Comparision of various approaches in Fault-Tolerant and Attack-Resistant system design

Filip Štěpánek, Martin Novotný

Faculty of Information Technology
Czech Technical University in Prague
{filip.stepanek, martin.novotny}@fit.cvut.cz

Abstract. Fault-tolerance and attack-resistance are often discussed properties of embedded systems but are rarely achieved at the same time. The deployment of fault-tolerant systems demands some kind of reliability in hazard environment or the possibility of recovery in case of failure of the system to protect human lives or to prevent damage to property. The attack-resistant devices on the other hand protect the secrets/money or some other sensitive information of others from being misused or stolen. But as the number of attacks on software systems become more frequent and as the required education of attackers keeps decreasing, the question is – "When the safety-critical systems become target of malicious attacks?" The aim of this presentation is to discuss various fault tolerant and attack resistant system design approaches, to find common properties and to compare them to the ordinary design flow of the embedded systems. The goal of this work is to discuss the possibility of having both fault-tolerance and attack-resistance in embedded systems at the same time.