DEVELOPMENT OF A SYSTEMATIC APPROACH FOR SAFETY ASSESSMENT OF PLD BASED EQUIPMENT OF I&C SYSTEMS

Ewgenij Piljugin, Claudia Quester, Manuela Jopen
Gesellschaft fuer Anlagen- und Reaktorsicherheit (GRS) gGmbH
Schwertnergasse 1, 50667 Cologne, Germany
ewgenij.piljugin@grs.de; claudia.quester@grs.de; manuela.jopen@grs.de

ABSTRACT

Nuclear power plants (NPPs) increasingly apply digital equipment for instrumentation and control (I&C) systems. During the life cycle of NPPs the operators, designers and manufactures are facing the need to replace or upgrade obsolete equipment or to implement new digital I&C systems. A relatively new challenge in this area is the deployment of programmable logic devices (PLDs) for the equipment of I&C systems. Regulatory approval for safety and safety related I&C systems demands confirmation of evidence that design as well as verification and validation (V&V) processes have ensured that the application of new equipment will fulfil safety and reliability requirements and its intended design function.

The objective of the recent research project of GRS is developing a systematic approach for the assessment of PLD-based equipment in safety and safety-related I&C systems regarding the fulfilment of regulatory requirements and identification of undesired failure effects.

A generic approach for the safety-oriented assessment of PLD-based equipment has been developed, based on the principles of a Plan-Do-Check-Act (PDCA) cycle. The approach comprises planning of the assessment, predefined analysis steps and methodologies, as well as required input information, criteria for decision making process, the tasks concerning identification of improvement potential and determining documentation.

Key Words: digital, I&C system, programmable logic device, safety assessment, PDCA cycle

1 INTRODUCTION

Nuclear power plants (NPPs) increasingly apply digital equipment for instrumentation and control (I&C) systems. During the life cycle of a NPP the operators, designers and manufactures are facing the need to replace or upgrade obsolete equipment or to implement new I&C systems. A relatively new challenge in this area is the deployment of programmable logic devices (PLDs) for the equipment of I&C systems. The PLD-based I&C equipment may apply different technologies and a variety of the device designs, e.g. field programmable gate arrays (FPGA), application specific integrated circuits (ASIC), complex PLDs (CPLD) or high-integrated circuits as a system on chip (SoC) design [1], [2], [3]. The functionality of a PLD device can be expanded by the integration of additional programmable and microprocessor based elements (e.g. processor architecture with memory controller and peripherals), which increase the complexity of such assemblies and make their qualification and safety analysis particularly complex [4], [5].

In general, PLD-based devices have a combination of properties that are characteristic of both hardware and software. A PLD module contains an array of programmable logic blocks (e.g. Boolean logic gates) and may also include memory elements. The interconnections of a PLD module will be established by electrical circuits and these links can be configured by programming. When programming PLDs, a distinction is made between different types that allow for one-time or re-

configurable programming. In this context, programming is understood as a process in which the structure of integrated circuits is created using hardware description languages (HDL) and subsequently these data are transferred as configuration to the PLD module. In this way, the interconnection of the predetermined elements and the function of individual blocks of a PLD are determined. The terms programming and configuration are often used synonymously in this context. The HDL programming tools are important for design, implementation and verification and validation (V&V) of the PLD-based equipment [1], [4].

The required functional safety of the PLD-based I&C equipment shall be achieved by fulfilling the requirements of current industry standards with regard to the application of measures for fault avoidance and management of probable failure effects [6], [7]. If this equipment will be used for safety-relevant functions of the automation and process control technology, the reliability required for the purpose of use must be demonstrated in the context of certification and qualification procedures [8]. Regulatory approval for safety and safety related I&C systems demands confirmation of evidence that design and (V&V) processes have ensured that the application of the considered new equipment will fulfil safety and reliability requirements and its intended design function.

The objective of the recent research project of GRS is developing a systematic approach for the assessment of PLD-based equipment of safety and safety-related I&C systems regarding the fulfillment of regulatory requirements and identification of undesired failure effects.

Initially, a study has been performed concerning the state of the art of PLD technology in digital automation and process control systems and V&V methodologies for PLD-based equipment. Various information sources were evaluated with regard to aspects of hardware and software of the PLD technology and to the requirements for the design, manufacturing and operation of PLD-based equipment of I&C systems. Furthermore, some generic failure modes of generic PLD-based I&C equipment have been identified.

Main part of the research work was focused on development of an approach for evaluation of safety aspects concerning the usage of PLD-based equipment for safety-relevant functions of I&C systems. The approach's core is implemented as flow charts representing the decision making process and usage of applicable analysis tools and methodologies (e.g. FMEA – Failure Mode and Effect Analysis, FTA – Fault Tree Analysis) [9]. The flow charts of the approach comprise a number of decision trees with supporting matrices considering task tailored requirements.

Finally, for the evaluation of the developed methodology, GRS has performed a model-based testing of the approach on an analytical model considering typical features of generic PLD-based modules of a hypothetical I&C system. The paper presents preliminary results of the development of the approach for the safety assessment of PLD-based equipment of I&C systems.

2 DEVELOPMENT OF THE ASSESSMENT METHODOLOGY

2.1 Description of the Concept - CAMIC approach

As already mentioned in section 1, within the scope of research work an approach for the assessment of PLD-based I&C equipment in NPPs has been developed based on the Plan-Do-Check-Act cycle (PDCA) the method CAMIC (Cyclic Analytic Methodology for I&C). It provides guidance for the analysis of the different types of PLD-based devices of I&C systems and for investigation of the effects of probable malfunctions on control systems and control functions. Furthermore the CAMIC methodology can be used for evaluation of the measures to prevent or to mitigate undesired failure effects of the I&C equipment.

The assessment of the intended utilization of the PLD-based I&C equipment in NPPs is usually a multistage process. This process should be carried out within the framework of the CAMIC methodology according to the principles of the PDCA cycle [10]. As a first step of the CAMIC assessment it will be established a screening task to identify the scope, intendent place of installation and function of the assessed PLD-based equipment in the I&C architecture. Fig. 1 presents the PDCA cycle of the CAMIC approach.

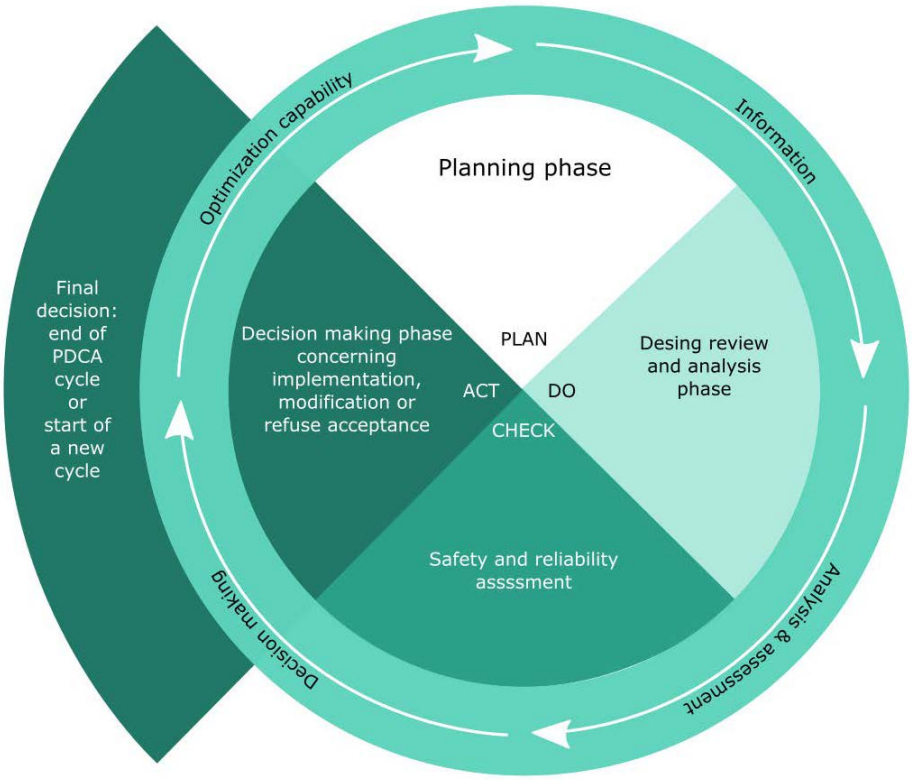

Figure 1. PDCA cycle of the CAMIC approach

The PDCA cycle can be used in many ways through a general approach and offers the opportunity to adapt the four steps "Plan-Do-Check-Act" to specific objectives and requirements, e.g.

- Design of new I&C systems, equipment and functions,
- Assessment of the current state of the I&C in a NPP and development of improvement proposals,
- Assessment of potential CCF of the I&C.

The CAMIC approach consists of the following process steps:

- **PLAN:** In this process step, all information relevant to the analysis regarding the planned application of PLD-based devices and all the requirements relevant for the corresponding I&C system, including their equipment must be gathered.
- **DO:** In this step, an analysis of the intended use of the PLD will be carried out as a sequence of different analysis steps adapted to the specific condition (e.g. operational mode, maintenance, repair, consideration of fault tolerant measures). This part of the analysis

should provide results regarding probable (negative) effects of all failure modes of the PLD-based devices within the I&C architecture.

- **CHECK:** The essential aspect of the process step CHECK is the evaluation of the analysis results to determine whether the possible effects due to the use of the PLD-based device are admissible.
- **ACT:** First, a decision must be made in the process step ACT based on the results of the process step CHECK as to whether the use of the PLD-based devices can take place as intended. If the PLD-based device can't be used as planned due to certain reasons (e.g. self-signaling failure, fail-safe failure state), an analysis of the whole I&C system should be performed with the focus on the identification of the propagation of the failure effects through the I&C architecture and possible impacts on the safety relevant function. The findings provide feedback for the PLAN phase and thus complete the PCDA cycle.

After completion of the first PDCA cycle, the findings may lead to changes in the design or in the utilization of the PLD-based I&C equipment and therefore to the further run of the next PDCA cycle. A successful completion of a PDCA cycle is prerequisite for deployment of the planned design, e.g. as a part of an approval (certification) process. The termination of the PDCA cycle is in principle possible in any process step with negative analysis results.

2.2 Decision Making Process of the CAMIC Approach

The CAMIC method is based on the following basic parts for all PDCA steps:

- Definition of start points, breakpoints and end points
- Definition and acquirement of input information for the assessment of the PLD based equipment
- Definition of criteria for the decision making process
- Interface to the analysis methods (e.g. FMEA, FTA, CCF analysis)
- Output information as intermediate results of each PDCA step

The workflow of the CAMIC comprises a number of flow charts (decision making trees) with start, hold and end points for each PDCA step. The flow charts were prepared in accordance with German industrial standards [11] and use specified boxes, e.g.

- processing step, usually called activity, and denoted as a rectangular box
- decision criteria, usually denoted as diamond boxes
- interim results, denoted as parallelogram boxes
- start points, breakpoints and end points, denoted as colored ellipse
- input information, denoted as rectangular boxes with one wavelike side.

Definition of start, breakpoints and end points:

- The start point is the initial condition for each assessment step of the PDCA cycle
- Breakpoints characterize possible situations as they are at the end of a process step and provide information for the subsequent process step. Breakpoints can also provide information concerning consequences, as result of the assessment (e.g. additional regulatory request, demands for additional information) of this process step.
- The endpoints describe possible situations at the end of the assessment process.

The decision criteria of the CAMIC are formulated as a query matrix. The binary responses (YES or NO) to these questions determine the sequence of analysis steps. Table 1 presents an excerpt of the linking, query and criteria matrices for the decision making process of the CAMIC approach.

Table I. Summarized representation of the CAMIC matrices

Definition of the assessment steps of the PDCA cycle				
Identifier	**Assessment step**	**Required input**	**Scope**	**Step**
A-P1	Evaluation of the I&C architecture concerning implementation of new I&C equipment	I-P1	I&C device I&C function I&C system Interface	P1
A-Pn	Description of the task A-Xn	-	-	-
Input information				
Identifier	**Required input information**	**Output & link mark**		**Step**
I-P1	Description of the modernization concept	A-P1, A-P2		P1, P2
I-Pn	Description of further inputs	-		-
Criteria for decision making process				
Identifier	**Decision criterion**	**Output & link mark**		**Step**
E-D1	Can the signal paths of several I&C functions be affected by the use of the new equipment?	Z-P1, Z-P2		D1
E-Dn	Description of the criterion E-Dn	-		-
Objective for intermediate results of the analysis steps				
Identifier	**Intermediate results**	**Assessment step**		**Step**
Z-P1	Estimation of the extent (number and types) of the of PLD-based I&C devices in the framework of the modernization project	A-P1		P1
Z-Pn	Description of the result Z-Pn	-		-

An identification mark is assigned to each analysis step and to each decision criterion, as well as to each input and to each intermediate result. These marks will be systematically used in the CAMIC flowcharts (PDCA decision trees):

- A – assessment step
- I – input

- E – decision criterion
- Z – intermediate result

The identifier is followed by a dash with the uppercase letter of the process step ("P" for plan, "D" for Do, "C" for check, and "A" for act) and a serial number (e.g. E-D1 - Decision criterion in process step DO with the consecutive number 1). Fig. 2 shows an example of a CAMIC flowchart for the PLAN step of the assessment process.

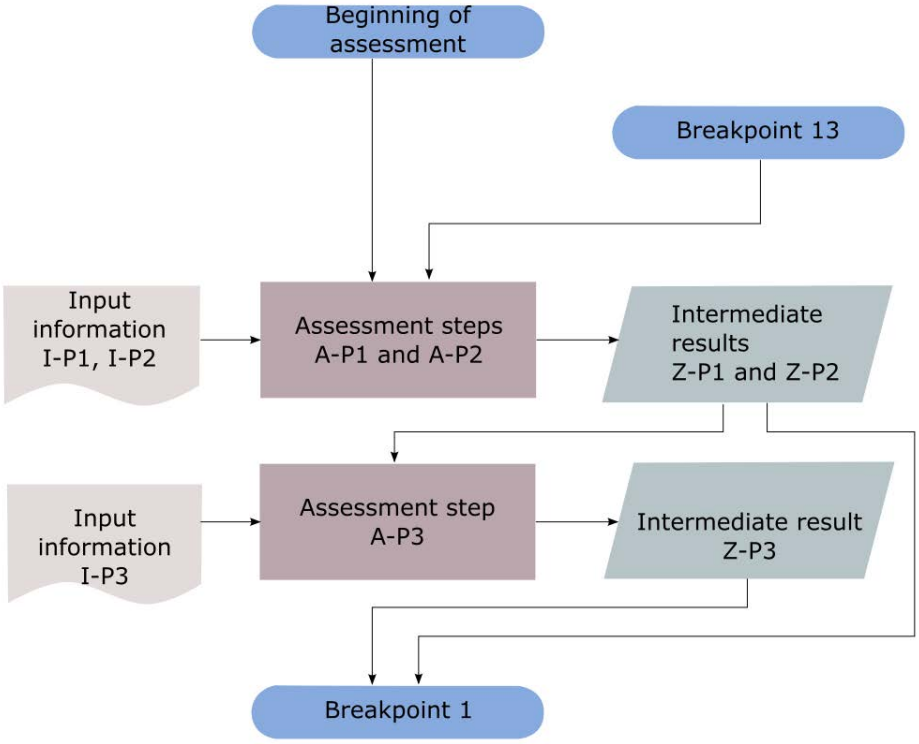

Figure 2. Example of a CAMIC flowchart

The result of a CAMIC assessment process is considered positive if no inconsistencies were found during the PDCA cycle between the requirements determined in the process step PLAN and the intended use of the PLD-based I&C equipment. Within the framework of the CAMIC method, a positive process completion is only provided in process step ACT. If minor deviations from requirements have been determined without influence on safety-relevant functions of the equipment, then these can be accepted in the step ACT only. Otherwise corrective actions in the step DO are necessary.

There may be several reasons for a negative result of the assessment process. On the one hand, the use of the I&C equipment may be rejected because of inconsistencies between requirements determined in the process step PLAN (e.g. incomplete documentation, inadequate specification, unsatisfactory performance, maintenance issues, probable hazardous failure modes). On the other hand, the rejection decision can be made when probable effects of a malfunction of the equipment (step CHECK) cannot be accepted in the process step ACT.

2.3 Model-based Testing of the CAMIC Approach

Generally, the CAMIC method requires a safety and reliability analysis of the PLD-based I&C equipment in the step DO and the evaluation of the analysis results in the step CHECK. For validation of these process steps, a test case was carried out using a FMEA and FTA methodology [9].

The focus of the development of the CAMIC method is the assessment of the PLD-based I&C equipment regarding fault avoidance, failure prevention and failure control. Consequently, the causes and the identification of all probable failure modes and its effects have to be taken into account in the modeling. The following assumptions were made:

- Failure modes of modules should be determined by an abstraction level dependent FMEA analysis
- Global failure effects should be divided into the categories “spurious failure” and “failure on demand”, independent of the abstraction level
- The width of the consequences of a failure mode should be defined as single failure of one module or common cause failure (CCF) of several modules
- The detection of a failure mode should be divided into the categories “self-signaling” and “non-self-signaling”

The model development was made on the basis of assumptions considering typical characteristics and functions of a drive control unit, because several types of the PLD-based control devices with different functionalities (redundant signal processing, automatic monitoring, communication features, etc.) are already used in I&C systems in NPPs. Since the information on the PLD-based equipment is not always available to the required extent and level of detail, the modeling was carried out step by step with increasing detail using feedback from the model analysis. The following modeling approaches were used:

- A Black-Box model describes the behavior of the input and output signals of the module in a descriptive manner and uses a general model approach (including rule-based and knowledge-based modeling) to approximate the behavior of the module in case of one or more errors
- A White-box model represents causal relationships within an assembly or a system. The functional relationships can be described analytically and modeled using available information (e.g. MATLAB/Simulink, Fault Tree model), whereby the iterative approach can be used for this purpose
- A Gray-Box model is a hybrid of Black-Box and White-Box models.

In general, a drive control unit consists of a command module, a monitoring module and a power supply module. In the first model one PLD in the command module was considered. It was assumed that detailed information about the hardware and software of the module is not available. Therefore a Black-Box model was used. Furthermore, it was assumed that for some functions and signal connections more detailed information was available. In this case, a Grey-Box model was applied. Fig. 3 presents a simplified block diagram of the model AS-PLD-BB of a PLD-based drive control module.

For the FMEA analysis, the function blocks of the considered model were subdivided into function elements (e.g. different input/output signals, status signals). These elements were recorded in a FMEA table to analyze their potential failure modes with regard to their impact on the intended I&C functions, e.g.

- manual and automatic start and shutdown of the motor drive
- acquisition of the check-back signals from the motor drive (switchgear unit).

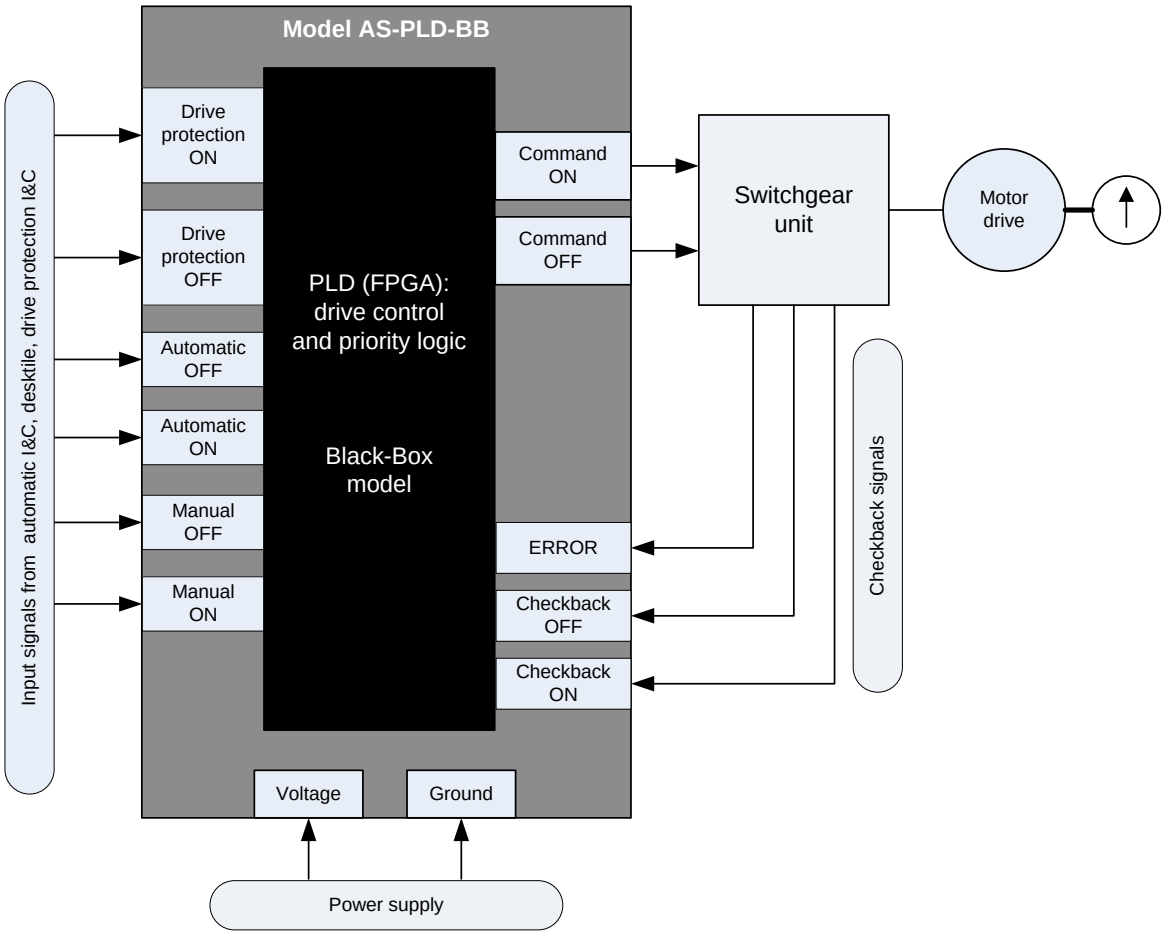

Figure 3. Model of a PLD-based motor drive control device

The FMEA results of the first test case have shown clear indications with regard to a model extension, especially for the further specification of the signal processing in the PLD command module.

Since the model AS-PLD-BB didn't contain any other redundant modules for drive control, a CCF analysis was not applicable with this model. Therefore, an extended model of the motor drive control function was developed, which contained two redundant drive control units with specified priority logic inside the switchgear unit. The new model provides possibilities to apply different types of the PLD-based devices for evaluation of the specified diversity attributes. For this purpose a comprehensive analysis has been performed using FMEA and FTA methodology. Subsequently the analysis results were used for evaluation of the CAMIC approach. The testing showed the principal applicability of the CAMIC approach for the assessment of the reliability of PLD-based equipment. Necessary improvements of the CAMIC were determined for the interface between assessment steps and analysis methods (e.g. FMEA, FTA). The work has not yet been completed and will be continued.

3 CONCLUSION

This paper gives an overview on the current state of the research work conducted by GRS in the frame of a R&D project, which was funded by the German Federal Ministry for Economics and Energy. The generic method CAMIC has been developed and tested for the safety-oriented assessment of PLD-based equipment regarding the fulfillment of regulatory requirements and identification of undesired failure effects. The focus of the development was the assessment of fault avoidance, failure prevention and failure control. The approach comprises planning of the assessment, predefined analysis steps and methodologies as well as required input information about the considered system, requirements and criteria for the decision making process and the tasks for the identification of potential improvements.

The CAMIC method can be applied to all life cycle phases (e.g. design, production, operation, modification) of the PLD-based equipment. To test the CAMIC method, different models of the motor drive control center were developed and a FMEA and for a certain case a FTA analysis were performed.

In this project, a first assessment approach for PLD-based equipment in I&C systems was developed. It demonstrates the potential for a consistent assessment method generally for digital I&C systems. Nevertheless, several aspects were realized, which indicate the necessity for further development, which will be implemented in a follow-up research project:

- So far, only the component level for PLD-based equipment in I&C systems is considered. The analysis of the impact of PLD-based equipment on system or functional level will be implemented and extended from PLD-based equipment to digital equipment in general
- To get a better handling, consistency and documentation of the method, a computer based implementation of the methodology is necessary and will be implemented
- An interface for the application of additional tools will be defined in a clear manner
- The CAMIC approach will be extended regarding requirements for use of Black-Box and White-Box models.

4 ACKNOWLEDGMENTS

The authors want to acknowledge the support provided by the German Federal Ministry for Econo mics and Energy (Bundesministerium für Wirtschaft und Energie) for funding the GRS development of an assessment methodology for PLD-based I&C equipment in the frame of the R&D project RS1525.

5 REFERENCES

1. Deutsches Institut für Normung (DIN) e. V.: *Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions (IEC 62566:2012)*; German version EN 62566:2014.
2. International Atomic Energy Agency (IAEA): *Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants*; IAEA Nuclear Energy Series, No. NP-T-3.17, Vienna 2016.
3. Menon, C., Guerra, S.: *Field Programmable Gate Arrays in safety related instrumentation and control applications*. Energieforsk Report 2015:112, ISBN: 978-91-7673-112-3. 2015.
4. Bobrek, M., Bouldin, D., Holcomb, D., Killough, S., Smith, S., Ward, C., Wood. R.T.: *Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems.* U.S. NRC, Office of Nuclear Regulatory Research, NUREG/CR-7006, 2010.

5. Ranta, J.: *The current state of FPGA technology in the nuclear domain*. ISBN 978-951-38-7622, VTT Technology, 10.12.2011.
6. Deutsches Institut für Normung (DIN) e. V.: *Dependability management - Part 3-1: Application guide - Analysis techniques for dependability - Guide on methodology (IEC 60300-3-1:2003)*; German version EN 60300-3-1:2004.
7. Deutsches Institut für Normung (DIN) e. V.*: Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (IEC 61508-1:2010)*; German version EN 61508-1:2010.
8. Nuclear Safety Standards Commission KTA (Germany), *KTA 3503, Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System,* 2015.
9. Nuclear Energy Agency: *Failure modes taxonomy for reliability assessment of digital I&C systems for PRA. Committee on the safety of nuclear installations*, NEA/CSNI/R (2014)16. 16.02.2015.
10. Deutsches Institut für Normung (DIN) e. V.: *Quality management systems - Requirements (ISO 9001:2015)*; German and English version EN ISO 9001:2015.
11. Deutsches Institut für Normung (DIN) e.V.: *Informationsverarbeitung; Sinnbilder und ihre Anwendung; DIN 66001*, Dezember 1984.