Nuclear Engineering and Design 331 (2018) 194–203

Contents lists available at ScienceDirect

Nuclear Engineering and Design

journal homepage: www.elsevier.com/locate/nucengdes

Complexity reduction of the Engineered Safety Features Component Control System

Joyce Mayaka, Jae Cheon Jung*

Department of Nuclear Power Plant Engineering, KEPCO International Nuclear Graduate School, 1456-1, Shinam-ri, Seosaeng-myeon, Ulju-gun, Ulsan 689-882, Republic of Korea

ARTICLE INFO

Keywords:
Field Programmable Gate Arrays
Nuclear facility regulation
McCabe's cyclomatic complexity
Software metrics

ABSTRACT

A complexity reduction methodology for the ESF-CCS (Engineered Safety Features- Component Control System) based on system analysis is developed in this work. The primary objective of this work is to demonstrate that the adoption of an FPGA (Field Programmable Gate Array) based architecture results in a decrease in the system complexity. The concepts of complexity and complexity metrics, as well as the ways in which the FPGA platform can result in a decrease in complexity, are defined. Following this, an analysis of the ESF-CCS is performed. The sources of complexity are identified and the system complexity is measured using McCabe's cyclomatic complexity metric. An FPGA-based design with reduced complexity is then presented. The reduction in complexity is achieved by the use of flat hardware logic, System on Chip architecture, and the separation of logically independent functions. By adopting an FPGA architecture, the control logic can be reduced to around a half. This reduction in complexity results in systems with higher reliability, which are easier to test and maintain.

1. Introduction

The Instrumentation and Control (I&C) systems in Nuclear Power Plants (NPP) are responsible for the sensing of plant parameters and the regulation of plant processes. In particular, the safety systems are responsible for shutting down the reactor in the event of Anticipated Operational Occurrences or accident conditions. These systems also actuate the Engineered Safety Features (ESF) to prevent the release of radioactive material and damage to the nuclear plant. Traditionally, the safety systems have been implemented using analog technologies, which are becoming increasingly obsolete. As a result, the legacy I&C systems are being replaced with modern digital electrical technologies, which offer numerous advantages such as the capability for self-testing, drift-free operation and advanced Human-System Interfaces (Fink et al., 2011). The predominant technology that has been used is microprocessor-based Programmable Logic Controllers (PLCs). However, this technology has several drawbacks such as high complexity and rapid obsolescence.

To cope with these shortcomings, Field Programmable Gate Arrays (FPGAs) have been proposed as an alternative technology. FPGAs are programmable devices composed of logic blocks linked through programmable interconnects. They are large-scale integrated circuits fabricated without any application-specific functionality, where the internal architecture is configured for a specific application after production through the use of Hardware Description Languages (HDL) such as VHDL and Verilog. Unlike microcontroller or computer-based technologies, FPGAs do not contain any operating system or middleware, only logic gates and interconnections. FPGAs have been used in multiple industries and are gaining increased attention as an alternative digital platform to PLCs in NPP I&C systems, particularly for safety applications. FPGAs offer numerous advantages such as portability, reconfigurability, and high speed of operation. In addition, this architecture promises a reduction in the complexity of the developed system as the final product, like traditional analog electronics, can be designed to consist of only hardware. Despite the fact that the final FPGA product is hardware, the design and implementation strategies are similar to those of a software-based system (Bobrekl, 2010). Previous studies have looked into design life cycles and methodologies for safety critical FPGA-based I&C systems (Chen, 2011; Jung and Ahmed, 2016).

Further, as the safety systems are responsible for preventing damage to the reactor and the release of radioactive material, they must be developed to a high level of reliability. Reliability is the probability that a system functions correctly for a given time period (U.S. Nuclear Regulatory Commission, 2001). Reliability analysis of FPGA-based I&C systems using dynamic flow graphs and fault trees has been carried out (McNelles and Lixuan, 2016; McNelles et al., 2016). However, no study has looked into the complexity of FPGA-based instrumentation and control systems. Complexity is considered to be an indicator of system

* Corresponding author.
E-mail addresses: jmayaka@email.kings.ac.kr (J. Mayaka), jcjung@kings.ac.kr (J.C. Jung).

https://doi.org/10.1016/j.nucengdes.2018.01.003
Received 11 August 2017; Received in revised form 19 December 2017; Accepted 2 January 2018

reliability (U.S. Department of Transportation Federal Aviation Administration, 1991; Fink et al., 2009); the lower the system complexity, the easier it is to verify, validate and maintain, all of which point to an increase in reliability. The aim of this work is to demonstrate that the adoption of the FPGA architecture results in a decrease in system complexity. In this study, a design of the Engineered Safety Features Component Control System (ESF-CCS) that exploits the advantages of FPGAs was developed. Further, the complexity of the developed system was computed using McCabe's cyclomatic complexity metric and was determined to be significantly less than that of the PLC-based system.

This paper is structured as follows. Section 2 introduces the concepts of complexity and complexity metrics. In Section 3, the FPGA architecture and its advantages are presented. A description of the current PLC-based system and an analysis of its complexity is then presented in Section 4. Subsequently, an improved architecture based on FPGA technology is detailed in Section 5, with a conclusion given in Section 6.

2. Complexity and complexity metrics

2.1. Complexity

IEEE Std. 610.12 defines complexity as the "degree to which a process is difficult to analyze, understand or explain" (IEEE Standard Glossary of Software Engineering Terminology, 1990). When evaluating a system design from a safety perspective, the simpler design options are those that accomplish the function with the most confidence and the least ambiguity (U.S Nuclear Regulatory Commission, 2013). Therefore, the evaluation of the system complexity enables design choices to be justified or altered if the complexity is found to be too great.

Although there are no regulations, standards, or guidance to address the aspect of simplicity for digital I&C systems in NPPs, complex I&C systems challenge the demonstration of conformance with safety systems design criteria such as independence, reliability, and maintainability. In this context, the U.S. Nuclear Regulatory Commission (NRC) (U.S Nuclear Regulatory Commission, 2013) considers simplicity "as supporting all fundamental design principles for developing safety systems with high reliability".

The detection and correction of complexity problems can be achieved if the system architecture is evaluated before going on to the next phase of development. Empirical studies referred to by McCabe (1976) show that there is a positive correlation between the measured complexity and the number of errors found in the implemented system. Furthermore, the prediction and subsequent reduction of complexity have been found to result in large savings in maintenance costs and efforts (Stark et al., 1994; Chidamber and Kemerer, 1994) . Therefore, the simpler a system is, the easier it is to implement, verify, maintain, and the less likely it is to contain latent errors.

2.2. Complexity metrics

Quality Metrics are measures whose purpose is to quantify quality-factors of a system, such as reliability, maintainability, and testability (U.S. Department of Transportation Federal Aviation Administration, 1991). Metrics that are an indication of the quality factors are computed during the life cycle development process in order to validate to what extent, the factors have been met. Complexity is an indicator of the system reliability. However, there are several characterizations of system complexity (Cardoso, 2005):

1) Task Complexity: The number of tasks in a process.
2) Control Flow Complexity: The arrangement of tasks in a process and the associated decision points.
3) Data Flow Complexity: The degree of dependency of the information objects and their mapping to tasks and resources.
4) Resource Complexity: The level of coupling between resources and their allocation to tasks.

Selecting a metric is therefore dependent on the facet of complexity of interest.

Over the past four decades, numerous complexity metrics have been developed. De Silva et al. (De Silva et al., 2012) define at least 20 complexity metrics in chronological order, beginning with McCabe (1976) in 1976, down to Cardoso (2005) in 2008. Each of these metrics defines complexity as a function of different aspects of the system. For instance, Halstead's (1977) calculation is based on operators and operands of a software program while Kafura and Henry (1981) define complexity as a function of the data flow between modules. For real-time safety systems in nuclear power plants, Preckshot (1993) suggests using either Halstead's, McCabe's or Henry's metrics as they call for fewer subjective judgments.

Additionally, different metrics are suited for use at different stages of the life cycle process. The earlier the metric is used, the easier and more cost-effective it is to identify complex system modules and correct them. Smidts and Li (2000) ranked different metrics for their applicability in different life cycle phases, based on expert opinion. Cyclomatic complexity was ranked in the top 3, for both the design and implementation phases. Further, in NUREG/CR 1042, cyclomatic complexity was identified as a measure for use during the Design, Coding, Testing, and Operation phases to predict the reliability of software in nuclear safety-critical applications (Smidts et al., 2011). Thus, as this study is aimed at reducing and computing complexity at the design phase, Cyclomatic complexity was chosen as a suitable metric.

Cyclomatic Complexity is a measure of the control flow complexity of a system. This metric is derived from a flow graph and is mathematically computed using graph theory. In the graph, each node corresponds to a section of code in which the flow is sequential. The arcs are representative of branches in the program. The Cyclomatic complexity of a graph, with n vertices, e edges, and P connected components is calculated as:

$$v(G) = e - n + P \quad (1)$$

The complexity computed is equal to the maximum number of linearly independent paths – basis paths – in the program.

The cyclomatic complexity metric measures the amount of decision logic in a function and is independent of the programming language (Watson and McCabe, 1996) since most languages utilize the same decision structures. Thus, a computed complexity value will have the same meaning regardless of which language the source code was written in. This means that a comparative analysis of the complexity of systems developed using different languages is possible, as the computed cyclomatic complexity is a function of the structure of the logic only.

McCabe extended his original work so that the principles used in the calculation of program complexity could be used to compute the complexity of the design architecture (McCabe and Butler, 1989). In this context, architectural design is defined as the framework or structure of a system with its associated functions and control interrelationship. McCabe postulates that the design reliability is enhanced when design complexity is quantified and limited, and when the integration and testing process is driven by design metrics. This allows the software designer to measure the system complexity and understand its implication before proceeding to implement the system.

3. Digital architectures

Currently, most safety critical digital I&C systems are implemented on PLC platforms. Table 1 gives a comparison of FPGA and PLC systems based on multiple criteria.