Titolo:

Safety-driven design of automation systems in nuclear facilities

Abstract:

L'impiego dell'automazione in operazioni critiche all'interno di impianti nucleari offre chiari vantaggi legati alla riduzione dell'esposizione del personale, ma porta con sé anche problematiche di affidabilità e di sicurezza connessi ai potenziali scenari di guasto. I settori dell'automazione industriale e quello nucleare affrontano la valutazione e l'integrazione della sicurezza in modo diverso. Questa tesi vuole dimostrare come l'integrazione precoce della sicurezza nelle fasi di progettazione possa portare dei vantaggi sia in termini di miglioramento dell'affidabilità, sia di riduzione del rischio. Lo studio sfrutta l'infrastruttura di gestione remota, attualmente in fase di sviluppo, dedicata al trasporto e stoccaggio delle unità Target Ion Source (TIS) radioattive del laboratorio di ricerca nucleare Selective Production of Exotic Species (SPES). Un'analisi del rischio semi-quantitativo di tipo PRA è stata sviluppata per valutare gli scenari gravi che possono insorgere durante le procedure automatiche. Questa metodologia ibrida, che combina le analisi HAZOP e LOPA, verifica sistematicamente i vari nodi, determina la probabilità di accadimento degli scenari di guasto e valuta le loro conseguenze. Oltre all'identificazione delle criticità, l'analisi ha proposto una serie di misure di sicurezza, di raccomandazioni e di migliorie al design che possono aumentare la robustezza e la manutentabilità dei componenti più critici. Tra i punti deboli del progetto, vi è la valutazione e l'ottimizzazione degli interventi di manutenzione. Per affrontare queste tematiche, alcuni sottosistemi del Front-End sono stati riprogettati al fine di migliorarne la manutenzione e di introdurre dei dispositivi di attuazione di riserva. Inoltre, gli interventi di manutenzione più critici sono stati valutati tramite un'ampia campagna sperimentale che ha permesso di ottimizzare le attività in accordo con i principi ALARA e di stimare il tempo necessario per lo svolgimento di ciascuna attività. Nell'ultima sezione viene discussa la sicurezza del software di automazione. La logica di controllo dell'Horizontal Handling Machine (HHM), utilizzata come caso rappresentativo, è stata riprogettata secondo lo standard IEC 61499. Questo ha permesso l'applicazione di una serie di strumenti integrati che consentono lo sviluppo, la simulazione e la verifica formale del software prima del suo rilascio. Il caso in esame ha dimostrato come sia possibile integrare nelle fasi di sviluppo degli strumenti di model checking che permettano la verifica formale di proprietà di tipo LTL. L'adozione delle tecniche qui presentate ha portato ad un incremento significativo del livello di sicurezza dell'automazione nell'impianto. L'approccio proposto può essere facilmente esteso alla progettazione di sistemi critici in altri contesti.