of Event	=	DO.15	O.15	4 VDC	= DI.15	0
0	DI.16	4 VDC	0	st of Event	=	DO.16	O.16	4 VDC	= DI.16	0

This means that the TS is able to generate signals in several test modes (TS Setup j), which uniquely determine the states of each of the outputs of the TS (TS Output i). The state of each of the inputs of the QTS (QTS Input i) is equivalent to the state of the corresponding connected output of the TS. The QTS performs a logical conversion of the input data to the outputs. The state of each of the outputs of the QTS (QTS Output i) is determined by the executed algorithm (f QTS) and the data received at the corresponding connected input. The input data of each of the inputs of the TS (TS Input i) is equivalent to the state of the corresponding assembled output of the QTS.

It should be noticed that such an approach to programming the QTS for components of CCS to perform the functions necessary for conducting environmental (EQ) tests can be applied not only to the PLCs, but also to embedded systems and to the IoT.

4. Plan and Procedures for Equipment Qualification Testing

Let's consider planning and documenting of EQ tests. EQ testing can be performed on different sites by different personnel. The entire EQ testing process can take some months, so it is important to have a single basis for all the performed activities. Therefore, when planning this process, a general Equipment Qualification Test Plan (EQTP) is required (see Fig. 4).

The diagram represents an option for the EQTP content compliant with standards used for EQ testing. In needed, this structure can be modified.

The considered content of the EQTP includes the following sections:

- Purpose – purpose of the conducted tests.
- Approach to the definition of a set of tests (Scope).

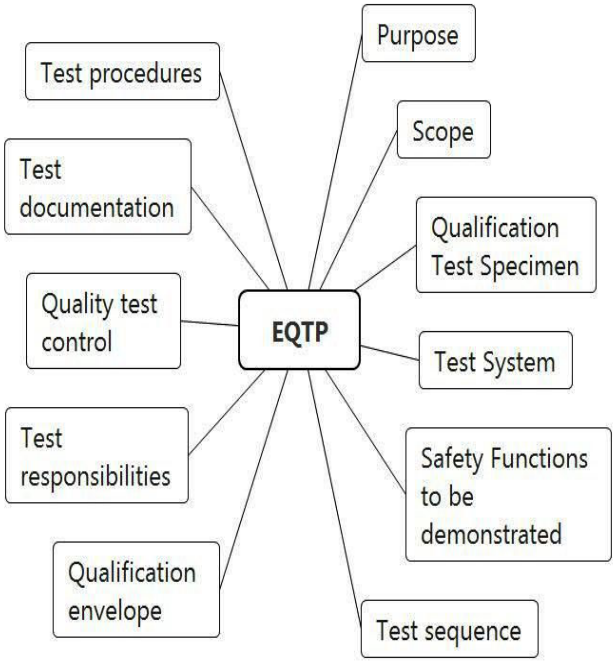

Fig. 4. A content of the Equipment Qualification Test Plan.

- Qualification Test Specimen – configuration and functions he QTS, which is carried out for qualification tests.
- Test System – configuration and functions of the TS.
- Safety Functions to be demonstrated – these functions are determined by test types and sequence.

- Test sequence – it is important to notice, that all types of tests are performed for the same QTS in a predetermined consistent sequence. For example, the referenced above EPRI TR-107330 requires to perform firstly climatic tests, then seismic tests, then electromagnetic compatibility tests (EMC).
- Qualification envelope – environmental test impact levels with are required by EQ standards.
- Test responsibilities – personnel assignment to perform specifies tests.
- Quality test control – applicable requirements of the Quality Management System used for testing activities control.
- Test documentation – a list of procedures and reports that should be developed to document the process of EQ testing.
- Test procedures – a list and summaries of test procedures, which are developed for each type of EQ testing. Further, the requirements for each type of test are detailed in the corresponding procedures.

5. Conclusions

The paper represents the EQ Testing Framework based on MDD and MBT. This framework includes the following activities.

The SUT (QTS) functionality is implemented as it is required by the document of the U.S. Electrical Power Research Institute (EPRI) called EPRI TR-107330 "General Specification of Requirements for the Qualification of Commercial PLCs for Safety-Related Applications at Nuclear Power Plants".

Hardware configuration for the SUT (QTS) includes Logic Control Module as well as modules for processing of input and output analog and discrete signals.

Design of software (as named control logic) for the (SUT) shall include functional blocks to support performance of the following tests: analog inputs and outputs accuracy, response time, timer accuracy and inputs fast switching tests.

Verification of the SUT (QTS) and TS can be done with use of MBT. Different tools can be applied to automate MBT.

Templates for development of EQ Test Plan and EQ Test Procedures are propose taking into account requirements of standards in area of environmental testing.

Analysis of the SUT (QTS) and TS operation during EQ tests performance is also one of the inputs of verification. Depending on the type of testing, the requirements to the functioning of the SUT (QTS) and the TS may be updated. In some cases that may lead to software correction.

The proposed EQ Testing Framework has been successfully used in industrial projects related with licensing and certification in nuclear domain [7,8].

References:

[1] O. Olawumi, A. Väänänen, K. Haataja, P. Toivanen, Security Issues in Smart Homes and Mobile Health System: Threat Analysis, Possible Countermeasures and Lessons Learned, *Int. J. on Information Technologies and Security*, **1** (2017)

[2] I. Atanasov, Modeling Aspects of Autonomous Smart Metering Information System, *Int. J. on Information Technologies and Security*, **1** (2016)

[3] N. Leveson, A New Accident Model for Engineering Safer Systems, *Safety Science*, **42** (2004)

[4] M. Yastrebenetsky, V. Kharchenko (Eds), Nuclear Power Plant Instrumentation and Control Systems for Safety and Security, IGI Global (2014)

[5] O. Siora, V. Kharchenko, V. Sklyar, A. Andrashov, Innovative Approach to Implementation of FPGA-based NPP I&C systems, *Int. J. of Nuclear Safety and Simulation,* **4** (2011)

[6] P. Bishop, R. Bloomfield, A Methodology for Safety Case Development, *Proc. of the 6th Safety-critical Systems Symposium* (1998)

[7] V. Sklyar, Safety-critical Certification of FPGA-based Platform against Requirements of U.S. Nuclear Regulatory Commission (NRC): Industrial Case Study, *Proc. of 'ICTERI 2016'*, (2016).

[8] V. Sklyar, V. Kharchenko, Assurance Case Driven Design based on the Harmonized Framework of Safety and Security Requirements *Proc. of 'ICTERI 2017'*, (2017)

[9] D. Di Ruscio, I. Malavolta, H. Muccini, P. Pelliccione, A. Pierantonio, Model-Driven Techniques to Enhance Architectural Languages Interoperability, *Proc. of 'FASE 2012'*, Springer-Verlag, LNCS 7212, (2012)

[10] P. Zhang, H. Muccini B. Li, A classification and comparison of model checking software architecture techniques, *J. of Systems and Software*, **83** (2010)