Sûreté de fonctionnement des systèmes critiques
Diagnostic et tolérance aux fautes
Ecole Centrale de Lille – Jeudi 25 octobre 2012

Tolérance aux pannes et architecture d'un Système Instrumenté de Sécurité

Bertrand Ricque
Chef de Programme – Sagem Défense Sécurité
+33 6 87 47 84 64 – bertrand.ricque@sagem.com

Key-words: *IEC61508, IEC61511, IEC62061, ISA S84, SIS, architectural constraints, Safe Failure Fraction, SIF, system engineering, hardware fault tolerance*

The IEC 61508 series standards are based on restrictive hypothesis concerning the Safety Instrumented Systems and their actions. This talk highlights the consequences of these hypotheses.

We first review the definitions of the terms used by the standards and draw some conclusions with respect to recursivity in the architectures. We propose a classification of the situations of the Safety Instrumented Systems in relation with the risk they are supposed to reduce. We show that some base concepts of the standards, such as the safe failure fraction (SFF), are not applicable in all the cases.

We propose a structured architecture engineering methodology for the Safety Instrumented Systems able to solve the exceptions where the strict application of the standards is impossible.

Mots clés : *IEC61508, IEC61511, IEC62061, ISA S84, SIS, contraintes d'architecture, fraction de panne sure, ingénierie système, tolérance aux pannes matérielles*

Les normes issues du référentiel IEC 61508 sont basées sur des hypothèses restrictives sur la structure et les actions des systèmes instrumentés de sécurité. Cet exposé met en évidence les conséquences de ces hypothèses.

Nous rappelons d'abord les définitions des termes employés dans les normes en tirons des conclusions vis-à-vis de la récursivité dans les architectures. Nous proposons ensuite une classification des situations des Systèmes Instrumentés de Sécurité par rapport au risque qu'ils sont censés réduire. Nous montrons que certains concepts fondamentaux des normes, comme la fraction de panne sûre (SFF) ne sont pas applicables dans tous les cas.

Nous proposons ensuite une méthode structurée de construction des architectures des Systèmes Instrumentés de Sécurité permettant de résoudre les exceptions pour lesquels l'application stricte des normes est impossible.