Sommario Tesi Italiano

Youssef Driouich

I sistemi ciberfisici (CPS) sono integrazioni del calcolo con i processi fisici. Le applicazioni dei CPS probabilmente hanno il potere di sovrastare la rivoluzione IT del XX secolo. Oggigiorno, l'appli- cazione dei sistemi ciberfisici a molti settori come Smart Grid, trasporto e salute, ci aiuta a gestire le nostre vite e le nostre attività senza problemi, con successo e in sicurezza.
Poiché i malfunzionamenti in questi sistemi ciberfisici possono avere conseguenze gravi, costose e talvolta fatali, gli strumenti di verifica basata sulla simulazione (SBV) sono fondamentali per ridurre al minimo la probabilità di errori che si verificano durante il processo di sviluppo e oltre. La loro applicabilità è supportata dall'uso sempre più diffuso di strumenti Model Based Design (MBD). MBD consente la simulazione di modelli CPS al fine di verificare il loro corretto comportamento sin dalla fase di progettazione iniziale. Lo svantaggio è che la verifica basata sulla simulazione per CPS complessi è un processo estremamente dispendioso in termini di tempo e risorse, che in genere richiede diversi mesi di simulazione. Gli attuali strumenti SBV mirano ad accelerare il processo di verifica con più simulatori che lavorano simultaneamente. A tal fine, calcolano tutti gli scenari in anticipo in modo tale da suddividerli e simularli in parallelo. Tuttavia, esistono ancora limitazioni che impediscono un'adozione più diffusa degli strumenti di verifica basata sulla simulazione. A tal fine, presentiamo una metodologia MBD che mira alla modellazione e alla verifica acausual tramite metodi formali, in particolare le tecniche di model checking, il sistema sotto verifica. Il nostro approccio si basa essenzialmente su: In primo luogo, l'analisi degli stati stazionari del CPS e la tecnica di delimitazione dello stato del sistema in parallelo con la simulazione al fine di identificare lo spazio dello stato del sistema simulandolo solo una volta, quindi rappresentarlo come una macchina a stati finiti(FSM). In secondo luogo, verificare esaurientemente l'FSM risultante utilizzando un symbolic model checker ed esprimere le proprietà desiderate nella logica temporale classica. L'applicazione a un power management system viene presentata come caso di studio.