Hardware resilience: a way to achieve reliability and safety in new nuclear reactors i&c systems

M. S., Farias[1], P. V. R., Carvalho[1], N., Nedjah[2]
e-mail: msantana@ien.gov.br, paulov@ien.gov.br, nadia@eng.uerj.br

[1]*SEINS, IEN;* [2]*UERJ*

Keywords: nuclear reactors, hardware resilience, safety-critical systems

The idea that systems have a property called 'resilience' has emerged in the last decade [1]. In this work we intend to bring the idea of resilient systems for the hardware applied in safety-critical systems, such as the new nuclear reactor instrumentation and control (I&C) systems. Basic concepts of resilience in complex systems were analyzed from the point of view of hardware architectures, leading to linkages between concepts and methods for resilience using an approach based in HDL programmable devices.

The flexibility found in processor and software-based systems pose a major challenge for critical applications, as the complexity involved in guaranteeing that these systems keep their reliability is something massive. Developing architectures for critical systems closer to hardware, with less reliance on processors and software, has proven to be a good choice for the development of reliable systems in new projects [2]. We examined basic concepts of resilience applied to hardware, indicating architectures that can satisfy these concepts.

- Resilience and Robustness - In hardware, robustness can be seen as redundancy. Triple Modular Redundancy (TMR) has become the most common practice because of its straightforward implementation and reliable results. Figure 1 shows a triple-redundant module with a single voter at the output.
- Resilience and Return to Equilibrium - For transient faults, a way to achieve a return to equilibrium in hardware is to use temporal redundancy. For this it is necessary to identify a failed module and repeat the execution. Comparators should be used in conjunction with, at least, two redundant modules to be able to identify a failed module. Figure 1 shows this approach.
- Resilience and "Extra Adaptive Capacity"- Thinking about the hardware we are trying to preserve from failures, a surprise event that challenges its limits would be when a failure occurs in two redundant modules and become permanent. The hardware architecture to mitigate faults of this type would have to use the techniques previously presented to mask (TMR) and detect (comparison) the faulted module, replacing this faulting module with a spare module (or reconfiguring the module) before a second module fails.

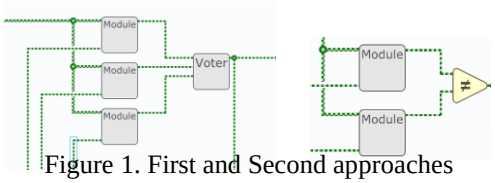

Figure 1. First and Second approaches

Using functions in Labview, the failure injection (FI) in the module is simulated by randomly changing the value of the bit in its output. The injection of a fault is done in the same module and at the same time in all three hardware architectures. Table 1 shows the results.

Table 1 – Simulation results

	First approach	Second approach	Third approach
FI	17963	12041	17963
Output changed	85	214	78
Percentage	0,473%	1,777%	0,434%

As expected, the third approach, which masks and detects the failed module, has proved more resilient to mitigate failures. However, the improvement is not so significant in relation to the first approach, TMR only. The great advantage of this approach will be to mitigate permanents failures in a module. Permanent changes, simulating a permanent hardware failure, will be evaluated later. The simulations have shown that these hardware architectures work efficiently to mitigate module failures, allowing subsequent studies to use these approaches to assess the resilience of critical systems using FPGA.

References

[1] WOODS, D. D. Four concepts for resilience and the implications for the future of resilience engineering. **Reliability Engineering and System Safety,** [S.l.], v. 141, p. 5-9, set. 2015. Disponível em: <http://dx.doi.org/10.1016/j.ress.2015.03.018> Acesso em: 1 mar. 2018.

[2] O'NEILL, K.; NEWELL, G. R.; ODIGA, S. K. Protecting flight critical systems against security threats. In: DIGITAL AVIONICS SYSTEMS CONFERENCE. 35., 2016, Sacramento, CA. **Anais…** Whashington: IEEE, 2016, p. 1-7.