УДК 004.7:004.9

ВИКЛИКИ ТА РІШЕННЯ ІНЖЕНЕРІЇ МОБІЛЬНИХ КІБЕРФІЗИЧНИХ СИСТЕМ

Мазикін О.А.
oleksandrmazikin@gmail.com
Черкаський державний фаховий бізнес-коледж
Медолиз М.М.
м. Черкаси, Україна

Традиційно інформаційні технології будувалися як ізольовані та стабільні системи. Класичний дата-центр або серверна – це добре контрольоване середовище з налаштованим кліматом, резервними джерелами живлення та чітко визначеним розташуванням обладнання. Уся інфраструктура заздалегідь спроєктована, а зміни вносяться рідко і за певними правилами. У таких умовах адміністрування є відносно простим: легко відстежити роботу систем, контролювати навантаження та швидко знаходити несправності. Якщо виникає проблема, її зазвичай можна локалізувати до конкретного сервера, мережевого пристрою або кабелю. Це значно спрощує обслуговування та ремонт.

Крім того, фізичний доступ до обладнання суворо обмежений. Використовуються системи безпеки, контроль доступу та фізичні бар'єри, що захищають інфраструктуру від несанкціонованого втручання. Завдяки цьому ризики, пов'язані з людським фактором або зовнішніми впливами, мінімізуються. Загалом така модель забезпечує високу надійність і передбачуваність роботи систем, але водночас вона є менш гнучкою і гірше пристосованою до швидких змін та масштабування.

Сьогодні IT-галузь переживає суттєві зміни: обчислювальні ресурси більше не зосереджені лише в дата-центрах, а розподіляються і працюють безпосередньо у фізичному середовищі. Наприклад, сучасні промислові дрони, складські AGV-системи (Automated Guided Vehicles) чи роботизовані платформи - це вже не просто техніка, а повноцінні мобільні обчислювальні вузли. Вони мають достатню потужність для обробки даних на місці, зокрема для роботи з

нейромережами, а також оснащені різними сенсорами (лідари, інерціальні системи) та виконавчими механізмами.

Ключова проблема мобільних кіберфізичних систем полягає в тому, як забезпечити стабільну та передбачувану передачу даних. На відміну від статичних серверів з дубльованою оптоволоконною лінією, рухомі агенти залежать від бездротових технологій, які піддаються впливу фізичних перешкод, радіоінтерференції та багатопроменевого поширення сигналу [1].

У масштабних індустріальних середовищах мобільні агенти змушені постійно перемикатися між точками доступу, а стандартний протокол Wi-Fi функціонує за парадигмою «break-before-make» (відключення перед новим з'єднанням). Це ініціює затримки під час хендоверу (handoff), що генерує втрату пакетів даних. Для системи, яка працює в режимі реального часу, затримка у кілька сотень мілісекунд може призвести до критичної просторової помилки.

Враховуючи ймовірність деградації сигналу, архітектура має передбачати автономні протоколи безпеки (Network Loss Autonomy):. При втраті з'єднання ініціюються апаратні сторожові таймери (Watchdogs). Відповідно до алгоритму, система або переходить у безпечний стан (Safe Mode) з плавною зупинкою, або продовжує місію, спираючись виключно на локальні обчислювальні потужності (Edge Computing) та бортову сенсорику[2].

Програмне забезпечення кіберфізичних систем кардинально відрізняється від класичних десктопних чи серверних рішень. Воно вимагає детермінованості, яку забезпечують операційні системи реального часу (RTOS), та модульного підходу до обробки даних.

Фреймворк ROS (Robot Operating System), незважаючи на назву, не є повноцінною операційною системою. Це спеціалізований middleware, який працює поверх UNIX-подібних систем, найчастіше Ubuntu.

ROS надає зручну архітектуру для побудови робототехнічних систем: окремі компоненти (наприклад, драйвери пристроїв або модулі навігації) працюють як незалежні вузли (nodes) і обмінюються даними через спеціальний

механізм «публікатор–підписник». Такий підхід дозволяє гнучко комбінувати різні частини системи та масштабувати її.

Водночас ефективність роботи всієї системи значною мірою залежить від правильної організації цього графа вузлів. Тому оптимізація взаємодії між вузлами, зменшення затримок і навантаження на мережу є важливим завданням для сучасного адміністратора або розробника [3].

Щоб забезпечити масштабованість і уникнути конфліктів між програмними компонентами, використовують контейнеризацію, наприклад, за допомогою Docker або його легших аналогів для вбудованих систем. Це дає змогу ізолювати окремі процеси разом із їхніми залежностями та забезпечити їхню стабільну роботу [4].

Еволюція обчислювальних систем не просто вдосконалює технології, а й кардинально змінює саму логіку побудови безпеки. Якщо класична кібербезпека фокусується на захисті конфіденційності та цілісності інформації, то кіберфізична безпека (Cyber-Physical Security) спрямована на захист фізичного середовища від скомпрометованих апаратних комплексів [2].

У сучасних умовах проблема вразливості обчислювальних систем набуває багатовимірного характеру, виходячи за межі суто інформаційних чи фінансових ризиків. Якщо компрометація бази даних традиційно асоціюється з економічними втратами, то несанкціонований доступ до промислових маніпуляторів, аграрних безпілотних апаратів або медичних роботизованих систем створює безпосередню загрозу життю та здоров’ю людей. Таким чином, безпека інформаційних технологій трансформується у сферу, де цифрові ризики мають прямі фізичні наслідки.

Особливу увагу в цьому контексті слід приділяти захисту апаратних інтерфейсів. Мобільні системи функціонують у відкритому середовищі, що підвищує ймовірність фізичного доступу зловмисників до портів вводу-виводу, зокрема USB та UART. З огляду на це сучасні протоколи безпеки передбачають комплекс превентивних заходів: відключення налагоджувальних інтерфейсів на рівні ядра операційної системи, застосування зашифрованих завантажувачів

(Secure Boot), а також апаратне блокування потенційних точок входу до системи. Такий підхід формує нову парадигму захисту, де інтеграція програмних і апаратних механізмів стає необхідною умовою забезпечення цілісності та стійкості обчислювальних систем.

Отже, інтеграція обчислювальних потужностей у мобільні фізичні об’єкти зумовлює необхідність переосмислення ролі фахівців з інфраструктури, адже їхня діяльність більше не обмежується суто програмним адмініструванням. У сучасних умовах інженер у сфері RoboOps постає як мультидисциплінарний експерт, здатний поєднувати компетенції мережевого архітектора, спеціаліста з кіберфізичної безпеки та системного інженера. Такий фахівець не лише володіє знаннями щодо побудови та захисту мережевих структур, але й розуміє фізику процесів, що відбуваються у взаємодії апаратних і програмних компонентів у реальному часі. Це забезпечує комплексний підхід до управління роботизованими системами, де технічна експертиза поєднується з глибоким розумінням алгоритмічних та фізичних аспектів їхньої роботи.

Список використаних джерел:

1. Quigley M. et al. ROS: an open-source Robot Operating System // Proceedings of the IEEE International Conference on Robotics and Automation (ICRA Workshop). 2009. P. 1–6.
2. Lee E. A. Cyber-Physical Systems: Design Challenges // Proceedings of the 11th IEEE International Symposium on Object-Oriented Real-Time Distributed Computing (ISORC). 2008. P. 363–369.
3. Merkel D. Docker: Lightweight Linux Containers for Consistent Development and Deployment // Linux Journal. 2014. № 239. P. 2.
4. Maruyama Y., Kato S., Azumi T. Exploring the Performance of ROS2 // Proceedings of the 13th International Conference on Embedded Software. – 2016. P. 1–10.