2021 International Nuclear Atlantic Conference – INAC 2021
Virtual meeting, Brazil, November 29 – December 2, 2021

ISBN: 978-65-594-1256-3

Functional Analysis, Diversity and Defense-in-Depth Principle Applied for Instrumentation and Control Architecture in accordance with U.S.NRC

Claudio Siqueira Santos [1], Luciano Ondir Freire[2], and Delvonei Alves de Andrade[3]

[1] *clau.ssantos@gmail.com, Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)*
Av. Professor Lineu Prestes, 2242
05508-000 São Paulo, SP

[2] *luciano.ondir@gmail.com, Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)*
Av. Professor Lineu Prestes, 2242
05508-000 São Paulo, SP

[3] *delvonei@ipen.br, Instituto de Pesquisas Energéticas e Nucleares (IPEN / CNEN - SP)*
Av. Professor Lineu Prestes, 2242
05508-000 São Paulo, SP

1. Introduction

According to IAEA (2020), a large number of Nuclear Power Plants (NPP) is completing 30 to 40 years of operation, and many of them can extend the lifetime for variable periods of operation. Besides that, new applications and methods of NPP design are in direction of adopting Small Modular Reactors (SMR) to optimize the NPP projects in relation to cost and safety (Black et al., 2021). Other way is to apply NPP in naval plants, providing efficient manners to generate energy (Freire, 2018). All these ways can make nuclear energy a viable alternative, and consequently to contribute with low carbon power demands, and stabilize the global energy matrix helping to meet climate goals in the next decades (IAEA, 2020).

One of the sensing points in NPP project nowadays is the introduction of advanced digital Instrumentation and Control (I&C) technologies. In digital I&C design based on nuclear normative basis, it is imperative to be adherent with the safety and Human Factors Engineering (HFE) requirements. This paper proposes the formalization of a plant-level Functional Analysis (FA) methodology with Diversity and Defense-in-Depth (D3) principles, considering the U.S.NRC normative basis.

2. Methodology

The complexity involved in I&C design should lead the engineers to specify with more clearance the method of safety classification for I&C systems in a NPP. One mode to comply with the reliability

objectives is the implementation of the D3 strategy. With the coming of digital technologies some validation and verifications process (V&V) have been difficult. Some problems like different terminologies, a lack of guidelines and papers about this, and safety criteria are cause doubts by engineers, suppliers, designers, licensers, etc.

The U.S.NRC has published about it. In NUREG/CR-6303 (1994) and NUREG/CR-7007 (2010) the NRC describes methods for analyzing computer-based control systems. The application of them can contribute with a FA and D3 methodology for the overall I&C architecture design. The potential for common-mode failure (CMF) is pointed as an important issued to be evaluated, describing what portions or blocks into the I&C architecture would be uncompensated by D3 strategy. Some FA and D3 into a licensing report are U.S. EPR (AREVA, 2006), ESBWR (GE Energy Nuclear, 2006), and AP1000 (WESTINGHOUSE, 2007), for instance.

The key point of D3 method is to define the "System Block Diagram", which could be characterized in a I&C architecture (IAEA, 2018). In this way, it is necessary to have a global functional analysis (FA) to determine the system blocks and their respective functional links. The evaluation proposed by A. Chernyaev and A. Anokhin (2017) can lead to an effective interactions between the I&C teams with the process engineers, through the formalization of the FA in an overall I&C architecture. The premises of this formalization is an application of the Cognitive Work Analysis (CWA), proposed by K. Vicent (1999). CWA Derived from a functional decomposition of systems using the Work Domain Analysis (WDA), developed by J. Ramussen, A. Pejtersen and L. Goodstein (1994). In this case, every design process can be mainly linked with the availability and safety criteria, including the programs of HFE and cyber security.

Fig. 1 presents the hierarchical abstraction of FA, based on Simplified WDA (CHERNYAEV, 2017).

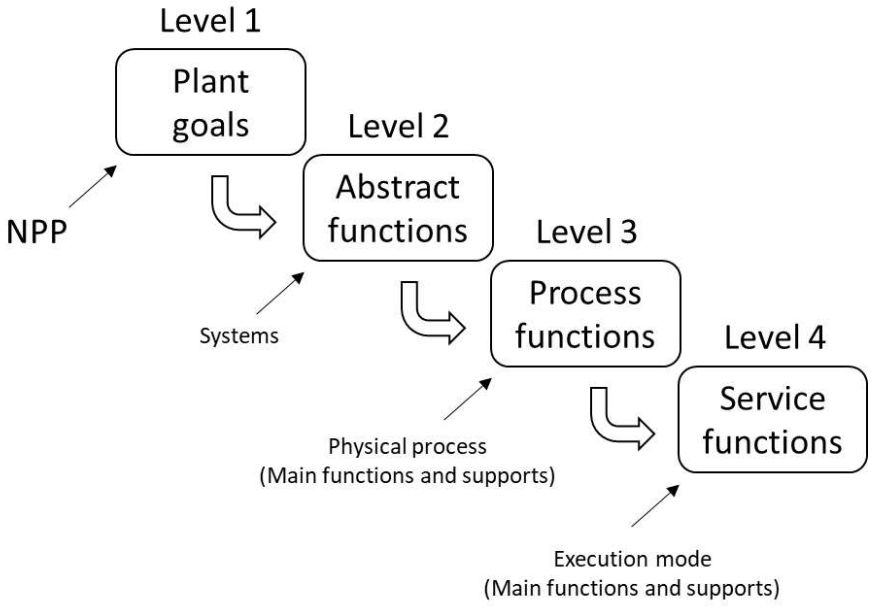

Figure 1: Functional Decomposition using Simplified WDA.

Following the U.S.NRC normative basis, based on 10CFR50 – Appendix A ("*General Design Criteria*") and with the auxiliary of the ANSI/ANS 58.14 ("*Safety and pressure integrity classification criteria for light water reactors*"), it is possible to compose a FA. In a top-down hierarchical structure Table I discriminates the plant-level functions, from high-level (Goals of the NPP), up to lower-levels, in a rationale functional decomposition strictly based on normative basis.

Table I: Hierarchical plant-level functions of a typical NPP.

Level	General NPP Objectives						
	Plant Availability				Plant Safety		
1 (Goals)	To generate energy				To prevent radioactivity releases		
2 (Abstract functions)	To control aggressions	To manage the fuel	To generate steam	To generate electricity	To ensure the integrity of the RCPB	To ensure the capability to shut down the reactor	To prevent potential off-site exposures
3 (Process functions)	(...)	(...)	(...)	(...)	(...)	(...)	(...)
4 (Service functions)	(...)	(...)	(...)	(...)	(...)	(...)	(...)

Note: (...) was used to point the fields to be defined with other several functions.

3. Results and Discussion

Using the functional decomposition based on Simplified WDA, it is possible to compose a functional tree hierarchically disposed in accordance with U.S.NRC, where the highest level plant-level functions specify the NPP goals: Energy generation and Radioactivity release prevention. According to 10CFR50 (from U.S.NRC), the three safety-related functions are necessary to ensure nuclear safety: (1) To ensure the integrity of the Reactor Coolant Pressure Boundary (RCPB); (2) To ensure the capability to shut down the reactor and maintain it in a safe shutdown condition; or (3) To ensure prevent off-site exposures.

This functional decomposition is implicitly into ANSI/ANS 58.14 and ANSI/ANS 51.1 up to level 4/5. FA is mandatory for HFE program (NUREG-0700) into U.S. NRC licensing. The use of this approach could contribute for a systematic design procedure or methodology if implemented as design basis for overall system design, and not only for HFE program. Consequently, this methodology also could assure a consistent interaction in all I&C life-cycle including traceability and consistency between the design and the cyber security and HFE programs. Beyond that, it would guarantee adherence with the regulatory criteria related to the safety, and it could facilitate the license reviews based on U.S.NRC normative basis.

4. Conclusions

In this way, it is possible to conclude that functional analysis with respective levels of D3 in a I&C architecture is a good way to organize the project activities, clarifying the scope of each design team with focus to the safety objectives defined by the whole design architecture. However, NPP lifecycles need to pay attention that there is a dynamic relationship to be considered in the implementation of new digital

I&C designs. Traditional methods can not capture all interactions necessary to implement the safety objectives, or in many cases, create rework on accomplishment of the license demands.

Quality processes with the collaboration of different disciplines inside of a NPP, including technical developers, human organizations and operators shall impress a safety culture in the whole enterprise. Moreover, methodologies shall look for models that can model the operating and safety concepts, providing relevant elements to compose the requirements to be acquired in all lifecycle. Therefore, FA complemented with D3 principles (based on regulatory requirements) are fundamentals to specify an I&C architecture.

Acknowledgements

Authors acknowledge the support and assistance of the Instituto de Pesquisas Energéticas e Nucleares (IPEN/CNEN), Universidade de São Paulo (USP), Brazil.

References

[1] IAEA – International Atomic Energy Agency, *Climate Change and Nuclear Power 2020*, Vienna & Austria (2020).

[2] G. Black, D. Shropshire, and K. Araújo, *Small modular reactor (SMR) adoption: Opportunities and challenges for emerging markets*, ELSEVIER, Boise & United States (2021).

[3] L. O. Freire, *Metodologia de especificação e projeto aplicado a usinas nucleares móveis*, IPEN/USP, São Paulo & Brazil (2018).

[4] U.S. NRC – Nuclear Regulatory Commission, *Methods for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, Washington & United States (1994).

[5] U.S. NRC – Nuclear Regulatory Commission, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control System*, NUREG/CR-7007, Washington & United States (2010).

[6] IAEA – International Atomic Energy Agency, *Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants*, NP-T-2.11, Vienna & Austria (2018).

[7] AREVA NP Inc., *U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report*, ANP-10284 Rev.0, Lynchburg & Germany (2007).

[8] GE Company, *ESBWR System Functional Requirements Analysis Implementation Plan*, NEDO-33219 Rev.0, Wilmington & United States (2006).

[9] WESTINGHOUSE Electric Company LLC, *AP1000 VCS Nuclear Station Updated Final Safety Analysis Report*, VCS UFSAR Rev.3, Pittsburgh & United States (2007).

[10] A. CHERNYAEV, A, ANOKHIN, *Formalization of the functional analysis methodology to improve NPP I&C design process*, JSC “Rusatom Automated Control Systems”, Moscow & Russia (2017).

[11] J. K. Vicent, *Cognitive Work Analysis: Towards safe, productive, and healthy computer-based work. Mahwah*, NJ: Lawrence Erlbaum Associates, New Jersey & United States (1999).

[12] J. Ramussen, A. Pejtersen and L. Goodstein, *Cognitive systems engineering*, WILEY, New Jersey & United States (1994).