

Megbízható kiber-fizikai rendszerek tervezése és ellenőrzése

A kiber-fizikai rendszerek (Cyber-Physical System – CPS) egyre fontosabbak és pótolhatatlanok az élet több egymástól lényegesen különböző területein, legyen az akár az egészségügy, szállítmányozás, okos gyártás vagy a biztonságtechnika. Az új funkcionalitásokra való igény lehetővé teszi a technológia fejlődését az érintett iparágakban, megfelelő tervezéssel és kivitelezéssel biztosítva a megbízhatóságot és a biztonságot. A kutatásom célja egy módszertan létrehozása volt, amivel követelmény vezérelt módon létrehozható egy megbízható, működő és biztonságos CPS. A módszertan algoritmikus módszerrel támogatja a megfelelő technológia kiválasztását, hogy a rendszer követelményei teljesüljenek.

A CPS fizikai világ és az informatika összekapcsolódásaként jön létre. A fizikai világból származó adatok feldolgozásához szolgáló logika megosztható a lokális erőforrások és a kibertérbeliek között (felhő). A kibertér ugyanakkor megjelenhet adatforrásként is (pl.: publikus érzékelési adatok, mint a meteorológiai előrejelzések), illetve intelligenciaforrásként is (pl.: távoli adatfeldolgozási eljárások). Az adatok nem csak a rendszer belső működését befolyásolhatják, hanem a CPS be is avatkozhat a fizikai világba. A két világ közti kapcsolatot gyakran beágyazott rendszerek adják a kibertérbeli megoldások interfészeként. A CPS világában a szolgáltatások bővülése és kifinomultsága tovább növelhető az egyes CPS-k egy nagyobb rendszerré való egybefűzésével (System of Systems – SoS).

Miután a számítógépes vezérlés hibáit a fizikai világgal való kölcsönhatás akár katasztrófálissá is erősítheti, növekszik a megbízhatóság, interoperabilitás és biztonság iránti igény. A CPS megalkotása a tervezéstől fogva összetett feladat. A kritikus CPS rendszerekben a szolgáltatásminőség biztosításához szükséges a széleskörű funkcionális és extra-funkcionális követelmények kielégítése.

A mérnöki világban bevett gyakorlat a különböző módszertanok használata a rendszer tervezése során. Ezek lehetnek ajánlások vagy egy adott szervezet által bevált gyakorlatok, mint a NASA System Engineering Handbook vagy az NIST CPS Framework. Hasonlóan, de-facto és ipari szabványok meghatároznak illetve ajánlanak referenciaarchitektúrákat és platformokat, biztosítva az átjárhatóságot és az interoperabilitást a rendszerek és komponenseik között.

Különböző technológiák (pl.: Data Distribution Service – DDS, Blockchain, MQTT) hasonló funkcionalitások mellett más-más extra-funkcionális tulajdonságokkal (pl.: biztonság, áteresztőképesség, időszerűség, letagadhatatlanság) rendelkeznek. A megfelelő technológia kiválasztása kulcs a megfelelő szolgáltatás garantálásához. A szolgáltatások szintjének biztosításához kulcsfontosságú a követelmények teljesítése. A követelmények architektúrális leképezésének validációja és verifikációka döntő tényező a rendszer tervezésének fázisában.

Célom a tervezési fázisban végrehajtandó ellenőrzési tevékenységek algoritmikus támogatása volt. A szóba jövő illetve kiválasztott architektúra leképezhető kényszerek hálózatára. A hálózatban az egyes csomópontok megmutatják, hogy azok mennyire felelnek meg a követelmények egyes aspektusainak (biztonság, időszerűség, megbízhatóság, biztonságosság, integritás és letagadhatatlanság).

Az így létrejövő kényszerkielégítési probléma (CSP – Constraint Satisfaction Problem) garantálhatja a megfelelőséget egy egyedi megoldás ellenőrzésével vagy akár megadhatja az összes szóba jövő megoldást is.

A fenti módszerek lehetővé teszik a garantált minőségű CPS tervezését algoritmikus úton. A módszer segíthet a költségek és a tervezési idő csökkentésében.