Proceedings of the 5th International Conference on Integrity-Reliability-Failure, Porto/Portugal 24-28 July 2016
Editors J.F. Silva Gomes and S.A. Meguid
Publ. INEGI/FEUP (2016)

PAPER REF: 6201

IEC 61499 REPLICATION FOR FAULT TOLERANT SYSTEM

Adriano A. Santos[1(*)], Mário de Sousa[2], Pessoa Magalhães[3], António F. da Silva[1]
[1]Department of Mechanical Engineering (DEM), ISEP/IPP, Portugal.
[2]Department of Electrical and Computer Engineering (DECE), FEUP/U.Porto, Portugal.
[3]Department of Mechanical Engineering (DEM), University of Porto, Portugal.
[(*)]*Email:* ads@isep.ipp.pt

ABSTRACT

The IEC 61499 was developed thinking about the new generation of distributed control and automation systems. This provides essential resources for the development of distributed systems such as encapsulation, portability and reconfiguration. In this sense, and to ensure confidence in the operation should be implemented fault tolerance techniques dealing with hardware failures and errors off software associated with us where the distributed application runs. In this paper, we propose an approach to deal with failures in distributed systems tolerance problems, based on a replication model based on replication software/hardware as a means to achieve confidence in the operation.

Keywords: IEC 61499, distributed systems, fault tolerance, replication, function block.

INTRODUCTION

Industrial control applications are based on programmable logic controllers (PLCs). These applications are programmed using standard languages defined according to IEC 61131 (IEC 1993). The connection of multiple PLCs through a communication network meant that these applications are transformed into control systems distributed where in most of them, it is necessary to complement them with real-time synchronization and attributes of fault tolerance so as to provide necessary confidence in the operation. The new architecture IEC 61499 (IEC, 2005) was designed to integrate several known solutions for distributed automation problems. It can be said that the IEC 61499 standard proposes a programming language at the level of distributed control systems that bridges the gap between PLCs programming languages and distributed systems (Vyatkin, 2009).

Associated with the distributed nature of the control applications, new challenges must be taken into account, including, reliability, allowing the introduction of techniques for fault tolerance in the application architecture by implementing the components of replication (hardware or software entities). Replication should be performed only for critical software components, by running a single copy of the non-critical components. This approach ensures that if any one replica fails, the remaining replicas continue in operation, they are able to mask the presence of the replica fails before the rest of the application for which the system will continue in operation. It should be noted that in order to tolerate the failure of replies, it is necessary $2 \times f + 1$ replicas to tolerate f faults. So that can tolerate a single failure in a process P it is necessary replicated them in a three devices and dividing in three equivalent processes P (1, 2 and 3), Fig. 1. After the execution the result R (1, 2 and 3) it must be consolidated in the next step yielding the result R. The decision results of a vote process using for this purpose one of several voting algorithms (2 in 3, mean, median, etc.) (Storey, 1996).

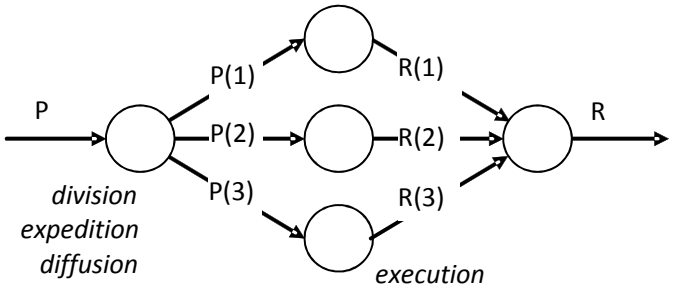

Fig. 1 - Triple Modular Redundancy (TMR)

The choice of the voting algorithm depends on the application semantics and the need to stay synchronized the application so, the consistency and synchronization of internal states and interactions between replicas will not be an easy task (Santos, 2008).

RESULTS AND CONCLUSIONS

The IEC 61499 has proved to be an important working tool used for the development of distributed control systems, reconfiguration and fault tolerance.

In this paper, we present an analysis of the replication process, the interfaces and mechanisms to ensure the correct functioning of the flow of information between replicas and determinism and synchronization of same. Moreover, the use of TMR systems with triplicate voter not only ensures a reliable system at the hardware level, tripling the active equipment, as well as the software level, active dynamic redundancy, increasing the system availability and reliability.

The proposed model provides to the system software support that enables secure communication between the replicated elements. This provide the communication interface, backed by a modification of SIFB (Service Interface Function Block), the atomic diffusion mechanisms and the algorithm used for voting replicated data. The synchronization of replicas is obtained based on time delivery by the support software needs to know Worst Case Execution Time to ensure that all replicas receive the same events/data at the time they are shipped. The support software ensures that all replicas receive the new values.

REFERENCES

[1]-International Electrotechnical Commission, International Standard IEC 61131-3, Programmable Logic Controllers, Geneva, 1993.

[2]-International Electrotechnical Commission, International Standard IEC 61499-1, Function Block Architecture Part 1, Geneva, 2005.

[3]-Santos, Adriano A. e Sousa, Mário de. Framework for Management of Replicated IEC 61499 Applications. In 13th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA'08), 2008, p. 200-206.

[4]-Storey, Neil. Safety Critical Computer Systems. Addison-Wesley, Pearson/Prentice Hall, 1996.

[5]-Vyatkin, Valeriy. The IEC 6149 Standard and Its Semantics. In IEEE Industrial Electronics Magazine, 2009, Vol. 3(4), p. 40-48.