Orvosi készülékekben használható modern fejlesztési technológiák lehetőségeinek vizsgálata

Biztonságkritikus funkciók továbbfejlesztési lehetőségei.

Kutatói beszámoló
Molnár László
2013.08.27.

Bevezetés:

Egy rendszerben azért van szükség biztonságkritikus funkciók megvalósítására, hogy elkerülhetővé váljanak a meghibásodásokból, emberi hibákból fakadó balesetek. Különösen jelentős hangsúly kerül a biztonságra, ha emberi életek forognak kockán, például egy atomerőműben, vagy az orvosi szoftverfejlesztés területén.

Az orvosi szoftverfejlesztés területén alapvető elvárás a kockázat elemzés (*risk analysis*), amely során a lehetséges meghibásodásokat, és azok hatásait kell felmérni, és kategorizálni, majd az elemzés alapján a kockázatok kezelése. Ha egy meghibásodás emberi életet, vagy emberi életeket veszélyeztet, alapvető elvárás a hiba tűrő tervezés (*fault tolerant design*). Ennek lényege hogy egyszeri hiba esetén az eszköz jelez a felhasználónak a hibáról, valamint biztonságos üzemmódban működik tovább (azaz nem veszélyeztet emberi életet, például leáll).

Ahhoz hogy az egyszeri hibákat biztonságosan tudjuk kezelni, az orvosi informatikában általában redundanciát alkalmazunk, azaz például nem egy, hanem két szenzorral mérjük a vizsgált értéket. A rendszer feladata, hogy az egyik szenzor meghibásodása esetén, detektálja a problémát, és jelezzen a felhasználónak.

Általában a használt eszközök meghibásodásának az esélye alapvetően is olyan alacsony, hogy két azonos ponton bekövetkező hiba valószínűsége elhanyagolható, így ez a módszer célravezető a gyakorlatban.

Nehézségek

A fent leírtak elméletben kiválóan működnek, és ideális esetben a gyakorlatban is megvalósíthatóak, azonban az elmélet átültetése a fizikai világba, mint oly sokszor problémákat vet fel. Ilyen probléma például hogy egy szenzor fizikai méretekkel rendelkezik, így nem tudunk egy jelet két szenzorral azonos ponton vizsgálni.

A jelet egy létező vezetéken továbbítja a szenzor a processzor irányába, illetve ha a processzor esetében is redundanciát használunk (hiszen ez is egy rendkívüli jelentőségű eleme a rendszernek), ezen processzoroknak is kommunikálniuk kell egymással, ami tovább növeli az aszinkronitást, így elképzelhető hogy a jelet nem egy időpillanatban vizsgálja a két szenzor.

Tovább nehezíti a helyzetet, hogy fizikai szenzorokról, és vezetékekről lévén szó, elképzelhetőek hibás mintavételek, zajos, nem egyértelmű jelek, valamint a rendszerben előforduló komoly késleltetések is. Képzeljük csak el milyen katasztrófát okozna egy atomerőműben, ha túl későn reagálnának egy blokk túlhevülésére. Ugyanakkor szintén katasztrófához vezetne, ha egy zajos jel hatására tévesen leállítanák a folyamatokat, áramkimaradást, és jelentős anyagi kárt okozva.

Szintén kulcsfontosságú, hogy detektáljuk az első meghibásodást amint lehetséges, hiszen a hiba bekövetkezését követően a rendszer egyszeres hibatűrése nem biztosított többé. Ilyenkor az előzetes kockázat analízis eredményének függvényében eldönthetjük mi a teendő. A helyzet súlyosságának függvényében elképzelhető hogy elegendő a felhasználónak jelezni hogy az egyik szenzor meghibásodott, de az is, hogy azonnal fel kell függeszteni a gép működését, a hiba kijavításáig.

Megoldások

Mindenekelőtt fontos a hibák, és reakciók pontos specifikálása a kockázati analízis során. Általában szigorú feltételek meghatározása a célravezető, hiszen egy téves hiba észlelés többnyire kevesebb kárt okoz, mint egy hiba észlelésének elmaradása.

Az aszinkronitásból származó téves hibák elkerülésére egy lehetőség például a jelek inkrementális gyűjtése, és hibajelzés ha elérünk egy értéket (meredekséget, stb.), valamint hiba jelzés ha a két szenzor által mért értékek különbsége meghalad egy értéket. Ez esetben az első hibajel a tényleges hiba jelzés, a második pedig az egyik szenzor hibás működésére utal.

Abban az esetben ha a szenzorok működésében túl nagy a különbség (pl. zaj miatt, vagy fizikai távolság okán), az egyik szenzor hibája jelezhető amennyiben, az egyik szenzor hibát észlel, a másik pedig úgy látja, még közel sem vagyunk a feltétel teljesüléséhez.

Általában a megfelelő algoritmussal a probléma megoldható, a nehézséget időnként a helyes algoritmus megtalálása okozza. Érdemes észben tartani, ha két szenzor közül az egyik helyes, a másik helytelen működést érzékel, hogy nem mindig a helyes működést jelző szenzor a hibás. Habár sajnos működés közben többnyire nem meghatározható melyik jelzés a helyes, így a hiba feltételezése a biztonságos megoldás.