

КІБЕР-ФІЗИЧНІ СИСТЕМИ ТА ЇХ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

CYBER-PHYSICAL SYSTEMS AND THEIR SOFTWARE

Ван Чунжі¹, проф., д.т.н.; Яцишин С.П.², д.т.н., проф.; Лиса О.В.³, к.т.н., доц., Мідик А-В.В.⁴, аспірант, e-mail: ovl2407@ukr.net

¹ - School of Computer Science, Hubei University of Technology, China; ² – Національний університет «Львівська політехніка», Україна; ³ - Львівський аграрний університет, Україна

⁴ – аспірантура, Національний університет «Львівська політехніка», Україна

Wang Chun Zhi¹, Prof., Dr.Sc.; Yatsyshyn S.², Dr.Sc.; Lysa O³, PhD, As.-Prof.; Midyk A-V.⁴, PhD Student, e-mail: ovl2407@ukr.net

¹ - School of Computer Science, Hubei University of Technology, China; ² – Lviv Polytechnic National University, Ukraine; ³ – Lviv Agricultural University, Ukraine; ⁴ – Postgraduate School, Lviv Polytechnic National University, Ukraine

Анотація

У зв'язку з посиленням розвитком кібер-фізичних систем істотна увага у світі приділяється різним аспектам їх формування й експлуатації. Так у 2014 року NIST, USA створила Громадську робочу групу кібер-фізичних систем для об'єднання широкого кола фахівців на відкритому громадському форумі, щоб допомогти визначити та сформувані їх основні характеристики для керівництва розробленням та впровадженням «інтелектуальних» програм у різних сферах, включаючи розумні виробництво, транспортування, енергетику та охорону здоров'я. Важливим, при цьому, вважається питання програмного забезпечення, оскільки, по-перше, вказані системи складаються із значної, нерегламентованої кількості компонентів, рознесених у просторі й часі, а, по-друге, компоненти систем мають змогу самостійно, під власні потреби, додатково встановлювати необхідне програмне забезпечення, назване, як Middleware.

Abstract

In connection with the enhanced development of cyber-physical systems, considerable attention in the world is given to various aspects of their formation and operation. So in 2014, NIST, USA has created a Cyber-Physical System (further CPS) Community Working Group to bring together a wide range of professionals at an open, public forum to help identify and shape the main characteristics of the CPS to guide the design and implementation of “intelligent” programs in various areas, including smart production, transportation, energy and healthcare.

By analyzing the known CPSs, their metrological and software, we can evidence that their number is steadily increasing, and the scope of application is expanding. Software and metrological assurance develop in the direction of supporting the work of existing CPSs as also and in the design of their suitability for new types of CPSs. Therefore, the requirements for creating a CPS are security, confidentiality, reliability, stability, guarantees for common interconnected devices and infrastructures, dynamism, compatibility (the ability to host different computing models), the support of different modes of communication in the network, the solvability of complexity problems (problems of accessing the obtained data and control with feedback in any architecture of the CPS), synchronization, interaction with the operating environment, the ability to cooperate with each other for the creation of the complex effects, the creation of effects that exceeds the sum of the effects of individual parts of the CPS, the ability to combine several goals.

CPSs are characterized by well-defined components: with known performance described by using standardized semantics and syntax. CPSs must support the flexibility of applications and domains. To realize this, the definition of components must be flexible and open. The architecture should support an accurate questioning of components in order to provide flexibility in the creation and adaptation of virtual systems and the promotion of innovation. The CPS should support a large scale of sizes, complexity and loading in addition. The components should be integrated or/and scaled quickly, even while operating. The CPS architecture should consist of independent, disconnected components for flexibility, reliability and resilience to changing situations. The solution must also exist between the architectural layers, allowing each layer to be changed, without affecting other layers. In order for the system to integrate different components, the interfaces to these components should be based on interpreted and unambiguous standards. Adaptation is achieved through the flexibility of internal components and interoperability. An important issue is software, since, firstly, these systems consist of a large, unregulated number of components spaced apart in space and time, and secondly, system components are able to independently install themselves for their own needs the required software denominated as Middleware.

Ключові слова

Кібер-фізичні системи, Смарт-засоби, Програмне забезпечення, Проміжне програмне забезпечення

Keywords

Cyber-Physical Systems, Smart Means, Software, Middleware

1. Вступ

Кібер-фізичні системи (далі - КФС) - це інтелектуальні системи, що включають інженерно-взаємодіючі мережі фізичних та обчислювальних компонентів. Вони проникають у всі сфери життєдіяльності людини: виробництво, будівництво, транспорт, енергетику, медицина тощо, де забезпечують нові функціональні можливості для покращення якості життя, дозволяють досягти технічного прогресу в різних областях і тому мають значний вплив на світову економіку. Основою розроблення різних моделей кібер-фізичних систем є наявність засобів вимірювання та їх програмного забезпечення. Засоби необхідні для контролю параметрів технологічних процесів та навколишнього середовища [1].

Суть "інтелектуальних" програм полягає в тому, що використовуючи дані сенсорів, які якнайшвидше і якнайточніше сигналізують про зміну параметрів середовища, спеціальні алгоритми приводять в дію автоматику вищого рівня для виконання адекватних дій. КФС виходить за рамки звичайного продукту, системи та архітектури прикладних програм. Зазвичай КФС включає в себе всі відомі аспекти роботи інформаційно-вимірювальних систем, ускладнених унаслідок взаємодії їх окремих компонентів через мережі. Вони об'єднують традиційні інформаційні технології: від поступлення даних від сенсорів з їх опрацюванням із використанням вбудованих обчислювальних потужностей або з використанням хмарних технологій, до традиційних операційних технологій контролю та управління. Інакше, особливістю КФС є поєднання інформаційних та операційних технологій, на що накладаються часо-просторові обмеження, оскільки КФС часто розпорозені у просторі та розділені у часі.

Питання впровадження "інтелектуальних" програм у різних сферах настільки актуальне, що NIST розробила класифікацію КФС, яка включає розумне виробництво (пряме та додаткове), розумні конструкції, розумний транспорт, розумну енергетику, розумну безпеку життя та розумну охорону здоров'я. Щоб забезпечити впровадження "інтелектуальних" програм, необхідно створити прикладну модель системи, мати відповідне метрологічне та програмне забезпечення. Крім того, необхідно досягнення сумісності між різнорідними компонентами та системами. У зв'язку з цим потрібні розробки у сфері метрології (калібрування, оцінка якості комплексних продуктів, діагностика на базі моделі), у сфері розроблення основного і проміжного програмного забезпечення. Програмне забезпечення формує адекватну прогнозовану поведінку системи – відповідь системи на зміну згаданих параметрів.

2. Недоліки

Особливої уваги заслуговує режим роботи КФС без участі фахівців (англ. – «man-out-loop» regime), який у поєднанні із гнучкістю системи, забезпечуваною автоматичним оновленням програмного забезпечення та впровадженням проміжного програмного забезпечення (англ. - Middleware), може призвести до виникнення критичних ситуацій у працездатності й ефективності роботи систем в цілому. До прикладу, метрологічна відмова, зумовлена погіршенням параметрів систем медичного догляду (автоматичного вприскування ліків із інсталюваною під шкірою пацієнта капсули), може призвести до незворотніх наслідків.

3. Мета роботи

Метою роботи є дослідження працездатності й ефективності кібер-фізичних систем у результаті аналізу особливостей їх метрологічного та програмного забезпечення.

4. Матеріали та методи

Аналізуючи відомі на сьогодні КФС, їх метрологічне та програмне забезпечення, бачимо, що невпинно зростає їх кількість, розширюються сфери застосування. Програмне та метрологічне забезпечення розвивається в напрямку підтримки роботи наявних КФС та їх придатності при конструюванні нових КФС. Тому вимогами, які ставляться при створенні КФС, є безпека, конфіденційність, надійність, стійкість, гарантії щодо поширених взаємопов'язаних пристроїв та інфраструктур, динамічність, сумісність (можливість розмістити різні обчислювальні моделі), підтримувальність різних режимів спілкування в мережі, вирішувальність проблем складності (проблеми зондування та керування із зворотним зв'язком у будь-якій архітектурі КФС), синхронізація, взаємодія з середовищем експлуатації, можливість співпрацювати між собою різних КФС для створення ефектів, більших за суму частин окремих КФС, можливість поєднання декількох цілей.

КФС характеризуються чітко визначеними компонентами: з відомими характеристиками, описаними з використанням стандартизованої семантики та синтаксису. КФС повинні підтримувати гнучкість додатків та доменів. Для цього визначення компонентів має бути гнучким і відкритим. Архітектура повинна підтримувати точне опитування смарт-речей, щоб забезпечити гнучкість у створенні та адаптації віртуальних систем та сприяння інноваціям. КФС повинні підтримувати великий діапазон розмірів, складності та навантаження на додаток. І у простій, і у складній розподіленій системі повинні використовуватися ті ж самі компоненти. Компоненти мають бути зібрані та масштабовані швидко, навіть під час роботи. КФС повинна складатися з незалежних компонентів для забезпечення гнучкості, надійності та стійкості до змінних ситуацій. Розв'язки повинні існувати між архітектурними шарами, що дає змогу змінювати кожен шар, не впливаючи на інші шари. Для того, щоб система могла інтегрувати різні компоненти, інтерфейси до цих компонентів повинні базуватися на інтерпретованих та однозначних стандартах. Стандартизація інтерфейсів дозволить забезпечити різні компоненти існуючих систем і майбутніх систем. Адаптація досягається через гнучкість внутрішніх компонентів та зовнішню сумісність.

Інакше, до КФС висуваються різноманітні вимоги. Тому вважаємо за доцільне охарактеризувати кожен з видів КФС з урахуванням метрологічного та програмного забезпечення, яке використовується при їх конструюванні.

4.1. Види КФС

4.1.1. КФС «Розумне виробництво» - багатофункціональні смарт-машини, вирізняються малими розмірами, адаптивністю до потреб користувачів (реалізується шляхом збору потрібної функціональності на одній машині). Отримавши інформацію про змінені вимоги, КФС сама вносить корективи в технологічний процес. Прикладом розумного виробництва є виробництво металу з використанням точних ваг. Їх нормальне функціонування забезпечується калібрування, виконувани на місці, без демонтажу конструкції КФС. До прикладу, завдяки «man-in-loop» технології проводиться дистанційна атестація точних ваг, що призводить до покращення їх продуктивності в певних операційних діапазонах до значень робочих еталонів. Переважно для таких КФС застосовують програмну оболонку Linux, а віддалений доступ до вагопроцесорів компонентів КФС безпосередньо на робочих місцях забезпечують завдяки використанню промислового Ethernet, як стандартизованого варіанту мережевого протоколу Ethernet, адаптованого для промислових умов з метою автоматизації та керування технологічними процесами.

4.1.2. КФС «Розумні будівлі» - інтелектуальні будівлі (з мінімальним чи нульовим споживанням ресурсів) - потребують постійного моніторингу. Тому вони повинні бути підключені до мереж інтелектуальних сенсорів і контролюватися засобами КФС. Основною вимогою є досягнення нульового споживання енергії. Для цього вивчають теплові умови за допомогою інтелектуальних сенсорів температури локальної мережі та забезпечують адекватну ізоляцію при безперервному багатоточковому контролі температури. Значна увага приділяється попередній оцінці теплових умов на етапі будівництва, усунення містків холоду тощо. Для цього використовують такі методи і засоби контролю тепла: методи інфрачервоної діагностики з допомогою тепловізора, метод дискретно-точкового вивчення температурного режиму обмежувальних площин, моніторинг температур у часі за допомогою чіпів з вбудованими сенсорами температури, прикріпленими до внутрішньої та зовнішньої поверхонь обмежувальних площин тощо. Так виявляють та усувають містки холоду, досліджують енергетичні відбивні покриття з невідомим коефіцієнтом чорноти і керують роботою енергетичних підсистем для електропостачання, опалення та вентиляції. У переважній більшості таких КФС застосовують програмне забезпечення StructureWare Building Operation.

Щоб поведінка програмного забезпечення КФС відповідала його специфікації під час використання в певному середовищі, проводять функціональну перевірку. Орієнтуються на детерміністичні й на стохастичні системи. Специфікація виражає стан безпеки, яку треба задовольнити при всіх можливих виконаннях програмного забезпечення (для детерміністичних систем) або з необхідною мінімальною вірогідністю (для стохастичних систем). КФС працюють у недетермінованих середовищах. Стосовно програмного забезпечення це означає, що деякі його входи - це випадкові величини. Тому обчислюють ймовірність того, що програмне забезпечення відповідає специфікаціям безпеки. Відомі два методи перевірки КФС: імовірнісна модель перевірки (система моделюється як ланцюжок Маркова, а ймовірність обчислюється шляхом побудови множини рівнянь та їх чисельного розв'язку), статистична перевірка моделі (кожне виконання системи розглядається як випробування Бернуллі, і вірогідність обчислюється за методом Монте-Карло).

4.2. Проміжне програмне забезпечення (ППЗ - Middleware) є передумовою ефективної роботи КФС [2]. Воно надає послуги програмним додаткам, окрім тих, що доступні в операційній системі, з'єднує компоненти програмного забезпечення та корпоративні програми. ППЗ включає в себе веб-сервери, сервери додатків, системи управління контентом та аналогічні інструменти, що підтримують розроблення та доставлення додатків, і дає змогу здійснювати зв'язок та керування даними в розподілених додатках. Це особливо стосується інформаційних технологій, що базуються: на розширеній мові розмітки (XML); на протоколі обміну структурованими повідомленнями в розподілених обчислювальних системах при доступі до об'єктів (SOAP);

на веб-сервісах; на модульному підході (SOA) до розроблення програмного забезпечення, що заснований на використанні розподілених, слабо пов'язаних замінних компонентів, оснащених стандартизованими інтерфейсами для взаємодії за стандартизованими протоколами; на інфраструктурі Web 2.0 та на протоколі легкого доступу до каталогів (LDAP). Послуги, які можна розглядати як проміжні програми, включають інтеграцію корпоративних додатків, інтеграцію даних, орієнтовані на повідомлення ППЗ (MOM), брокери запиту об'єктів (ORBs) та корпоративні сервісні шини (ESB).

Іншими прикладами проміжного програмного забезпечення є:

- програмне забезпечення Mer, що не має ядра Linux і якому бракує інтерфейсу. Mer більше стосується мобільно-орієнтованих операційних систем постачальників обладнання;
- операційна система Android, що використовує ядро Linux і забезпечує систему додатків, яку розробники включають у свої програми. Крім того, Android забезпечує рівень ППЗ, включаючи бібліотеки, які надають такі послуги, як зберігання даних, екранне відображення, мультимедіа та веб-переглядач. Оскільки бібліотеки складаються на машинній мові, команди виконуються швидко. Бібліотеки Middleware також реалізують функції, специфічні для пристроїв, тому додатки не потребують залежності від варіантів між різними пристроями Android. Проміжний шар Android також містить віртуальну машину Dalvik та її основні бібліотеки для додатків Java.
- У технології моделювання ППЗ використовується в контексті архітектури високого рівня, яка застосовується для багатьох розподілених моделювань. Це – шар програмного забезпечення, який лежить між кодом додатка та інфраструктурою під час виконання. ППЗ складається з бібліотеки функцій та дозволяє виконувати ряд програм-моделювань (федератів) - пересилати ці функції з загальної бібліотеки, а не створювати їх повторно для кожної програми.
- Розробники бездротових мереж використовують ППЗ для вирішення проблем, пов'язаних із бездротовими мережами сенсора. Впровадження програми ППЗ дає змогу розробникам цих мереж інтегрувати операційні системи та апаратні засоби з різними додатками.
- Universal Home API або UHAPI - це інтерфейс прикладного програмування для приладів побутової електроніки, створений Форумом UHAPI. Метою UHAPI є змогу стандартному ППЗ працювати на платформах потокового аудіо / відео через апаратно-незалежний промисловий стандартний API.
- Набори програмного забезпечення для ідентифікації радіочастот забезпечують ППЗ для фільтрування зашумлених та надлишкових вихідних даних.
- ILAND - це проміжне програмне забезпечення, призначене для використання в режимі реального часу, що пропонує детерміновану підтримку реконфігурації в обмежений час.

4.3. Розумні вимірювальні засоби є важливою передумовою для створення КФС, оскільки вони представляють собою основні компоненти інформаційно-вимірювальних підсистем. Розумні вимірювальні засоби поділяються на такі підкласи: розумні сенсори, розумні перетворювачі, їх мережі, які можуть спільно об'єднуватись у сучасних бездротових сенсорних мережах (BSM).

Розумний сенсор містить в одному корпусі чутливий елемент, мікросхеми аналогового інтерфейсу, АЦП і інтерфейс шини. Крім цього, у розумному сенсорі є мікропроцесор, який кондиціонує сигнали (встановлює амплітуди та форми сигналів перед відправленням їх до подальших вузлів, відфільтровує небажані шуми та усуває помилки перед відправленням даних). Проте, створення класу розумних сенсорів нового покоління передбачає необхідність у додаткових функціональних можливостях: самотестування, самоідентифікації, самовалідизації або самоадаптації. Доцільними є такі можливості розумних сенсорів, як самокалібрування та самодіагностика, можливість опрацювати сигнал, а також мультисенсорні можливості. Конструктивно розумний сенсор температури виконується як первинний аналоговий або цифровий термочутливий перетворювач, оснащений блоком опрацювання сигналу та інтерфейсом, який у змозі виконати низку розумних метрологічних функцій завдяки спеціальному метрологічному програмному забезпеченню.

Практично це може бути інтелектуальний сенсор температури з низкою спеціалізованих алгоритмів, передбачених на етапі проектування й виготовлення або установлених пізніше, тобто сенсор з такими вбудованими алгоритмами, які необхідні для забезпечення виконання спеціалізованих метрологічних функцій. Зокрема, такі функції включають здатність реалізувати автоматичне перемикання діапазонів вимірювання, залежно від значення вхідного сигналу; автоматичну самовалідизацію, самоперевірку, самодіагностику тощо; введення поправок у покази, коли зафіксовано дію фактора впливу; лінеаризацію номінальних характеристик; компенсацію температури холодного з'льоту термопар.

5. Результати і обговорення

Виходячи з прикладних аспектів роботи КФС з їх підсистемами температурного контролю необхідно розробляти засоби вимірювань, в тому числі, разових застосувань, так-звані ad-hoc підсистеми, або ж підсистеми «на вимогу». Мережа «на вимогу» є перескоковою, оскільки не стосується наперед усталеної

структури, зокрема відсутні маршрутизатори у дротових мережах чи точки доступу в організованій структурі БСМ [3]. Кожен існуючий вузол мережі приймає участь у маршрутизації, перекидаючи дані на сусідні вузли, оскільки визначення того, на які вузли здійснюється перекидання, виконується динамічно на основі мапи з'єднань мереж. У додаток до класичної маршрутизації мережі «на вимогу» можуть використовувати флудінг (англ. - Flooding) для перекидання даних. Таким є простий роутинговий алгоритм, за яким кожний вхідний пакет висилається на всі можливі адреси, за винятком того пункту, звідки він поступив. Флудінг поширений у мостах та в системах, таких як UseNet і файлообмінних мережах (peer-to-peer file sharing), а також як частина деяких роутингових протоколів, зокрема OSPF, DVMRP, а вони вже застосовуються у бездротових мережах «на вимогу».

Децентралізований тип БСМ – це багатоланкові мережі, складаються з бездротових автономних хостів, де кожен хост може служити, як маршрутизатор для передачі трафіку від інших вузлів. Бездротові однорангові мережі «на вимогу» охоплюються широким спектром мережевих видозмін, що містять сенсори, мобільний механізм перескоків, персональну специфіку чи інші мережі. Наукові розробки у цій галузі мають передбачати навчання сенсора (переведення його з розряду інтелектуальних - до розумних), вивчення безпекових аспектів за рахунок інтелектуальних можливостей вузла, зони покриття сенсора за його випадкового чи детермінованого розміщення, розташування об'єкта, визначення впливу розміщення сенсора, вивчення енергетичної ефективності передавання інформації і розкладу діяльності, маршрутизації, топологічних зв'язків, поширення даних і їх нагромадження, дослідження впливу дерева реконфігурації і конструювання конкретної топології. Для нормальної роботи мережева топологія передбачає розгляд не тільки сенсорних вузлів, а й базових станцій і крос-шарів. Структура крос-шарів є важливою для БСМ, оскільки вони можуть бути використані для оптимальної модуляції з метою підвищення параметрів передавання, таких як швидкість передачі даних, ефективність використання енергії тощо.

6. Висновки

Безперебійна та надійна робота кібер-фізичних систем базується на коректній організації вхідних потоків інформації, завдяки достовірній роботі підсистем, в тому числі, температурного контролю, а також надійного програмного забезпечення. Наявність різних видів сенсорів для кібер-фізичних систем вимагає не тільки уніфікованих вихідних сигналів різних типів сенсорів (для цього здійснюється кондиціонування їх сигналів [4]), скільки опрацювання значної, переважно надлишкової, кількості даних. Для цього слід застосовувати спеціальні алгоритми [5]. Водночас, для забезпечення метрологічної достовірності з допомогою інших алгоритмів опрацьовуються спільно дані, отримувані паралельно від різних типів сенсорів (data fusion). Це вимагає розроблення спеціального програмного забезпечення, яке, у свою чергу, потребує окремо виділеної метрологічної перевірки [6].

Подяка

Автори висловлюють вдячність колективу кафедри Інформаційно-вимірювальних технологій Національного університету «Львівська політехніка», Україна, за надану допомогу та всемірне сприяння у підготовці статті.

Список літератури

1. Микійчук М.М., Стадник Б.І., Яцишин С.П., Луцик Я.Т. (2017). Розумні вимірювальні засоби для кібер-фізичних систем. *Вимірювальна техніка та метрологія*: № 77, с.3-17.
2. "What is Middleware?". *Middleware.org. Defining Technology*. (2008). Retrieved 2013-08-11.
3. Ad-hoc Sensor Networks. <http://www.brunel.ac.uk/cedps/electronic-computer-engineering/research-activities/wnc/ad-hoc-sensor-networks>
4. Дорожовець М.М. (2014). Розділ «Кондиціонування сигналів сенсорів». У кн. «Сенсори». *Бескид Біт*, Львів, Україна, с.124-152.
5. Яцишин С.П., Микитин І.П., Кравець І.П. (2010). *Пожежні сповіщувачі. Засади оптимізації роботи та алгоритми прийняття рішень*, *Пожежна безпека*: № 17, с.14-19.
6. Олесків О.М., Микитин І.П. (2014). Аналітичний огляд процедур та методів метрологічної перевірки програмного забезпечення. *Вимірювальна техніка та метрологія*: № 75, с.2-7.

References

- [1] M. Mykyuchuk, B. Stadyk, S. Yatsyshyn, Ya. Lutsyk, "Measuring Smart Means for Cyber-Physical Systems", *Measuring Equipment and Metrology*, Lviv, Ukraine, iss.77, p.3-17, 2017.
- [2] "What is Middleware", *Middleware.org. Defining Technology*, 2008. Retrieved 2013-08-11.
- [3] Ad-hoc Sensor Networks. Brunel Univ. London. [On-line]. Available: <https://www.brunel.ac.uk/electronic-and-electrical-engineering/research-and-phd-programmes/Research-areas/Ad-hoc-Sensor-Networks>.
- [4] M. Dorozhovets. "Conditioning the Sensors Signals" in *Sensors*. Lviv, Ukraine: Publ. House "Beskyd-Bit", p.124-152, 2014.
- [5] S. Yatsyshyn, I. Mykytyn, I. Kravets, "Fire Sensors. Principles of Optimization of the Work and Algorithms of Decision Making", *Fire Safety*, Lviv, Ukraine, iss.17, p.14-19, 2010.
- [6] O. Oleskiv, I. Mykytyn, "Analytical Review of Procedures and Methods of Metrological Testing of Software",

