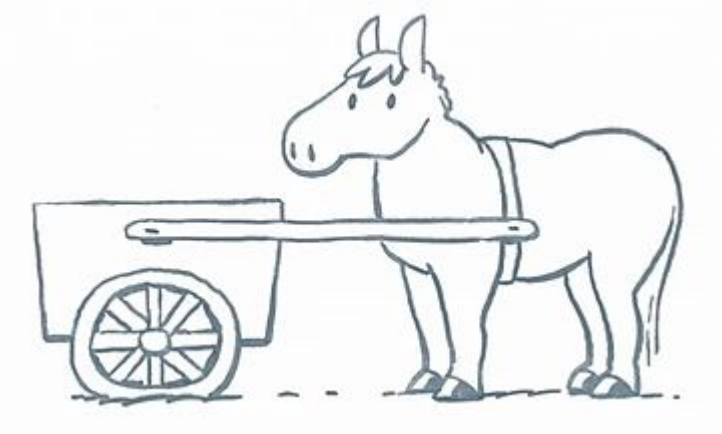
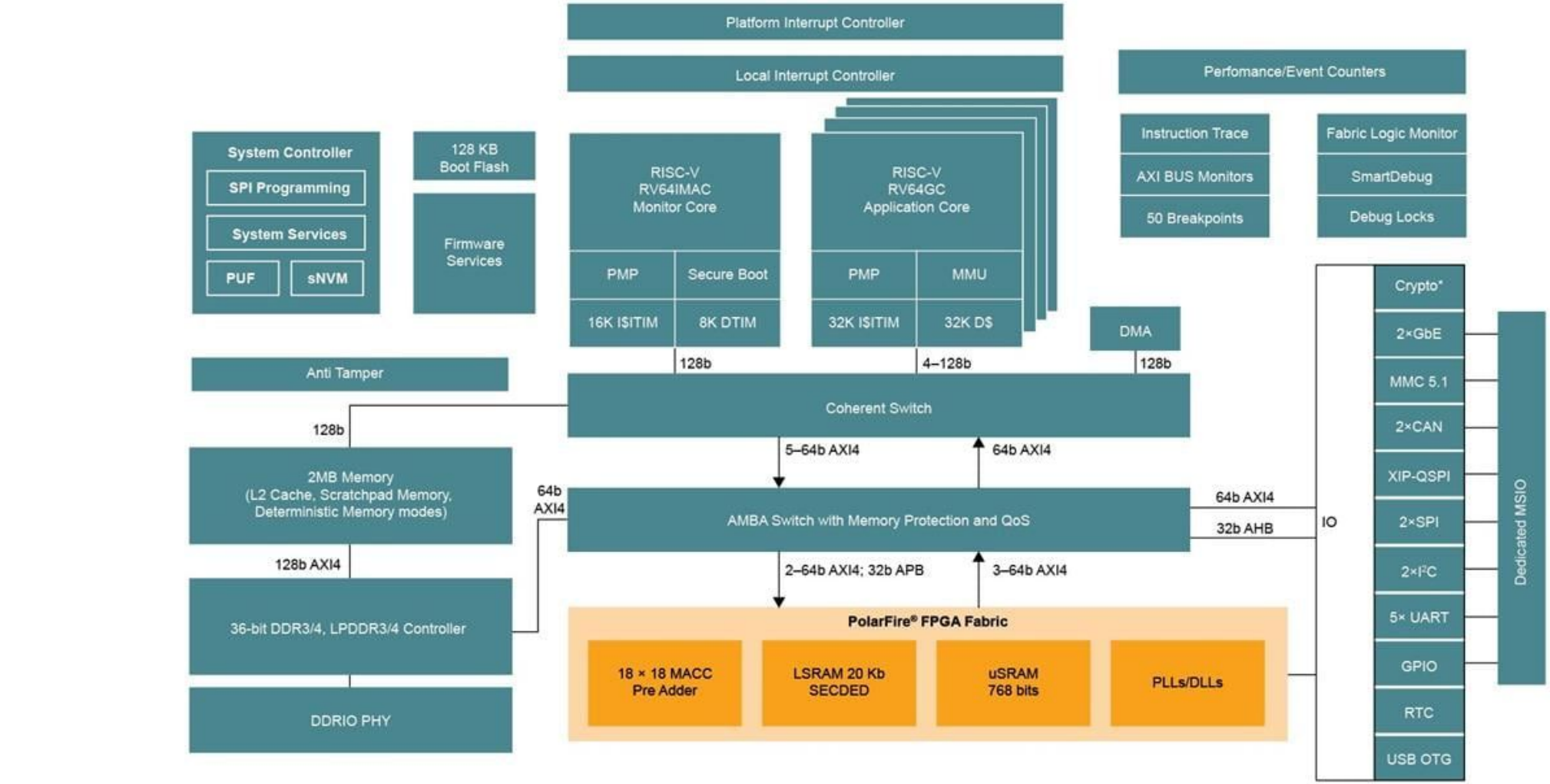
WorldGuard: une solution d'isolation matérielle pour le logiciel

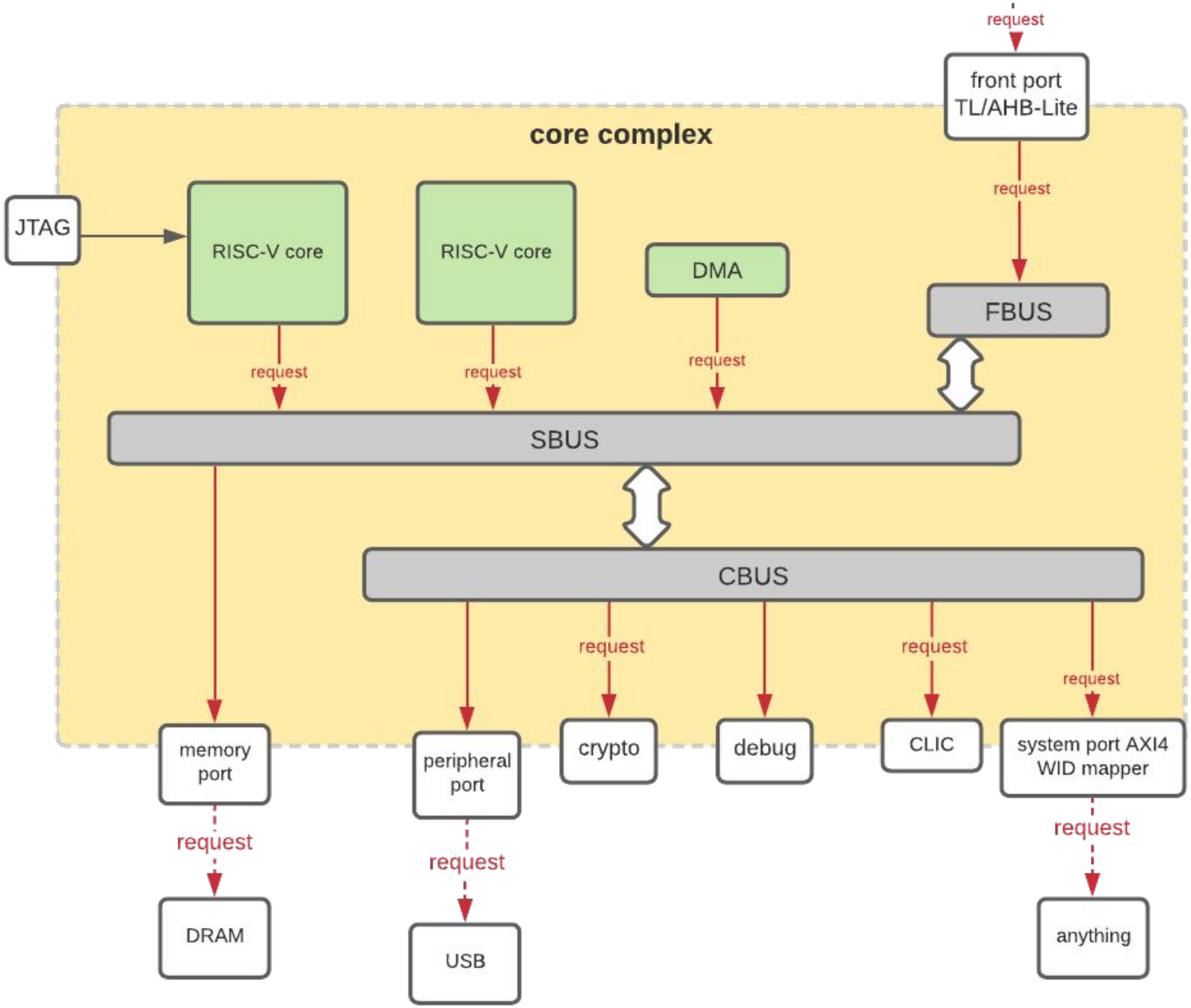
Yann Loisel, Oct 2021



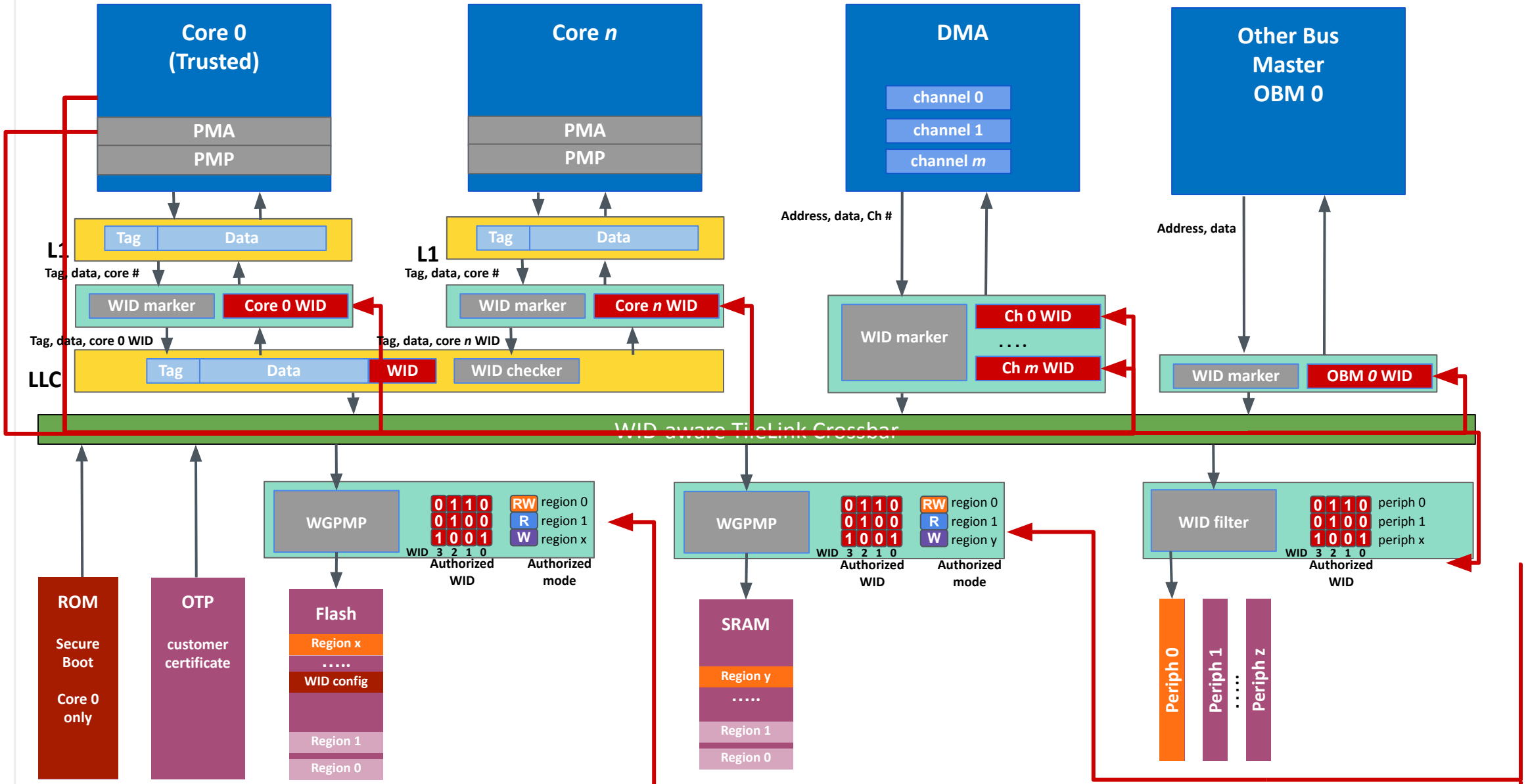


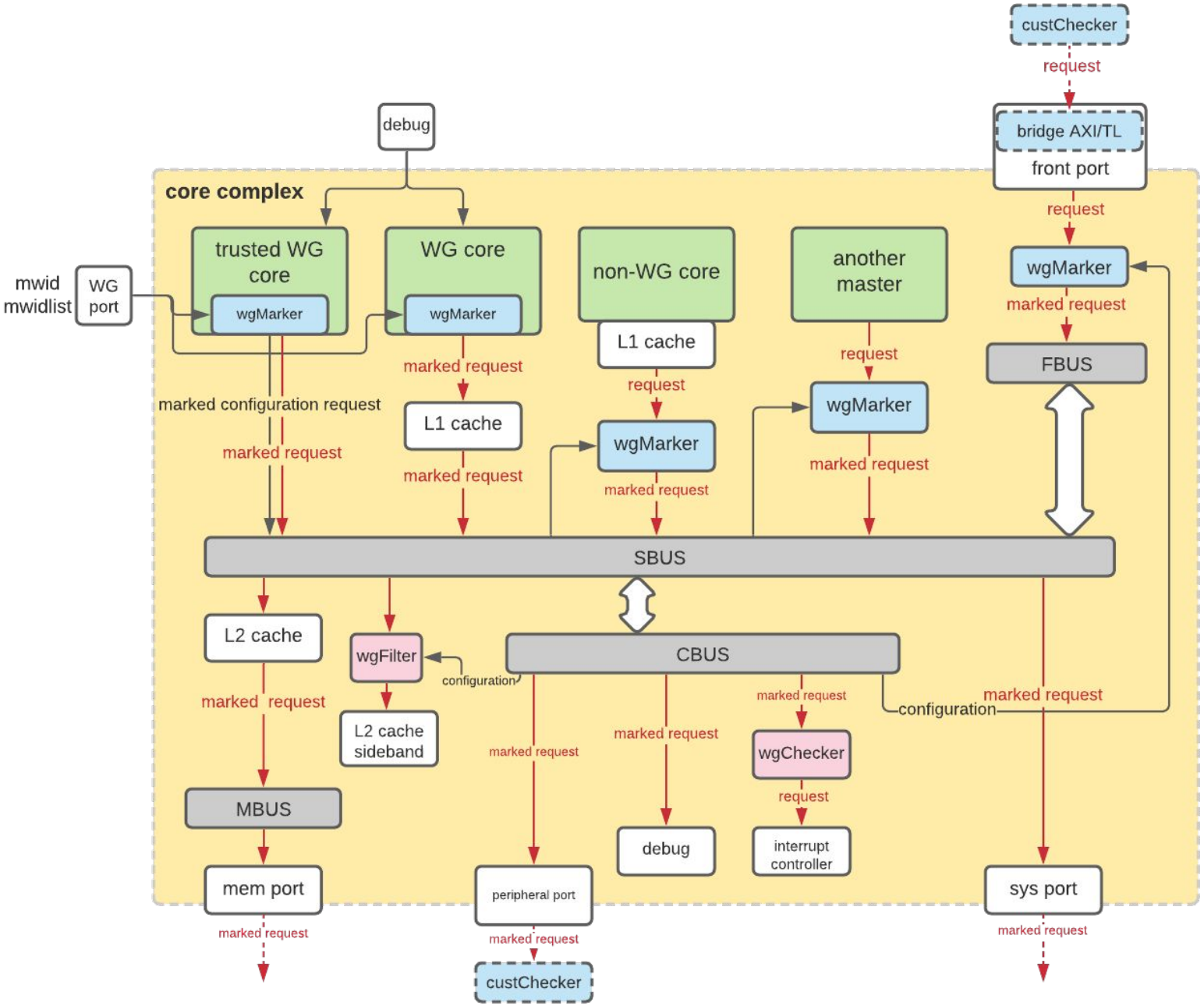
*DPA-Safe Crypto co-processor supported in S devices
**SECDED supported on all MSS memories

L’isolation logicielle est une fonctionnalité très importante requise pour différentes raisons, différents scenarii
La tendance à l’accroissement de la taille du code, ses origines diverses et variées, les différentes façons de les combiner introduisent des risques importants.



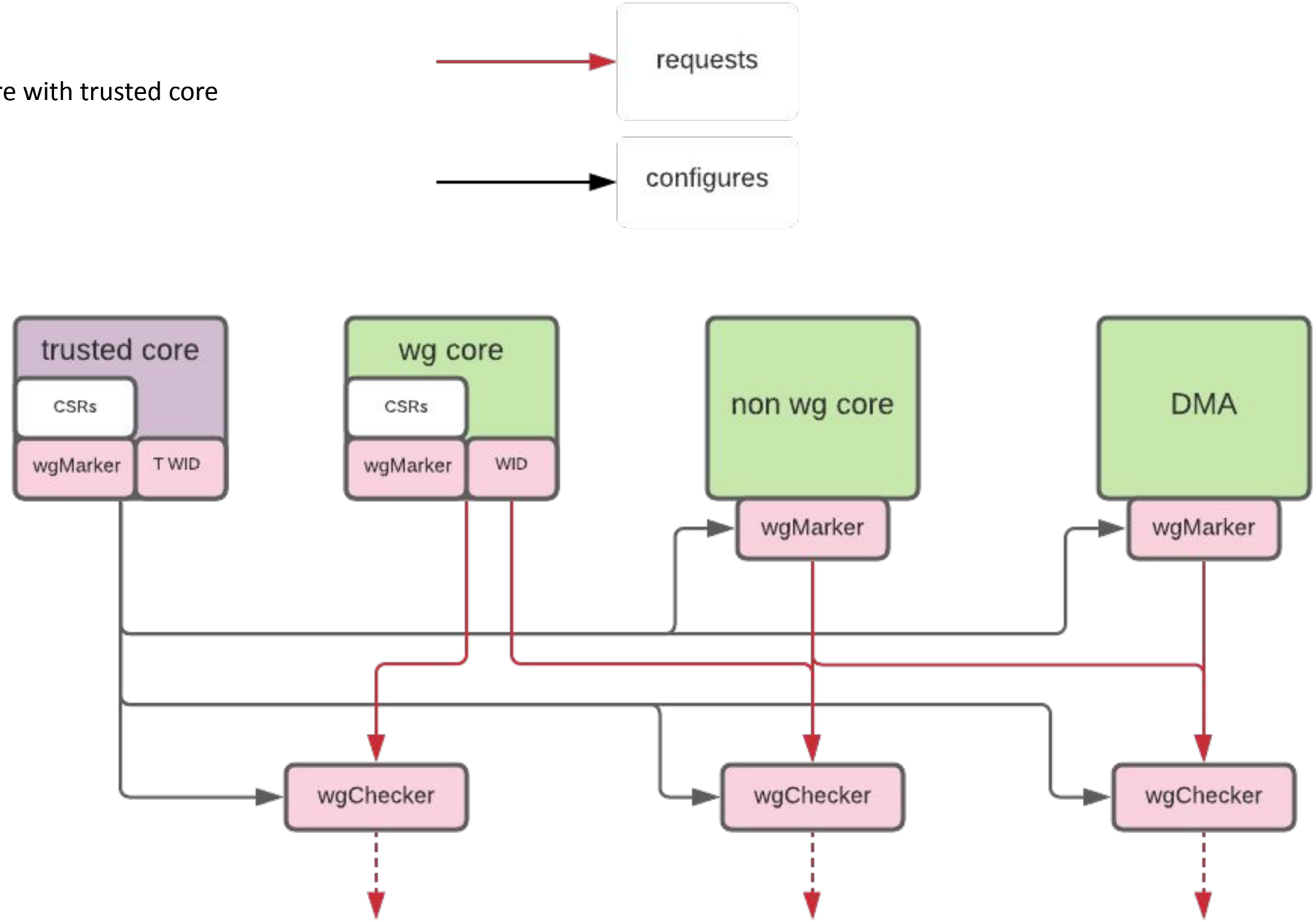
SiFive WorldGuard



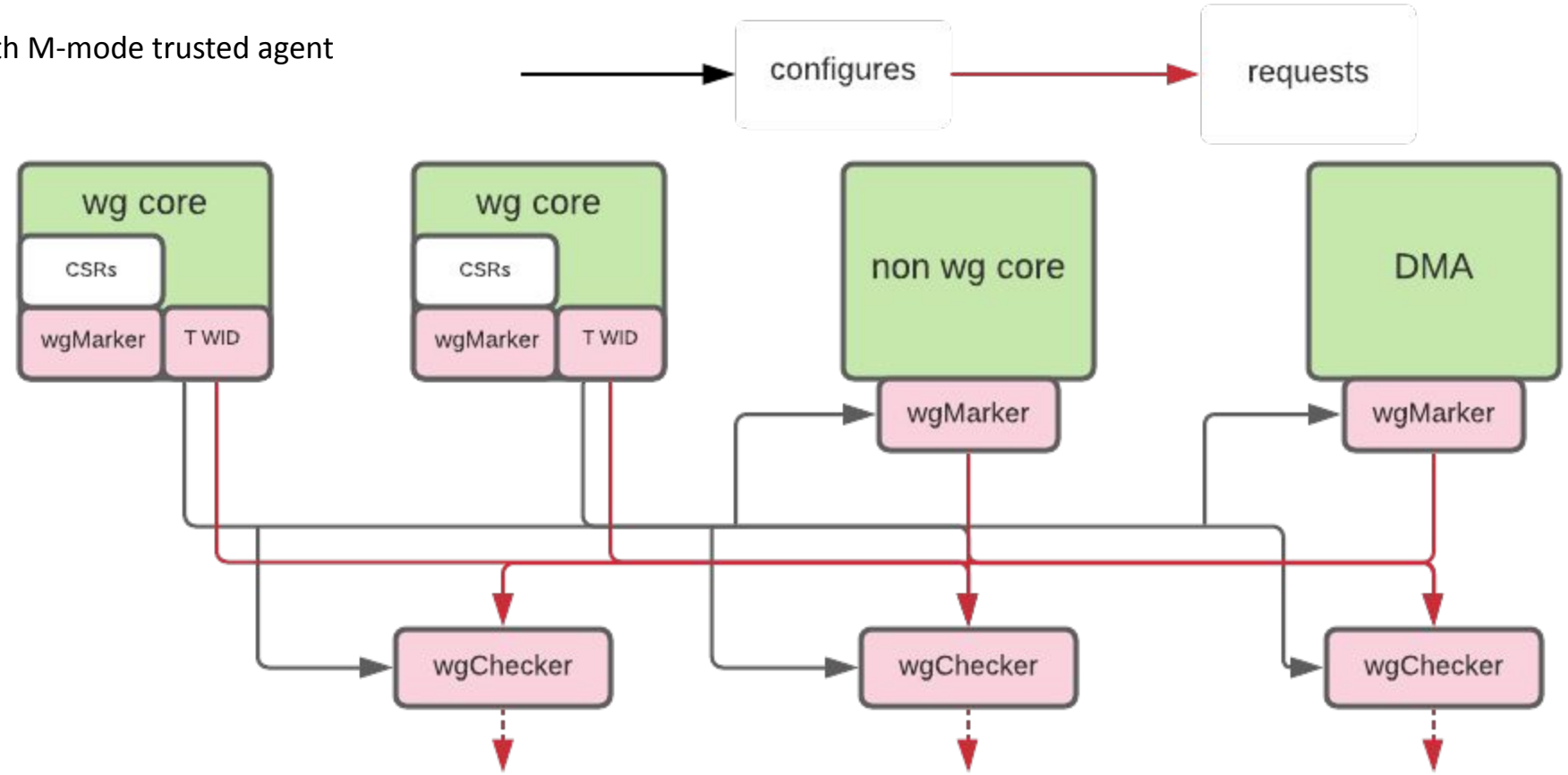


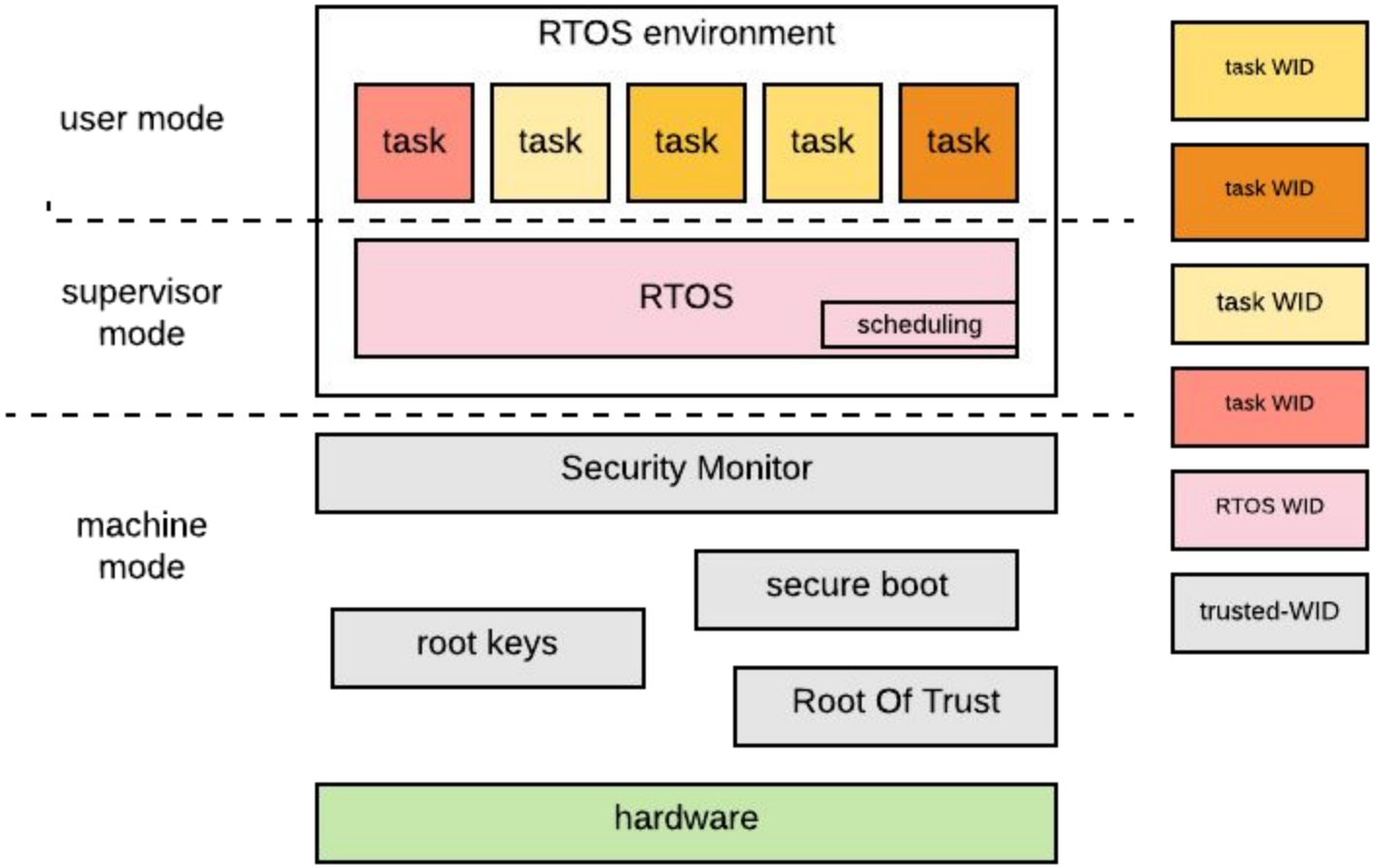
la solution WorldGuard propose une approche au niveau système pour sécuriser, contrôler les accès aux ressources par les applications logicielles

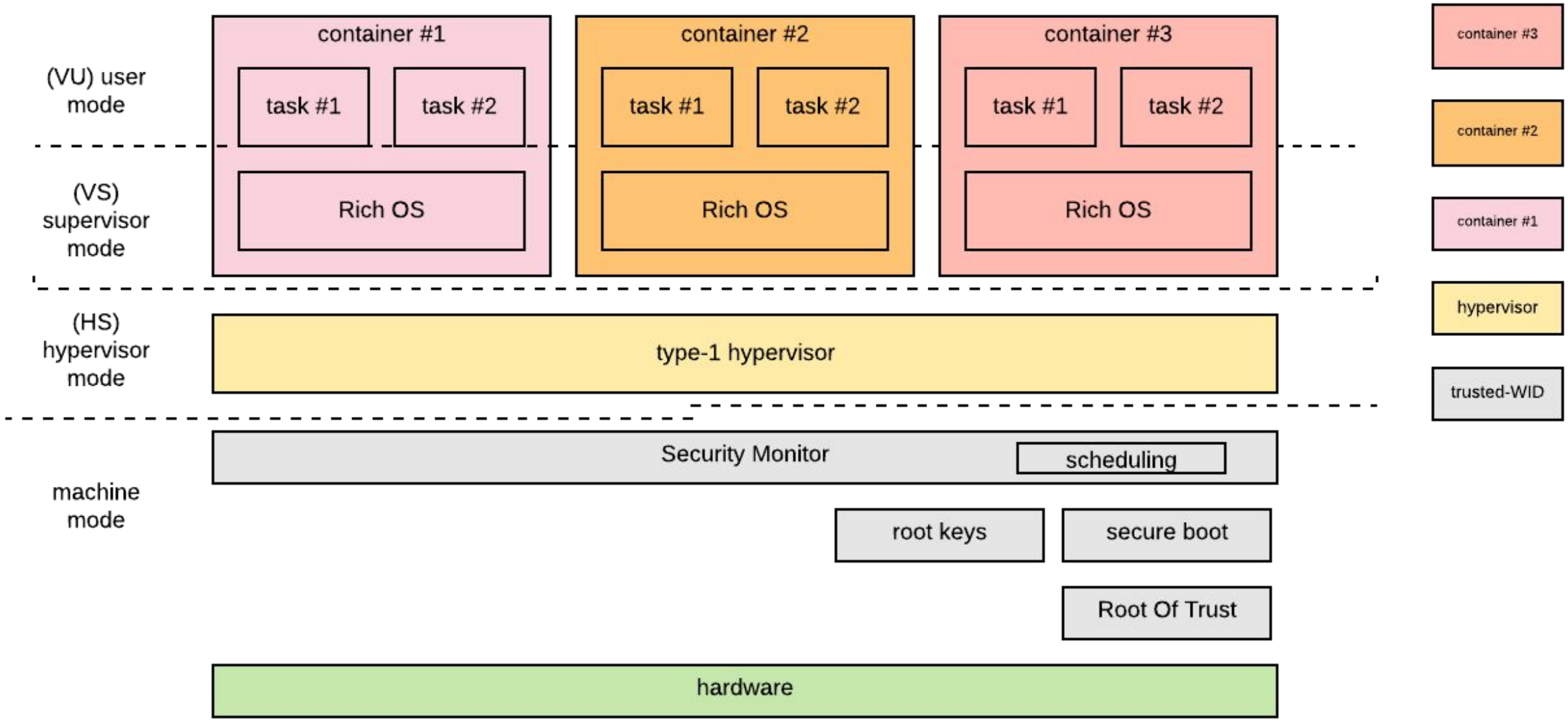
multi-core with trusted core

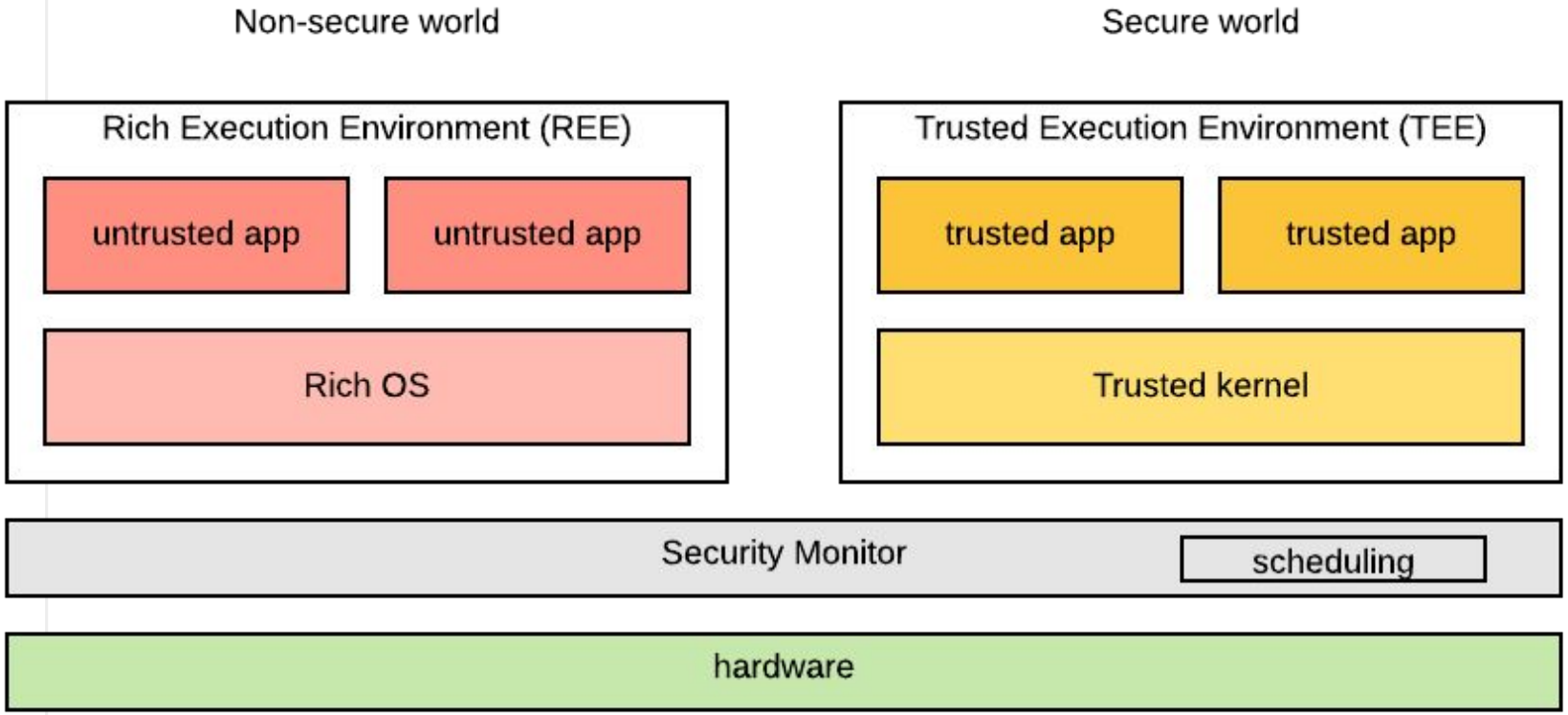


multi-core with M-mode trusted agent

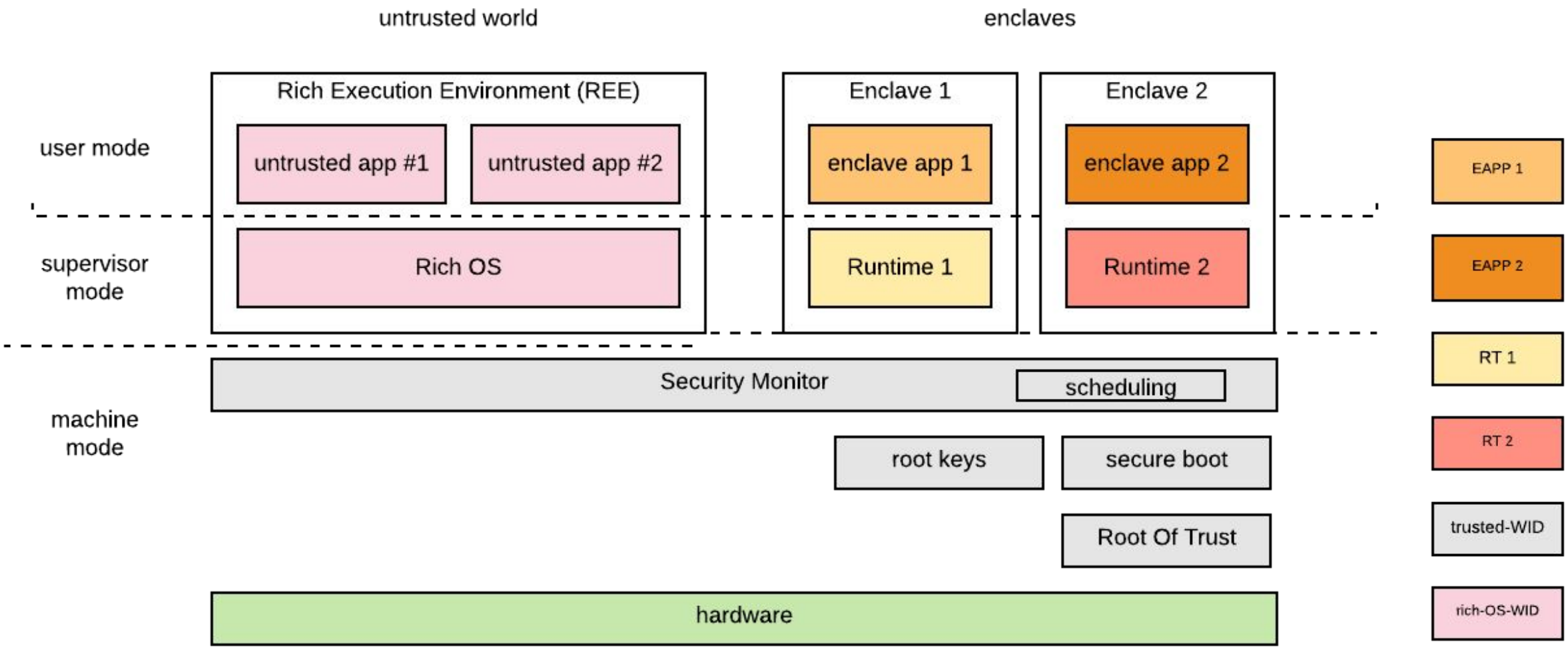


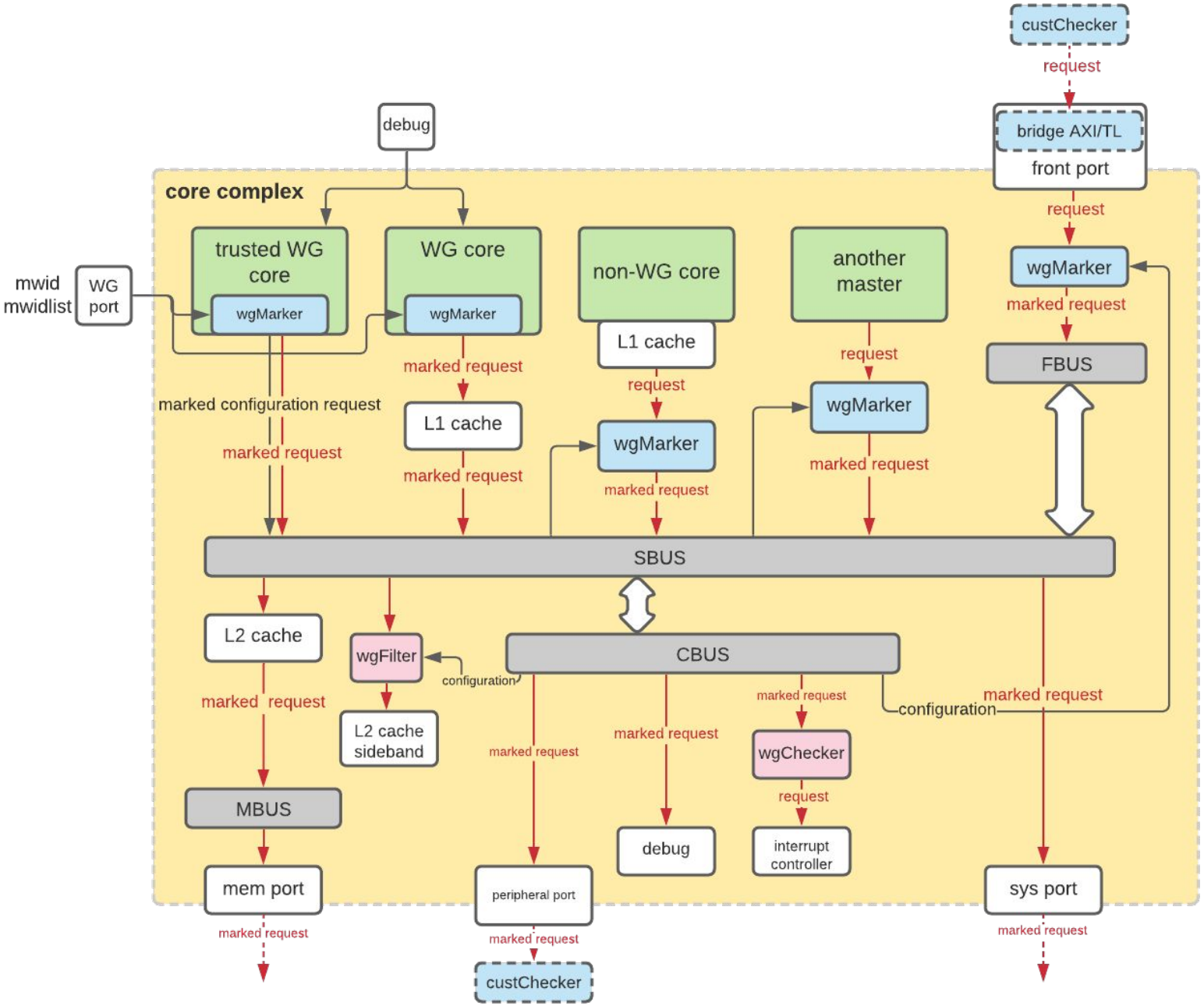


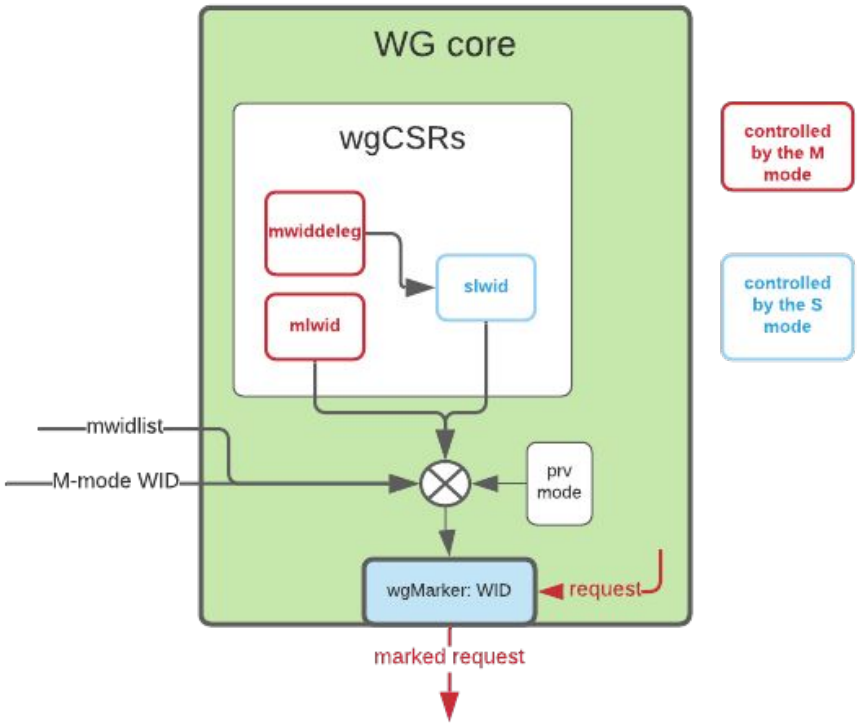


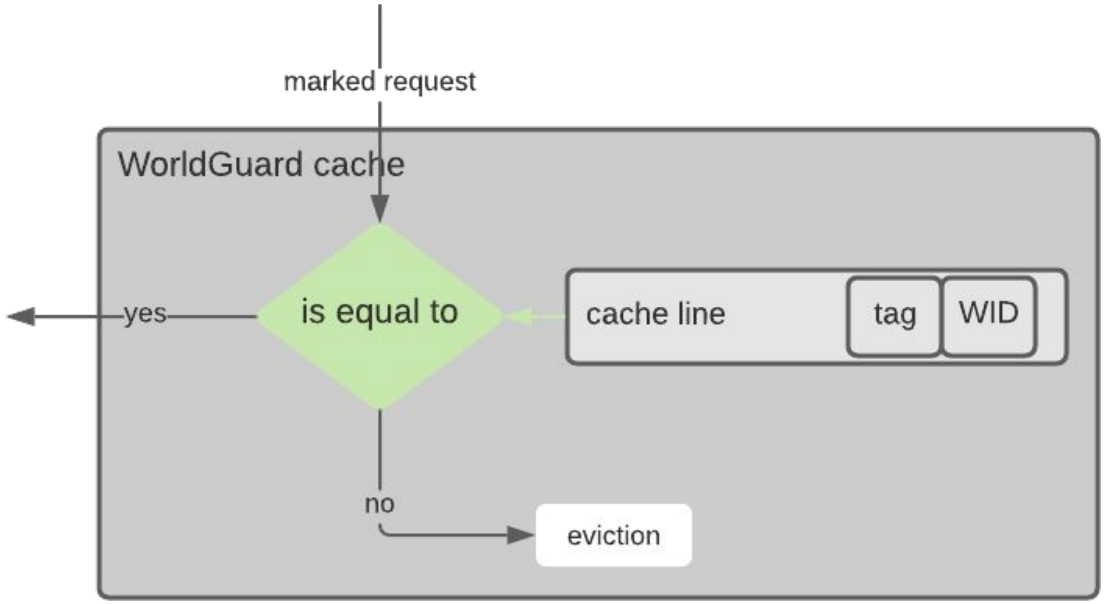


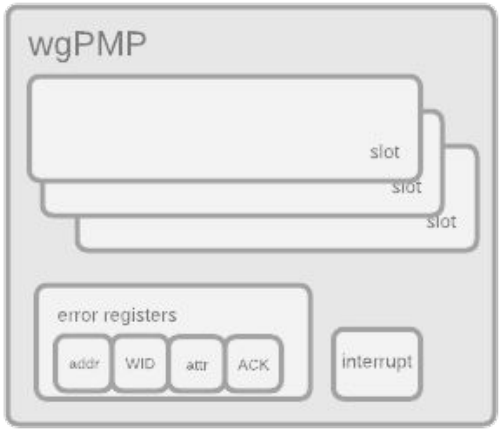
the security monitor is in charge of switches management between secure and non-secure states.
It manages the context switches (save, restore).
It's also in charge of interrupts handling











conclusion: une solution simple, extensible, flexible, au niveau système

Des questions ?