DIVERSITY FOR SAFETY AND SECURITY OF NPP I&C: POST NUREG/CR 7007 STAGE

Vyacheslav Kharchenko, Eugene Babeshko
Centre for Safety Infrastructure-Oriented Research and Analysis
37 Astronomicheskaya str., Kharkiv, 61085, Ukraine
v.kharchenko@csn.khai.edu; e.babeshko@csis.org.ua

Kostyantyn Leontiiev
Research and Production Corporation Radiy
29 Geroyev Stalingrada str., Kropyvnytskyi, 25009, Ukraine
ksleontiev@radiy.com

Vyacheslav Duzhy
National Aerospace University "Kharkiv Aviation Institute"
17 Chkalova str., Kharkiv, 61070, Ukraine
v.duzhy@csn.khai.edu

ABSTRACT

The paper summarizes authors' experience on diversity aspects of NPP I&C systems. It also discusses diversity analysis aspects according to NUREG/CR 7007 and other relevant standards. Diversity implementation challenges related to regulatory authorities, developers, auditors and operation engineers and managers are formulated and discussed. The paper presents a case study and developed tool to support diversity analysis and assessment using post NUREG/CR 7007 approach.

Key Words: Diversity, Common Cause Failure, NPP I&C System Analysis

1 INTRODUCTION

Diversity is proven to be a very general approach to ensure the required levels of various Nuclear Power Plant (NPP) Instrumentation and Control (I&C) Systems dependability attributes, first of all reliability and safety. Diversity application is recommended by national and international standards for different critical domains. The most well-known and detailed normative document NUREG/CR 7007 [1] that discusses diversity strategies and technique to assess diversity metrics for NPP I&C systems was issued in 2009. Since issue of NUREG/CR 7007 a lot of changes have occurred, including:

– Intensive usage of new components like FPGAs during NPP I&C systems modernization. Such components provide new possibilities for diversity utilization, that should be addressed to improve overall NPP I&C systems safety and security;

– Extending of diversity application for new safety critical domains such as automotive (standard ISO 26262:2011 [2] contains requirements to hardware and software diversity for on-board control systems). Analysis of operation statistics and best practices for different domains allows to improve understanding of all sides of diversity application;

– Improvement and implementation of techniques and tools based on NUREG 7007 and other normative documents;

– Cyber security related challenges or safety critical systems including NPP I&C systems. Diversity can be applied for NPP I&C systems security improvement, although this approach is not widely used so far [3].

The main challenges of diversity principle implementation are the following:

– For regulatory authorities: how to define the frameworks and formulate the requirements to application of diversity in sufficient detail. Besides, new technologies create additional possibilities for improving safety and cyber security by diversity approach implementation due to increasing number of diverse processes and product options. On the other side, they can be a reason for new safety deficit. Hence, new risks must be taken into account in regulatory documents;

– For developers: how to extend and choose the types and capacity of version redundancy to meet requirements and assure optimal design according to criteria "required safety-minimal costs". The other challenge is cyber security issue, because application of diversity can improve integrity but worsen confidentiality and (in some cases) availability;

– For (independent) verifiers and validators: how to assess actual level of diversity and confirm or refute that diversity related decisions completely meet requirements. Quantitative assessment of diversity is an actual challenge because failures of multi-version safety critical systems are very rare and application of statistical methods is limited by representativeness issue;

– For plant engineers and managers: how to maintain diversity-based systems considering more complex architecture and recovery activities. There are challenges caused by maintenance complexity and human factors.

The goals of our paper are to analyze these changes, challenges and possibilities of diversity application for NPP I&C systems safety and security assurance, to develop a system approach which would allow to consider possible measures of achieving safety and security by means of diversity, and to discuss possible tool support for this approach. To make a case study we present the analysis of FPGA-based RadICS platform and platform-based solutions for NPP I&C systems.

2 NUREG 7007/CR APPROACH

Appendix A of NUREG 7007/CR, “Evaluating diversity in system designs” defines seven diversity attributes and related diversity criteria. These attributes and related criteria are:

1) Design:

– Different technologies;

– Different approaches within a technology;

– Different architectures;

2) Equipment Manufacturer:

– Different manufacturers of fundamentally different equipment designs;

– Same manufacturer of fundamentally different equipment designs;

– Different manufacturers of same equipment design;

– Same manufacturer of different versions of the same equipment design;

3) Logic Processing Equipment:

– Different logic processing architectures;

– Different logic processing versions in same architecture;

– Different component integration architectures;

– Different data flow architectures;

4) Function:

– Different underlying mechanisms to accomplish safety function;

– Different purpose, function, control logic, or actuation means of same underlying mechanism;

– Different response time scale;

5) Life-cycle:

– Different design organizations/companies;

– Different management teams within the same company;

– Different designers, engineers, and/or programmers;

– Different implementation/validation teams (testers, installers, or certification personnel);

6) Signal:

– Different parameters sensed by different physical effects;

– Different parameters sensed by the same physical effects;

– Same parameter sensed by a different redundant set of similar sensors;

7) Logic:

– Different algorithms, logic, and program architecture;

– Different timing or order of execution;

– Different runtime environments;

– Different functional representations.

NUREG 7007/CR describes technique for diversity assessment which is based on additive convolution of metrics values. The values are calculated according to their priorities and weight coefficients for diversity attributes that are defined considering their application in NPP I&C systems. This technique doesn't allow to take into account other version redundancy types and procedures to calculate weight coefficients, as well as to consider possible attributes dependencies. The technique and NUREG 7007/CR as a whole can be used as an umbrella standard for developing own methods. The example of such method is provided in the case study section of this paper.

3 DIVERSITY-RELATED STANDARDS AFTER NUREG/CR 7007

Diversity issues were raised by several international standards issued after NUREG/CR 7007. These standards cover different critical domains like automotive and nuclear. Sections below provide overview of key statements from the most relevant standards.

3.1 Analysis of IEC 61508:2010

IEC 61508:2 [4] emphasizes the necessity for diversity application during hardware design.

Diverse hardware is not required if validation and extensive operational experience prove that the hardware is sufficiently free from design faults and sufficiently protected against common cause failures to fulfill the target failure measures.

IEC 61508:3 also contains requirements to software diversity.

For the selection of appropriate techniques and measures to implement the requirements of software architecture design, the following properties of the software architecture design should be considered:

– completeness with respect to software safety requirements specification;

– correctness with respect to software safety requirements specification;

– freedom from intrinsic design faults;

– simplicity and understandability;

– predictability of behavior;

– verifiable and testable design;

– fault tolerance;

– defense against common cause failure from external events.

The following architecture and design features should be targeted:

– diverse monitor techniques (with independence between the monitor and the monitored function in the same computer and separation between the monitor computer and the monitored computer as well);

– diverse redundancy (implementation of the same software safety requirements specification);

– functionally diverse redundancy (implementation of different software safety requirements specification).

3.2 Analysis of IEEE Std 7-4.3.2-2016

Annex B of IEEE Std 7-4.3.2-2016 [5] provides diversity requirements determination. It also specifies requirements and recommendations to diversity implementation of manual controls and displays, as well as requirements to automatic controls.

The document states that safety-related instrumentation and control systems shall have adequate defense in depth and diversity (D3) to compensate for credible common cause failure (CCF.)

If digital components have sufficient diversity, then CCF can be categorized as not credible between these components.

The following cautions regarding diversity are determined in this document:

– The justification for the level of diversity of equipment, or of related system software such as a real-time operating system, shall extend to the equipment's components to ensure that actual diversity exists.

– With respect to software diversity, experience indicates that independence of failure modes may not be achieved in cases where multiple versions of software are developed to the same software requirements.

It is determined that manual operator action may be credited as backup to safety functions disabled by postulated CCF, if the manual action can be performed reliably in a period when the plant response remains bounded by the acceptance criteria for radiation release. Diverse automation may be credited as back-up to safety functions disabled by a postulated CCF. The automation shall be provided by equipment that is not affected by the same postulated safety system CCF. This equipment may be digital or non-digital.

3.3 Analysis of ISO 26262-10:2011

Table A.7 of ISO 26262-10 [2] states that hardware faults, development faults, stresses due to specific situations like wear and ageing, and even environmental factors can be addressed by such measures as diversity.

3.4 Analysis of IAEA SSR-2/1:2016

IAEA SSR-2/1 [6] specifies that diversity shall be considered for I&C systems performing safety functions, as well as for support service systems, communication systems etc.

It is stated that functional diversity and diversity in component design and in concepts of operation shall be used to the extent practicable to prevent the loss of a safety function.

3.5 Analysis of IAEA NP-T-3.17:2016

IAEA NP-T-3.17:2016 [7] states that FPGA technology could constitute a viable option for diversity between primary and redundant safety functions. It is also stated that redundant microprocessor and FPGA based systems must, as a minimum, meet the following diversity criteria:

– Design diversity (different technologies and architecture);

– Equipment diversity;

– Functional diversity (different ways to achieve the same result);

– Software diversity (different programming languages, design methodologies and software architecture).

Section 3.1.7 summarizes utilization of FPGA features to provide diversity, in particular, within FPGA-based system itself.

3.6 Conclusion

Considering all mentioned above, it can be concluded that all the standards are not devoted to diversity only, like NUREG 7007/CR, and do not provide any details on diversity evaluation and ensuring. The standards do not provide recommendations for determination of diversity metrics, weights of diversity attributes. A more detailed classification of FPGA designs and systems features is not provided either.

4 TECHNIQUES AND TOOLS FOR ASSESSMENT OF DIVERSITY

Three diversity assessment techniques were analyzed in [8]:

a) NUREG7007-based technique;

b) Check-list-based diversity assessment technique integrated with metrics and reliability block diagram or/and Markov models-based assessment of safety (CLB technique);

c) Graph model-based diversity assessment (GMB-technique).

Advantages and disadvantages of the b) and c) techniques compared to NUREG-based technique are explained by diversity attributes classification and its detailing, metrics procedure determination etc.

Developed tools DivA (Diversity Analysis Helper) and DivAS (Diversity Analysis and Synthesis Helper) [7] are based on the CLB- and GMB-techniques, in particular, hierarchy (multi-level and extensible) of diversity types, calculated results (weights, metrics,…), options for metric calculations. Besides, the DivAS supports decision making to select diversity types according with ‘safety-cost’ criterion.

5 CASE STUDY: ANALYSIS OF RADICS PLATFORM DIVERSITY USING POST NUREG/CR 7007 APPROACH

5.1 Object of Analysis

RadICS platform is a SIL3-certified FPGA-based automation platform [9]. During different certification phases different designs of RadICS platform were provided. These designs differ in hardware and software parts, and, therefore, can be used as diverse solutions for implementation of NPP I&C systems.

5.2 Approach Description

To perform analysis of RadICS platform-based I&C systems, an approach that considers NUREG 7007/CR and other standards mentioned in previous section of the paper (so called post NUREG/CR 7007 approach) was developed. While applying this approach, the following attributes of diversity were considered:

– Design Diversity as the result of application of different approaches, including both software and hardware to solve the same or similar problems;

– Equipment Manufacturer Diversity as the result of using different vendors, manufactures, etc.;

– Logic Processing Equipment Diversity as the result of different logic processing architectures, logic processing versions in the same architecture, component integration architecture, data-flow architecture;

– Functional Diversity as the result of treating two systems as functionally diverse if they perform different physical functions;

– Life-Cycle Diversity as the result of having different specialists involved in the design, development, installation, operation, and maintenance of I&C systems;

– Logic Diversity as the result of differential features between systems in terms of algorithms, logic, and program architecture, timing and/or order of execution, runtime environment, etc.;

– Signal Diversity as differences in sensed parameters to initiate safety output signal of I&C.

The described approach uses the double level classification of diversity, including the types and subtypes (attribute and criteria, correspondently). The process of diversity assessment in this case is based on application of the two levels checklist filled by the experts.

Experts should determine and mark all diversity attributes and criteria presented in I&C systems and mark them in the checklist using values ‘Yes’ or ‘No’. If some criterion is applicable in the project (marked ‘Yes’), the expert also marks INT = intentional (x). Filling the checklist with particular diversity criteria can automatically cause the appearance of corresponding diversity criteria, which either expert or tool marks as INH = inherent (i). The weight of attribute depends on rate of application of the diversity type in I&C systems.

During the calculation of diversity metrics, both marks (‘x’ and ‘i') are processed identically. After the filling of checklist the diversity metrics are calculated with application of formulas as sum of weighted values of diversity attributes and criteria. The diversity metric obtained after calculation is not normalized and can take any values in the range [0-1.76]. In this method, the diversity metric equals 1.0 is considered to be sufficient for double level I&C system.

5.3 Tool Support

A special spreadsheet-based Diversity Assessment Tool implementing mentioned checklist was developed to support described approach. The examples of obtained results are shown on Figures 1 and 2.

	Attribute criteria	Rank	DCE WT	RadICS Platform INT	INH	Score
DESIGN	Design					
	Different technologies	1	0.500			0.000
	Different approaches within a technology	2	0.333			0.000
	Different architectures	3	0.167			0.000
	DAE weight and subtotals		1.000		0.000	0.000
EQUIP.MANUF.	Equipment Manufacturer					
	Different manufacturers of fundamentally different equipment designs	1	0.400			0.000
	Same manufacturer of fundamentally different equipment designs	2	0.300			0.000
	Different manufacturers of same equipment design	3	0.200			0.000
	Same manufacturer of different versions of the same equipment design	4	0.100			0.000
	DAE weight and subtotals		0.250		0.000	0.000
LOGIC PROC.EQUIP.	Logic Processing Equipment					
	Different logic processing architectures	1	0.400			0.000
	Different logic processing versions in same architecture	2	0.300			0.000
	Different component integration architectures	3	0.200	x		0.200
	Different data flow architectures	4	0.100			0.000
	DAE weight and subtotals		0.644		0.129	0.200
FUNCTION	Function					
	Different underlying mechanisms to accomplish safety function	1	0.500	x		0.500
	Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333	x		0.333
	Different response time scale	3	0.167	x		0.167
	DAE weight and subtotals		0.600		0.600	1.000
LIFE-CYCLE	Life-Cycle					
	Different design companies	1	0.400			0.000
	Different management teams within the same company	2	0.300	x		0.300
	Different designers, engineers, and/or programmers	3	0.200	x		0.200
	Different implementation/validation teams	4	0.100	x		0.100
	DAE weight and subtotals		0.683		0.410	0.600

Fig. 1. Diversity Assessment Tool Spreadsheet (Part 1).

	Attribute criteria	Rank	DCE WT	RadICS Platform INT	INH	Score
SIGNAL	Signal					
	Different reactor or process parameters sensed by different physical effect	1	0.500	x		0.500
	Different reactor or process parameters sensed by the same physical effect	2	0.333	x		0.333
	The same process parameter sensed by a different redundant set of similar sensors	3	0.167	x		0.167
	DAE weight and subtotals		0.867		0.867	1.000
LOGIC	Logic					
	Different algorithms, logic, and program architecture	1	0.400	x		0.400
	Different timing or order of execution	2	0.300		i	0.300
	Different runtime environments	3	0.200		i	0.200
	Different functional representations	4	0.100		i	0.100
	DAE weight and subtotals		0.733		0.733	1.000
	Score(*100)			274		
	Normalized score			1.01		
	Basis for normalizing	271				
	(X) INT = intentional use					
	(i) INH = inherent use					
	Index Diversity Maximal	1.76				

Fig. 2. Diversity Assessment Tool Spreadsheet (Part 2).

The developed tool allows to automate all approach steps that are presented in the previous section. We can conclude that application of RadICS platform to develop a two-version system assures accepted level of diversity by diversifying the process and product decisions. In this case a compromise is achieved according to criteria “safety-cost”, because such system meets standard requirements to diversity and minimizes risks and cost of maintenance.

6 CONCLUSIONS

Experience obtained during this work has confirmed that there is a strong need in the development of new international standards that could cover application of diversity issues taking into consideration new aspects that appeared since issue of NUREG 7007/CR. It concerns, first of all, more detailed requirements to diversity, more detailed descriptions of possible applied techniques and tools to efficiently support qualitative and quantitative assessment.

Influence of diversity approach on cyber security of safety critical NPP I&C systems remains both interesting and challenging.

The analysis performed while using specified approach shows that diversity attributes provided for different certified design revisions of RadICS platform are compliant with NUREG 7007/CR requirements.

7 REFERENCES

1. NUREG/CR 7007-2009. *Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems*, ONL, Oak Ridge, USA, 2009.
2. ISO 26262:2011. *Road vehicles – Functional safety*
3. V. Kharchenko. Diversity for Safety and Security of Embedded and Cyber Physical Systems: Fundamentals Review and Industrial Cases. *Proceedings of 15th Biennial Baltic Electronics Conference (BEC2016)*. P. 17-26.
4. IEC 61508-1:2010 Ed.2. *Functional safety of electrical/electronic/programmable electronic safety-related systems*
5. IEEE Std 7-4.3.2-2016. *IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations*.
6. IAEA Safety Standards Series No. SSR-2/1. *Safety of Nuclear Power Plants: Design. Specific Safety Requirements*. International Atomic Energy Agency, Vienna, 2016
7. IAEA Nuclear Energy Series No. NP-T-3.17. *Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants*. International Atomic Energy Agency, Vienna, 2016
8. V. Kharchenko, O. Siora, V. Duzhyi, D. Rusin, Standard Analysis and Tool-Based Assessment Technique of NPP I&C Systems Diversity. *Proceedings of the 22nd International Conference on Nuclear Engineering (ICONE 2014).* P. 1-10.
9. Safety Automation Equipment List. RPC Radiy. FPGA-Based Safety Controller (FSC) RadICS. http://www.exida.com/SAEL/rpc-radiy-fpga-based-safety-controller-fsc-radics (2017).