**Cyber Physical System Applications Verification and Validation**

**-Rezumat –**

**Ing. dipl. Madalin Gavrilescu**

Teza de doctorat elaborată prezintă un proces nou, complex si complet de testare si validare pentru aplicații ale sistemelor cyber fizice. Verificările amănunțite sunt făcute atât pentru proprietățile statice cat si cele dinamice ce apar in modelele UML corespunzătoare aplicațiilor pentru sisteme fizice.

Testarea si verificarea unei aplicații pentru sisteme cyber fizice parcurg toate nivele la care se specifica o astfel de rețea, începând de la nivel de componenta, continuând cu nivel de nod, iar la cel mai înalt nivel logic, nivelul de rețea.

Acest proces de testare si verificare vine ca o metoda de validare a metodologiei de modelare vizuala a sistemelor cyber fizice, dezvoltate in cadrul echipei de cercetare. Lucrarea demonstrează utilitatea unei astfel de abordări la nivel de verificare si validare a unor aplicații pentru sisteme cyber fizice prin studii de caz ce discută diferite modalități de testare a aplicațiilor pentru sisteme cyber fizice, din diverse domenii de activitate și cu nivel diferit de dificultate la nivel de cerințe de aplicație, in funcție de proprietățile testate.

Teza de doctorat conţine aproximativ 120 de pagini, grupate în 7 capitole şi aproximativ 98 referinţe bibliografice.

*Capitolul 1***- „Introduction”** prezintă tema de cercetare în ansamblu, obiectivele ce s-au dorit a fi îndeplinite la începutul cercetării, respectiv câteva idei generale despre modalitatea abordată pentru procesul de validare al aplicațiilor pentru sisteme cyber fizice. La acest nivel este prezentată și organizarea tezei pe capitole. Sistemele cyber fizice reprezintă o soluție adecvată în aplicații din numeroase domenii (monitorizare de infrastructură, trafic inteligent, sisteme medicale). Fiind un domeniu relativ nou, la ora actuală nu există soluții general valabile referitoare la partea de validare a unor astfel de aplicații. Astfel apare necesitatea unui proces de validare, care să permită utilizatorului verificarea aplicațiilor pentru sisteme cyber fizice, specificate prin modele UML. Metodologia se pretează sistemelor cyber fizice compuse din senzori, actuatori, unități de comunicare și unități de control. Validitatea metodologiei este indicata prin studii de caz ce prezintă testarea diverselor proprietăți ale aplicațiilor pentru sisteme cyber fizice.

*Capitolul 2 -* **„State of the art”** descrie stadiul actual al cercetării legat de toate aspectele ce compun metodologia prezentată în teză. La nivel de sisteme cyber fizice, autorul tezei a studiat modelarea si design-ul realizate prin intermediul unei arhitecturi bazate pe model, când cerințele aplicațiilor sunt tratate in maniera orientata pe obiective. Aceasta metodologie a fost dezvoltata in cadrul echipei de cercetare.

De asemenea, autorul tezei a studiat lucrări din literatura ce prezintă mediile de simulare pentru rețele de senzori existente la ora actuala, pentru a putea determina care este cel mai potrivit in testarea modelelor pentru aplicații ale sistemelor cyber fizice. Doctorandul a ales OMNeT++, care este un framework de simulare de rețea bazate pe evenimente discrete, ce este structurat intr-o maniera orientata pe obiecte. Un avantaj semnificativ al acestui mediu de simulare este faptul ca permite simularea paralela si menține propriul ciclu de tact.

Autorul tezei a mai studiat metodologiile de verificare pentru aplicații ale sistemelor cyber fizice ce se axează pe specificare riguroasa, urmata de verificare cu tool-uri specializate. In acest sens, el s-a oprit asupra limbajului Z, ce oferă o specificare matematica riguroasa si PVS, ce se pretează in cazul modelelor pentru sisteme cyber fizice de mari dimensiuni si este similar cu limbajele de programare si design-ul orientat pe obiecte.

Pentru metodologiile prezentate în acest capitol se prezintă motivele pentru care au fost luate în considerare la nivelul tezei. Fiecare subcapitol se încheie cu o recapitulare sau un tabel ce prezintă abordările descrise, din punct de vedere al beneficiilor aduse, al anului de apariție și al impactului în această teză.

*Capitolul 3* **-** **„Simulation models for PSoC based CPS applications”** prezintă, ca o extensie a framework-ului OMNeT++, modelele de simulare dezvoltate de către autorul tezei pentru testarea şi validarea aplicațiilor pentru sisteme cyber fizice. Se considera ca aceste sisteme sunt compuse cu ajutorul sistemelor pe chip programabile, fiecare menținându-si propriul ciclu de tact. Modelele de simulare prezentate pot fi folosite pentru testarea si validarea cu acuratețe de ciclu de tact a proprietăţilor dinamice in rețele embedded masiv distribuite si, in particular, sisteme cyber fizice.

Primul model de simulare permite testarea sistemelor cyber fizice compuse din sisteme pe chip programabile ce lucrează la aceeași frecventa de tact si ia in considerare timpul de simulare. Al doilea model permite testarea sistemelor cyber fizice compuse din sisteme pe chip programabile ce lucrează la frecvente de tact diferite. Aici se observa creșterea timpul de simulare, proporțional cu numărul de frecvente de tact distincte, existente la nivelul sistemelor componente.

Un al treilea model de simulare poate fi folosit in cazul rețelelor pentru sisteme cyber fizice ce conțin componente distribuite, ce pot avea defazaje fata de momentul de start-up al rețelei. Mecanismul de programare al OMNeT++ a fost extins in cadrul acestui model pentru a fi capabil sa considere in mod corect momentul in care mesajele trebuie sa fie programate sau primite.

Autorul tezei a dezvoltat de asemenea un model de simulare ce permite un timp redus de simulare in cadrul rețelelor de mari dimensiuni. Ideea ce a stat la baza modelului este separarea timpilor intre tactul intern al nodului de sistem pe chip programabil si timpul de simulare OMNeT++.

*Capitolul 4* **- „Validation of static properties in UML models for CPS applications”** prezintă validarea proprietăţilor statice din modelele UML definite pentru aplicații ale sistemelor cyber fizice prin intermediul specificării riguroase si validării cu ajutorul tool-urilor specializate. Autorul tezei arata faptul ca constrângerile OCL sunt de ajutor in specificarea prin modele UML, dar pentru o reprezentare fidela a cerințelor si constrângerilor unei aplicații pentru sisteme cyber fizice este necesar sa se apeleze la specificare riguroasa. In acest punct al cercetării, autorul a realizat o prezentare a validării proprietăţilor statice in cadrul sistemelor cyber fizice, iar validarea proprietăţilor dinamice este privita in perspectiva.

Autorul tezei discuta aceste modalităţi de validare inițial la nivel teoretic iar apoi la nivel de studii de caz. Pentru studiile de caz folosește atât limbajul Z cat si PVS, in funcția de complexitatea modelului analizat. Pe partea de specificare Z, autorul tezei discuta modelul pentru tipul de nod senzor, pentru care face o specificare riguroasa, respectiv o verificare a unei metode de modificare a unui atribut.

Pe partea de PVS, autorul tezei folosește limbajul PVS pentru a specifica o aplicație pentru un sistem de monitorizare a distribuției de gaze. El prezintă teoriile PVS necesare la fiecare nivel logic din cadrul rețelei de gaze: perimetre, zone si arii. Pentru partea de verificare a specificării PVS, doctorandul prezintă validarea unui model la nivel de arie prin testarea abilitații de comunicare intre zonele ce compun o arie, in cazul comunicării fără fir. Corecția se face prin includerea sensibilității receptorului in condiția teoremei PVS la nivel de arie.

*Capitolul 5* **- „Handling event-driven scenarios in CPS applications simulation”** prezintă un model orientat pe evenimente pentru specificarea aplicațiilor pentru sisteme cyber fizice distribuite. Modelul orientat pe evenimente este descris in format XML. Obiectivul urmărit este de a permite dezvoltatorului de aplicații pentru sisteme cyber fizice sa descrie scenarii de simulare specifice pentru aplicații distribuite. Astfel se urmărește validarea proprietăţilor dinamice in cadrul modelelor UML pentru aplicații ale sistemelor cyber fizice. De asemenea, autorul tezei a prezentat in lucrare un model de programare orientat pe evenimente pentru tratarea diferitelor scenarii ce pot apărea in aplicații ale sistemelor cyber fizice. Acest model de programare este unul generic ce poate fi implementat in orice mediu de simulare orientat pe evenimente. Doctorandul prezintă ca si concluzii la acest capitol optimizările obținute prin folosirea abordării descrise la nivel de număr de linii de cod. Îmbunătățirea depinde si de obiectivele aplicației pentru sisteme cyber fizice ce se dorește a fi testata si verificata.

*Capitolul 6* **- „Error handling in CPS applications implemented using goal-oriented approach”** prezintă o metodologie destinata verificării proprietăţilor dinamice ale aplicațiilor pentru sisteme cyber fizice, îndeplinirii obiectivelor asincrone ale aplicațiilor, respectiv tratarea cazurilor excepționale ce pot apărea pe parcursul ciclului de viață al unei aplicații si a eșecurilor apărute la nivel de nod. Aceasta metodologie a fost dezvoltata folosind Linear Programming si urmărește acele cazuri limita ce pot apărea, dar care nu sunt considerate erori, spre exemplu procedurile ce trebuie urmate in cazul in care se atinge nivelul minim de combustibil in interiorul unui rezervor, in cadrul unui sistem de management a combustibilului, nivel semnalizat prin intermediul senzorilor.

In astfel de cazuri particulare, exista posibilitatea ca folosind Linear Programming sa nu se obțină soluţii optime, aceasta metodologie fiind considerata prea restrictiva. Pentru rezolvarea acestor situaţii, autorul tezei considera aproximarea soluției valide prin schimbarea domeniului anumitor variabile sau prin reactualizarea ecuațiilor de control din sistemul de Linear Programming ce se dorește a fi optimizat. Un posibil dezavantaj al acestei soluții îl constituie restricția ca nodurile rețelei sa fie statice.

Autorul tezei a folosit in acest capitol ca si studiu de caz sistemul de management de combustibil din cadrul unui avion, atât pentru discutarea situațiilor speciale ce pot apărea in cadrul sistemului, când si in cazul in care unul dintre noduri nu mai funcționează corespunzător iar existenta lui trebuie înlocuita in cadrul rețelei.

Doctorandul prezintă pașii de urmat in cazul in care un nod (senzor sau actuator) nu mai funcționează corespunzător in cadrul rețelei. Se începe prin eliminarea termenilor corespunzători din sistemul de Linear Programming si reevaluarea relațiilor de Linear Programming pentru verificarea corectitudinii. Obiectivul este ca fiecare relație din sistem sa aibă termeni valizi. Se elimina acei termeni care nu mai corespund, pana in punctul in care toate relațiile sunt corecte din punct de vedere matematic in cazul sistemului de Linear Programming.

*Capitolul 7* **- „Conclusions and perspectives”** prezintă contribuțiile tezei, evidențiind importanța lor în verificarea aplicațiilor pentru sistemelor cyber fizice. Tot în acest capitol se prezintă publicaţiile ce stau la baza acestei teze, modul în care rezultatele au fost diseminate în cadrul unor jurnale cotate ISI si BDI, conferințe internaționale ISI și IEEE și workshop-uri în cadrul proiectului de Burse Doctorale.