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

ISBN: 978-65-594-1256-3

Hardware for IIoT in mission-critical nuclear applications

S. F. Marcos[1] and D. G. J. Guilherme[2],

[1]*msantana@ien.gov.br, Instituto de Engenharia Nuclear – Universidade Estácio de Sá*
[2]*gdjaime@ien.gov.br, Instituto de Engenharia Nuclear – Universidade Estácio de Sá*

1. Introduction

Digitalization has been a mainstream driving theme throughout sectors and society in recent years. Rapid advances in wireless communication and Internet of Things (IoT)-related technologies have produced new business opportunities and services. When IoT principles are utilized in industrial plants and processes, it is referred to as Industrial IoT (IIoT) [1]. As the IIoT becomes more widespread, it will totally transform how the industry interacts with data. It will also have a significant influence on mission-critical IIoT devices and the applications that they support. Mission-critical IIoT frequently includes a set of requirements, such as ultra-high reliability, which allows devices to operate in harsh conditions and at remote locations for extended periods; precision and accuracy in production operations; and security and resiliency to defend networks against attacks. This work aims to propose a reconfigurable hardware architecture model with ultra-high reliability for use in systems to mission-critical IIoT in nuclear applications.

2. Methodology

The IIoT is a growing technology that is expected to soon have a significant impact in nuclear applications. Although there are certain doubts and roadblocks to IIoT adoption in nuclear area, many nuclear field stakeholders and research groups are looking into ways to overcome impairments unique to the nuclear sector [2]. Success in mission-critical IIoT necessitates creativity. So, to take it to the next level, innovation must occur across all layers of the IIoT ecosystem, including the device layer, the wireless communications layer, and the network infrastructure layer. In this paper, we present a device layer solution, using redundant digital sensors to create a high-reliability measuring system for nuclear applications.

Fig. 1 illustrates the proposed redundant digital sensing system. Digital data from three redundant sensors and one spare sensor are made available to the proposed hardware architecture. The proposed hardware relies on a classic active redundancy model, the Triple Modular Redundancy (TMR) with one spare. This hardware model uses comparators, multiplexer, and a state machine-based control unit to respond with a high degree of reliability. The proposed solution is implemented in a Field Programmable Gate Array (FPGA) [3] device, using the VHDL [4] language.

In Fig.1, the controller gets the results from the comparators and runs a finite state machine (FSM) to detect failed redundant sensors and send a control signal to the multiplexer. The controller's main function is to keep track of the status of the redundant sensor modules and detect any faults. The outputs of these sensors are compared in pairs to discover the faulty redundant sensor module. Each comparison result signal is forwarded to the controller, which supervises the fault detection process through a state machine. The control signals from the controller and the output sensor modules are received by the multiplexer. The multiplexer uses the control signals from the controller to select one of the redundant sensors’ outputs.

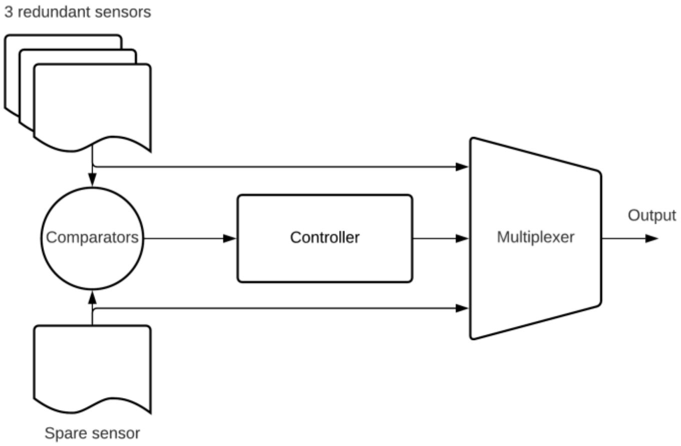

Figure 1: Proposed redundant sensing system

3. Results and Discussion

The measurement of reliability R reflects the probability of a fault not occurring throughout the system's operation time [5]. The assumption that failure occurrences in separate modules are mutually independent is common in redundant systems [6]. The Reliability Block Diagram (RBD) [7], which is a way for demonstrating how the reliability of modules contributes to the success or failure of a system, may be used to estimate the reliability.

TMR systems with voters are known to work adequately if two of the three modules are operational. Considering that the faults in the redundant modules are mutually independent, the system's reliability is given by the sum of the probabilities that at least two modules are functioning correctly. Since R is the reliability of each module and $(1-R)$ is the corresponding probability of failures, the reliability R_{TMR} of the system can be given by (1):

$$R_{TMR} = R^3 + 3(1-R)R^2 = 3R^2 - 2R^3. \quad (1)$$

As a strategy, the architecture must include additional characteristics in addition to the feature of masking a failure, so that a future fault does not produce an erroneous response. In this instance, the design necessitates a monitoring structural standard capable of detecting and locating a problem, allowing a type of restructuring to be utilized and the failed module to be separated and replaced with a spare. TMR-With-Spares systems combine the TMR with redundancy by replacement, two well-known redundancy principles. In this active system, the spares are a replacement unit. When one of the fundamental TMR modules failures, it is replaced with an identical spare module, which restores the TMR core. Under these conditions, the system's reliability may be calculated by adding the probabilities of situations in which the system functions properly, in this example when any two modules are operational. The reliability of TMR-with-spares models is defined as in (2):

$$R_{TMR/S} = \sum_{k=2}^{N=3+S} \binom{N}{k} R^k (1-R)^{N-k}, \quad (2)$$

where S is the number of used spares modules. Using (2), $R_{TMR/1}$ for TMR with-one-spare reliability is defined as in (3):

$$R_{TMR/1} = 3R^4 - 8R^3 + 6R^2. \tag{3}$$

Fig. 2 presents a comparison of the reliability of the models simple (without redundancy), TMR and TMR/1 (TMR with-one-spare) concerning system reliability vs. reliability of a sensor module. As predicted, the improvement in reliability is considerable. As a result, a system for mission-critical IIoT in nuclear facilities may be created using sensors with lesser reliability but at a cheaper cost. Missions can also retain acceptable reliability over considerably longer periods. For example, if a sensor's response reliability falls to 0.8, the reliability of TMR system remains at 0.896 and the reliability of the proposed redundant system remains at 0.973.

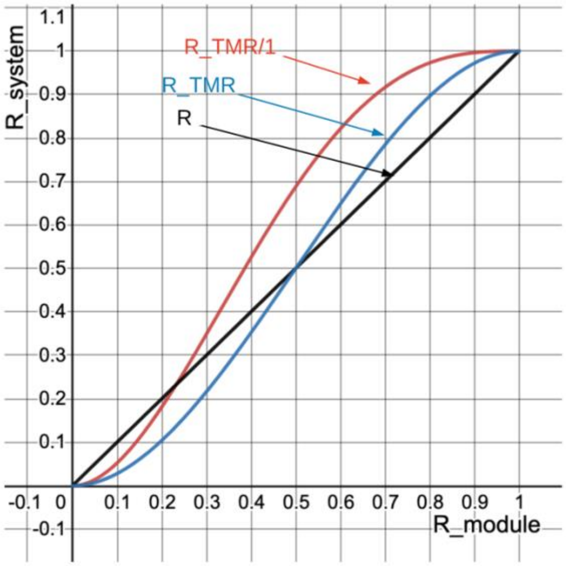

Figure 2: Comparison between the reliability of models.

The proposed architecture must continue to monitor the faulty module, and if the issue is determined to be temporary, the initial configuration must be resumed. This is an enhancement to the TMR-with-spares model that the proposed architecture adds: the ability to retain information about faulty modules and revert to the previous configuration when the temporary fault ceases to exist.

4. Conclusions

Mission-critical applications at nuclear plants are crucial because they deal with hazardous situations, and their failure can result in significant losses. All components of the mission-critical IIoT, including sensors, actuators, and processing systems, must be kept at a low failure rate. As a result, the growth of hardware designs to improve the reliability of mission-critical IIoT systems can effectively contribute to the advancement of these applications. Reconfigurable hardware devices, particularly FPGA devices, are gaining relevance in IIoT applications due to the flexibility they provide in creating high-performance signal processing and control systems. Mission-critical IIoT applications can take advantage of the FPGA device structure in capturing sensor data, processing this data, and routing this data across diverse networks to reach the servers. This work demonstrated the development of FPGA-based hardware that serves as a controller in redundant sensors' architecture based on TMR-with-one-spare. The improved reliability enables the deployment of redundant IIoT device layer solutions in mission-critical applications such as nuclear.

Acknowledgements

The authors gratefully acknowledge the infrastructure and financial support of Programa de Pesquisa Produtividade – Universidade Estácio de Sá, and Instituto de Engenharia Nuclear.

References

[1] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang and J. Rodriguez, "Massive Internet of Things for Industrial Applications: Addressing Wireless IIoT Connectivity Challenges and Ecosystem Fragmentation," in IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 28-33, March 2017, doi: 10.1109/MIE.2016.2618724.

[2] Farley, David Rushton, Negus, Mitch G., and Slaybaugh, Rachel N. "Industrial Internet-of-Things & Data Analytics for Nuclear Power & Safeguards." United States: N. p., 2018. Web. doi:10.2172/1481947.

[3] Korea Atomic Energy Research Institute (KAERI), Survey of the CPLD/FPGA Technology for Application to NPP Digital I&C System, Tech. Rep., 2009.

[4] IEEE Standard VHDL Language Reference Manual, in IEEE Std 1076-2008 (Revision of IEEE Std 1076-2002), Jan. 26 2009. doi: 10.1109/IEEESTD.2009.4772740.

[5] M. L. Shooman, "Introduction, in Reliability of Computer Systems and Networks: Fault Tolerance, Analysis And Design". John Wiley & Sons, Inc., New York, NY, USA, 2002.

[6] E. Dubrova, *Fault-Tolerant Design: An Introduction*. Kluwer Academic Publishers. 2008.

[7] M. Cepin, Reliability Block Diagram. Inn: *Assessment of Power System Reliability*. Springer, London, 2011.