Study of autonomous response and recovery mechanisms for embedded systems

Zoé Lagache*[1,2], Pierre-Henri Thevenon[1], Maxime Puys[3], and Oum-El-Kheir Aktouf[2]

[1]Commissariat à l'énergie atomique et aux énergies alternatives - Laboratoire d'Electronique et de Technologie de l'Information – Direction de Recherche Technologique (CEA) – France

[2]Laboratoire de Conception et d'Intégration des Systèmes – Université Grenoble Alpes, Institut polytechnique de Grenoble - Grenoble Institute of Technology, Institut Polytechnique de Grenoble - Grenoble Institute of Technology – France

[3]Laboratoire d'Informatique, de Modélisation et d'Optimisation des Systèmes – Ecole Nationale Supérieure des Mines de St Etienne, Centre National de la Recherche Scientifique, Université Clermont Auvergne, Institut national polytechnique Clermont Auvergne – France

Résumé

Embedded systems are increasingly numerous, complex and connected, and are used in critical environments such as healthcare systems and industrial systems. The security of embedded systems is essential to ensure the proper functioning of these applications. Conventional security mechanisms often rely on human intervention, which can be impractical or ineffective in real-time scenarios. Autonomous recovery mechanisms, which can mitigate, repair and respond to security attacks without human intervention, offer a promising approach to improve the security of embedded systems. This article presents a state of the art of autonomous recovery and response for the security of embedded devices after the detection of an undesirable event with consideration of their critical functions.

*Intervenant