

Functional analysis, diversity and defense-in-depth principle applied for instrumentation and control architecture in accordance with U.S.NRC

Análise funcional, diversidade e princípio da defesa em profundidade aplicado à arquitetura de instrumentação e controle em conformidade com o U.S.NRC

DOI:10.34117/bjdv8n4-586

Recebimento dos originais: 21/02/2022

Aceitação para publicação: 31/03/2022

Delvonei Alves de Andrade

Doutorado

Instituição: IPEN/CNEN-SP

Endereço: Avenida Lineu Prestes, 2242, Cidade Universitária, São Paulo - SP

CEP: 05508-000

E-mail: delvonei@ipen.br

Luciano Ondir Freire

Doutorado

Instituição: Marinha do Brasil

Endereço: Rua Primeiro de Março, 118 - Ed. Barão de Ladário - Centro

CEP: 20010-000 - Rio de Janeiro/RJ

E-mail: luciano.ondir@gmail.com

Claudio Siqueira Santos

Mestrado

Instituição: Amazônia Azul Tecnologias de Defesa S.A. - Amazul

Endereço: Avenida Lineu Prestes, 2468, Cidade Universitária, São Paulo - SP

CEP: 05508-000

E-mail: clau.ssantos@gmail.com

ABSTRACT

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 I&C technologies (Santos, 2021). 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.

Keywords: i&c architecture, functional analysis, defense-in-depth.

RESUMO

De acordo com a AIEA (2020), um grande número de centrais nucleares (NPP) está a completar 30 a 40 anos de funcionamento, e muitas delas podem prolongar a vida útil por períodos variáveis de funcionamento. Além disso, novas aplicações e métodos de concepção de centrais nucleares estão no sentido de adoptar pequenos reactores modulares (SMR) para otimizar os projectos de centrais nucleares em relação ao custo e à segurança (Black et al., 2021). Outra forma é aplicar a central nuclear em centrais navais, proporcionando maneiras eficientes de gerar energia (Freire, 2018). Todas estas formas podem tornar a energia nuclear uma alternativa viável e, conseqüentemente, contribuir com baixas emissões de carbono, e estabilizar a matriz energética global ajudando a cumprir os objectivos climáticos nas próximas décadas (IAEA, 2020). Um dos pontos de detecção no projecto da central nuclear nos dias de hoje é a introdução de tecnologias digitais avançadas de I&C (Santos, 2021). No projecto de I&C digital baseado na base normativa nuclear, é imperativo ser-se aderente aos requisitos de segurança e engenharia de factores humanos (HFE). Este documento propõe a formalização de uma metodologia de Análise Funcional (FA) ao nível da planta com princípios de Diversidade e Defesa em Profundidade (D3), considerando a base normativa do U.S.NRC.

Palavras-chave: arquitectura i&c, análise funcional, defesa-em-profundidade.

1 INTRODUCTION

The complexity involved in Instrumentation and Control (I&C) design should lead the engineers to specify with more clearance the method of safety classification for I&C systems in a NPP (Santos, 2021). One mode to comply with the reliability objectives is the implementation of the D3 strategy. With the coming of digital technologies some validation and verification 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, licensees etc.

Physically, the I&C systems are composed by electronic components (sensors, controllers, input and output modules, human-system interfaces, etc.). These elements execute functional demands (services) required by other systems and/or equipment which needs to be controlled. These functional demands are determined in a breakdown structure, in a decomposition of functions from high level for lower levels, in a top-down strategy.

Following this premises, it is possible to determine the control functions (lower service functions) and categorize them in accordance their respective nuclear safety classification. This step guarantee the accomplishment with the normative basis and licensing commitment demands, in the I&C architecture conception. This approach adopt the project requirements, and it tends to achieve the reliability rates required by

controlled systems in accordance with their functions.

In addition, two points were considered in this study. One point is the “Comissão Nacional de Energia Nuclear” (CNEN), otherwise the Brazilian nuclear regulation, is strongly influenced by the U.S. regulation model (Frutuoso et. al, 2012). For this reason, this paper gave attention for the standard from United States Nuclear Regulatory Commission (U.S. NRC). The second point is the I&C designs receives direct influences from Human-Factors Engineering (HFE) and Cybersecurity programs.

2 METHODOLOGY

Functional Analysis (FA) is an important process into the I&C design. With FA is possible to define the I&C components, to ensure the observability, the process controllability, specify and implement the control algorithms, adopting redundancy and diversity criteria etc. In summary, the FA assures that the I&C designs can comply with the NPP operational objectives, in a safety operation on power, start-up or shutdown situations.

One of sources of errors in the I&C design is relating the data consistency. A good management of these data could prevent and mitigate a substantial part of data inconsistencies. Almost of I&C data links should management since the higher levels of the NPP design, in a structuralized method that must decompose these links together than the functional decomposition and system allocations. For this reason, the control team shall contribute with the NPP functional analyses in the higher level defining the means and modes of the NPP control (Santos, 2021).

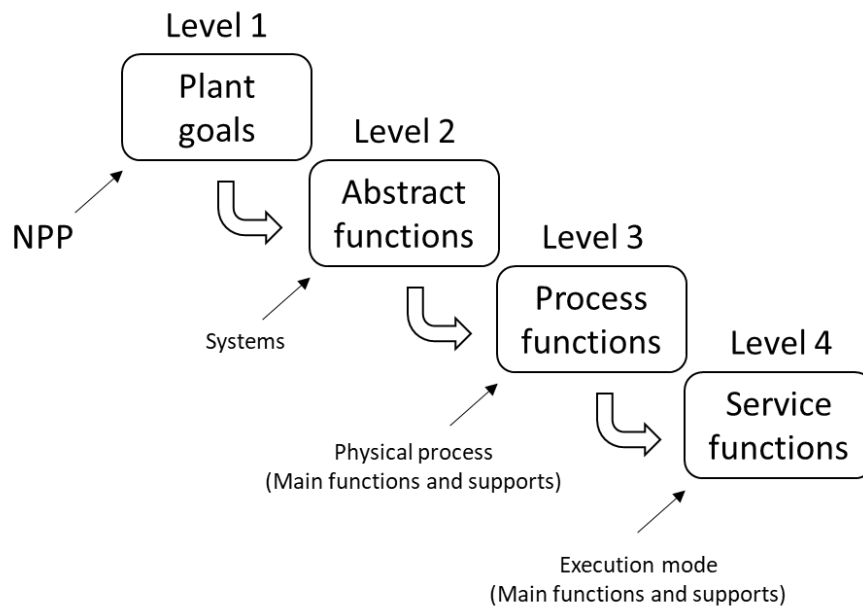
The incorporation of a global FA involving the NPP integrally is imperative. The decomposition of the functional needs to every systems and sub-systems can ensure a major reliability. The purpose of this study is merge the I&C functional analyses (that involves the active functions) with the other mechanical, supports and pressure-retaining functions (passive characteristics). The global FA approaching, including the protection barriers (passive), process control (sensors and actuators), control processing (automatic and semi-automatic commands and monitoring) and human interfaces control (manual commands and monitoring), permits an incorporation of all NPP objectives (high level principles) in I&C architecture (high level decomposition) and I&C design (lower level components).

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.



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.

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.

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] C. S. Santos, *Metodologia de especificação de sistemas de instrumentação e controle para usinas nucleares móveis*, IPEN/USP, São Paulo & Brazil (2021).
- [2] FRUTUOSO E MELO, P. F.; & OLIVEIRA, M. S.; & SALDANHA, *LWR Safety Analysis and Licensing and Implications for Advanced Reactors*, Nuclear Power - Operation, Safety and Environment. Dr. Pavel Tsvetkov (Ed.), ISBN: 978-953-307-507-5, InTech. p. 47-70, 2011.
- [3] G. Black, D. Shropshire, and K. Araújo, *Small modular reactor (SMR) adoption: Opportunities and challenges for emerging markets*, ELSEVIER, Boise & United States (2021).
- [4] L. O. Freire, *Metodologia de especificação e projeto aplicado a usinas nucleares móveis*, IPEN/USP, São Paulo & Brazil (2018).
- [5] 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).
- [6] U.S. NRC – Nuclear Regulatory Commission, *Diversity Strategies for Nuclear Power Plant Instrumentation and Control System*, NUREG/CR-7007, Washington & United States (2010).
- [7] IAEA – International Atomic Energy Agency, *Approaches for Overall Instrumentation and Control Architectures of Nuclear Power Plants*, NP-T-2.11, Vienna & Austria (2018).
- [8] IAEA – International Atomic Energy Agency, *Climate Change and Nuclear Power 2020*, Vienna & Austria (2020).
- [9] AREVA NP Inc., *U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report*, ANP-10284 Rev.0, Lynchburg & Germany (2007).
- [10] GE Company, *ESBWR System Functional Requirements Analysis Implementation Plan*, NEDO-33219 Rev.0, Wilmington & United States (2006).
- [11] WESTINGHOUSE Electric Company LLC, *AP1000 VCS Nuclear Station Updated Final Safety Analysis Report*, VCS UFSAR Rev.3, Pittsburgh & United States (2007).
- [12] 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).
- [13] J. K. Vicent, *Cognitive Work Analysis: Towards safe, productive, and healthy computer-based work*. Mahwah, NJ: Lawrence Erlbaum Associates, New Jersey & United States (1999).
- [14] J. Ramussen, A. Pejtersen and L. Goodstein, *Cognitive systems engineering*, WILEY, New Jersey & United States (1994).