Invitation à la soutenance publique de thèse de
Emery Kouassi ASSOGBA
Ingénieur civil, Master en Sciences Informatiques
Pour l’obtention du grade de Docteur en sciences
« Application Hardening by Adapting an Open-Source Operating System »
qui se déroulera
le mardi 27 août 2019 à 10h
Auditoire BARB 92
Place Sainte Barbe
1348 Louvain-la-Neuve

Jury members :
Prof. Marc Lobelle (UCLouvain), promoteur
Prof. Eugène C. Ezin (UAC, Bénin), promoteur
Prof. Charles Pecheur (UCLouvain), président
Prof. Olivier Bonaventure (UCLouvain), secrétaire
Prof. Jean-Didier Legat (UCLouvain)
Prof. Herbert Bos (VUAmsterdam, Pays-Bas)
Dr. Marc Durvaux (Industrie, Belgique)

Computers embedded in satellites are sensitive to cosmic radiations. These cause transient faults that must be avoided or corrected. The thesis proposes a new method of detection and correction of these faults. The method protects application programs running on these computers without having to modify them or know what these programs are doing. The method, called "blended hardening technique", exploits the capabilities of some processors to detect some errors and report them to the operating system. Errors not detected in this way by the hardware are detected in software by dividing the program into processing elements (PE) short enough (max 250μs) to not have to worry about more than one fault during a PE execution. Each PE is run twice and the results are compared. When the results differ or when a fault has been reported to the OS, the PE is simply restarted.
The hardening method includes several technical innovations. The first is that the choices are based on hypotheses based on realistic statistical analysis in order to be able to guarantee the efficiency of the protection. The second is a new instruction counting technique allowing to execute exactly twice the same instructions without any knowledge of what the program does. A third innovation is an efficient way of using the pagination system for the protection of the memory of a process against erratic behaviors of this process if it is hit by a SEU. All this has been implemented in the micro-kernel OS Minix3 and tested by faults injection. The overhead is usually 1 to 2 times the execution time of the program. Faults have been injected into critical processor registers at random times at a typical rate observed in open space conditions. All injected faults have been detected and corrected.