

Мнушка О.В.

Харківський національний
автомобільно-дорожній університет,
м. Харків, Україна,
E-mail: mnushka@live.com

**SCADA НА ОСНОВІ ПРОМИСЛОВОГО
ІНТЕРНЕТУ РЕЧЕЙ: АРХІТЕКТУРА СИСТЕМИ**

УДК 004.7

У роботі проаналізовано вимоги до побудови розподілених систем керування технологічними процесами (Supervisory Control And Data Acquisition, SCADA) на основі технологій промислового Інтернету речей (Industrial Internet of Things, IIoT). Запропоновано архітектуру системи телематики на основі хмарних технологій та технологій IIoT. Розглянуто основні модулі такої системи, їх призначення та технічні характеристики.

***Ключові слова:** Internet of Things (IoT), протокол, хмарні сервіси, телематика, технічний сервіс, НМІ*

Актуальність проблеми. Високий темп прогресу пристроїв та технологій IoT обумовлює їх широке застосування в усіх сферах повсякденної діяльності людини. Основними перевагами технологій IoT для систем телематики та технічного сервісу є наявність великої номенклатури технічних засобів (сенсорів) для збирання та передавання даних з об'єктів. В залежності від задачі використовують сенсорні мережі, технології машинової взаємодії (machine-to-machine, M2M), взаємодії між транспортними засобами (vehicle-to-vehicle, V2V) [1-3]. Системи IoT промислового призначення мають свої особливості відносно до звичайних систем IoT, в першу чергу в питаннях надійності, швидкодії, реального часу, безпеки тощо [4].

Метою роботи є формування вимог та розробка архітектури SCADA-системи для задоволення вимог технічного сервісу та телематики на основі аналізу архітектури існуючих систем різного призначення.

Аналіз останніх публікацій за даною проблематикою. Референсна модель IoT (рис. 1 [5]) містить наступні рівні та компоненти:

- рівень додатків (application);
- рівень підтримки послуг та додатків (service);
- рівень мереж (network);
- рівень пристрою (device);
- рівень керування (management);
- рівень безпеки (security)

Рівень додатків, що знаходиться на верхівці ієрархії, містить додатки IoT, які безпосередньо реалізують людино-машинний інтерфейс (НМІ). Рівень пристроїв реалізує функції пристроїв (сенсорів, інтелектуальних сенсорів й т. п.), а також функції шлюзів зв'язку. Рівень мережі забезпечує інкапсуляцію даних від пристрою та функції організації мереж – керування, автентифікацію, авторизацію, мобільність тощо. На рівні підтримки послуг та додатків забезпечуються загальні (обробка, зберігання, аналіз даних) та спеціальні для окремих додатків чи застосувань можливості.

Вертикальні наскрізні рівні керування та безпеки також містять загальні та спеціальні можливості, які є характерними для кожного горизонтального рівня (домена).

Референсна модель є відправною точкою для побудови будь-яких додатків IoT та чітко розмежовує задачі, які реалізуються на кожному рівні. Відповідно до такої моделі побудовано існуючі архітектури систем та протоколи обміну.

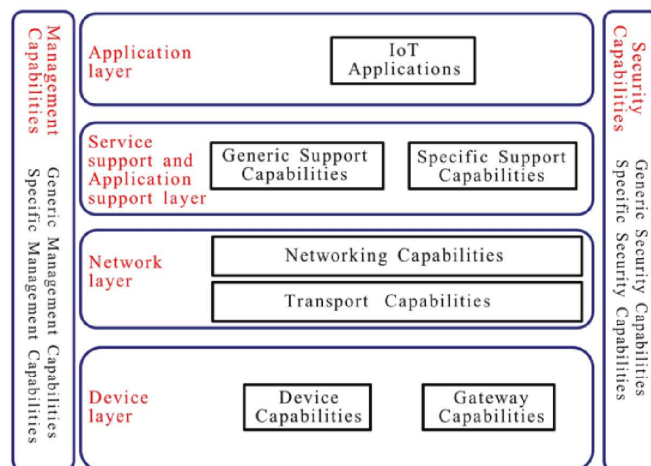


Рис. 1 – Еталонна модель IoT Y.4000/Y.2060 [5]

З точки зору загальної архітектури ПоТ є підмножиною IoT, при цьому треба врахувати особливості побудови промислових мереж, які наведені у табл. 1 відповідно до [4].

Таблиця 1

Порівняння промислових та комерційних мереж

Характеристика	ПоТ	IoT(комерційний)
Функціональне призначення	Контроль обладнання	Передавання даних та їх обробка
Типове застосування	Промисловість	Корпоративні та домашні застосунки
Особливості ієрархії	Функціонально розділені ієрархії із великої кількості протоколів	Уніфіковані інтегровані ієрархії та протоколи
Чутливість до помилок	Висока	Невисока
Надійність	Висока	Середня
Час обігу (RTT)	Менше 10 мс	Більше 50 мс
Передбачуваність	Висока	Низька
Структура даних	Малі пакети, періодичний або аперіодичний трафік	Великі пакети, аперіодичний трафік
Умови застосування	Високий рівень пилу, шуму, вібрації тощо	Чисті умови, чутливе обладнання

Підмножиною ПоТ є концепція Industrie 4.0, що, можливо, більше зосереджується на ефективності промислових процесів, в той час, коли ПоТ включає в себе всі аспекти промислових операцій, зосереджуючи увагу не тільки на ефективності процесу, але й на управлінні активами, технічному обслуговуванні. Із табл. 1 можна зробити висновок, що незважаючи на те що IoT та ПоТ складаються із взаємозв'язаних інтелектуальних пристроїв, що дозволяють здійснювати дистанційне зондування, збирання, обробку, моніторинг та керування даними, параметри, що виділяють підмножину ПоТ з IoT, є суттєвими вимогами до безперервної роботи та безпеки, різняться також операційні технології, що використовуються в промисловому секторі [5].

Референсна архітектура ПоТ [6] є також багаторівневою. В рекомендаціях наведено три різні шаблони:

- тривірнева (Three-Tier) модель;

- архітектура підключення та управління інтерфейсом шлюзів (Gateway-Mediated);
- багаторівнева модель DataBus.

З точки зору реалізації SCADA системи промислового призначення найбільш прийнятними є архітектури Three-Tier та DataBus, що дозволяють реалізувати весь функціонал. Gateway-Mediated архітектура забезпечує підключення різних ізольованих мереж до мережі підприємства.

В [7-10] розглянуто варіанти побудови SCADA систем різного призначення, архітектура та призначення основних блоків практично співпадає (рис. 2). В ній є один або декілька серверів, інтерфейс клієнта (HMI), контролери та програмовані логічні контролери (ПЛК), мережа сенсорів.

Відносно недавно основними системами керування різними об'єктами та технологічними процесами були локальні АСУ або SCADA-системи без можливості (або з дуже обмеженими можливостями) віддаленого моніторингу за роботою програмного забезпечення та устаткування. Із розвитком хмарних технологій такі системи все частіше продаються кінцевому користувачеві у вигляді хмарних сервісів (в першу чергу SaaS, але можливі й інші моделі – PaaS та IaaS)

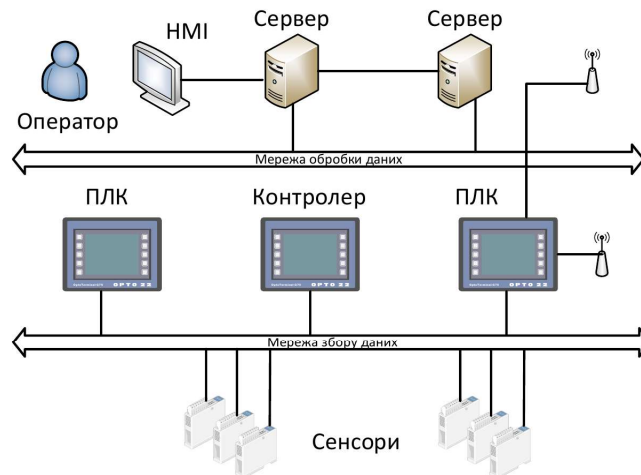


Рис. 2 – Типова структура SCADA

Архітектура та призначення складових запропонованої системи. Розглянемо архітектуру та призначення складових запропонованої клієнт-серверної SCADA-системи для потреб технічного сервісу та телематики (рис. 3). У даному випадку на першому етапі немає задач керування складними та небезпечними процесами, а основні задачі – це задачі збирання та обробки даних.

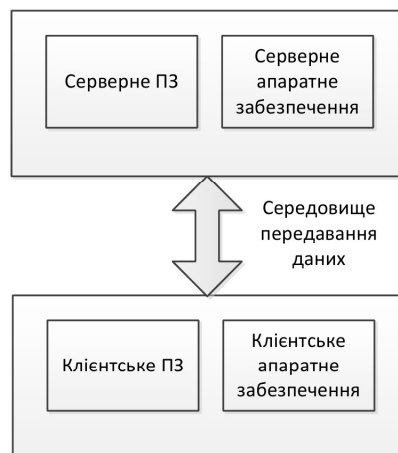


Рис. 3 – Узагальнена архітектура системи

На нижньому рівні, що складається з обладнання та програмного забезпечення (ПЗ) на об'єкті моніторингу, здійснюється збирання даних з об'єктів управління. У якості таких об'єктів може бути будь-яке обладнання що підтримує один із стандартних промислових протоколів обміну, наприклад Modbus, Profibus, CAN та ін.

У залежності від призначення апаратне забезпечення нижнього рівня має декілька портів Modbus, аналогові входи ($\pm 20\text{mA}$, $0-20\text{mA}$, $4-20\text{mA}$) та виходи, цифрові входи та виходи, що дозволяє підключити не тільки устаткування, але й різні сенсори. За необхідності можуть використовуватися модулі розширення входів-виходів (InteliSys NT, Siemens, Овен ін.) та конвертори протоколів.

На цьому рівні також працює обладнання зв'язку – модеми або маршрутизатори. Такі пристрої виступають або в якості таких, що керуються сервером (слейв-пристрої), або таких, що є активними учасниками обміну даними (майстер-пристрої).

Слейв-пристрої виконують наступні задачі:

- ініціалізація з'єднання із сервером;
- прийом команд із сервера і трансляція їх на підключений пристрій;
- прийом відповіді від пристрою та передавання даних на сервер.

ПЗ слейв-пристроїв має мінімальний набір функцій керованого модема, а їх налаштування здійснюється через веб-інтерфейс, через сервер або інші комунікаційні порти: Bluetooth, WIFI, Modbus тощо.

Майстер-пристрої виконують ті ж самі задачі, що й слейв-пристрої, але додатково можуть виконувати наступні функції:

- попередня обробка даних;
- тимчасове зберігання даних на час відсутності зв'язку із сервером;
- керування під'єднаними пристроями за заданими алгоритмами.

Майстер-пристрої за необхідності об'єднують у локальні мережі та створюють ієрархії. Майстер-пристрої можуть виконувати функції модема, маршрутизатора та програмованого логічного контролера.

За рахунок розширеного набору функцій схемотехніка та ПЗ майстер-пристроїв є більш комплексним, а їх налаштування може здійснюватися за допомогою локального ПЗ, в т. ч. локального веб-інтерфейсу.

За оцінками спеціалістів RedPine (<http://www.redpine.pro>) для таких архітектур на долю базових компонентів верхнього рівня приходиться до 55-60% (ПЗ – до 40%), а на долю компонентів нижнього рівня – 40-45% (ПЗ – до 25%), таким чином, загальна значимість ПЗ складає до 65%, причому ПЗ верхнього рівня несе навантаження з обробки та інтерпретації даних, що надходять з нижнього рівня, а також надає інструменти для прийняття рішень оператором або в автоматичному режимі.

Для таких систем велику значимість також має середовище передавання даних. Для віддалених об'єктів єдиним прийнятним засобом передачі даних є мережі мобільного зв'язку та Інтернету. Наразі в Україні переважають технології 2G, які поступово витісняються технологіями 3G.

Для перших характерні невисокі швидкості передачі (до 86 кбіт/с), що може мати негативний вплив на час реакції оператора, але покриття території є кращим. Зазначимо також, що у світі є стала тенденція відмови від мереж другого покоління і перехід на мережі 3-4, а подекуди й 5 покоління. Інші варіанти організації зв'язку є економічно необґрунтованими, особливо для систем, орієнтованих на режим роботи у форматі 24/7. З урахуванням вище сказаного структура клієнтської частини – інтеграційно-комунікаційного контролера, буде мати наступний вигляд (рис. 4).

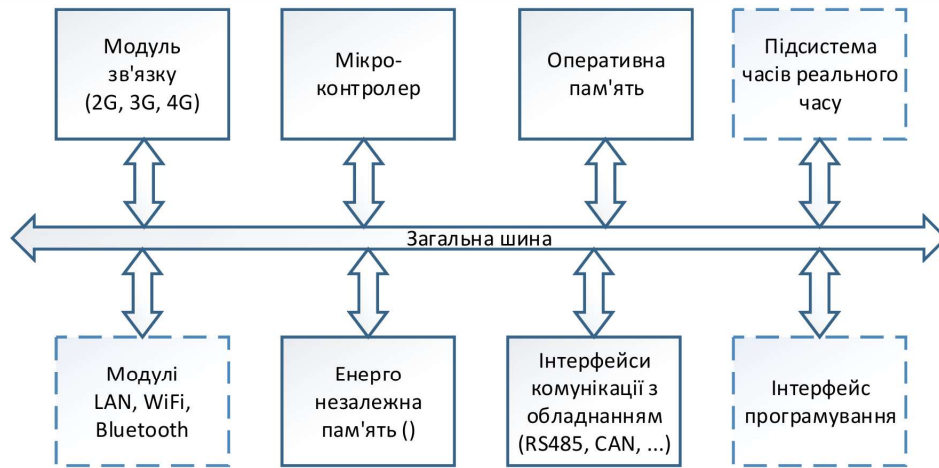


Рис. 4 – Структура інтеграційно-комунікаційного контролера

В обраній архітектурі модулі, обведені пунктирними лініями є необов'язковими та відсутні у базовій конфігурації задля здешевлення системи. При розширенні функціональних задач запропонованої системи ці модулі можуть бути доданими без особливих ускладнень.

У якості інтеграційно-комунікаційного контролера (рис. 4) використано мікрокомп'ютер Raspberry Pi третього покоління, що має можливості підключення як до мережі Ethernet, так і до інтелектуальних сенсорів, побудованих на базі Raspberry Pi Zero, Arduino тощо. Також такий підхід дозволяє використовувати стандартне програмне забезпечення ОС Linux. Мережу сенсорів доцільно виконувати із використанням стандартного протоколу Modbus та інтерфейсу RS 485.

Модуль зв'язку виконано на чіпах SimCom 5360 (3G HSPA+), у якості альтернативи розглядалися SimCom 7000, Telit xE866, Telit xE910, але вони мають більшу вартість при аналогічному функціональному наповненні. За рахунок використання можливостей самих модулів, що часто підтримують стек TCP/IP, FTP, HTTPS, HTTP, HTTPS, SMTP, POP3, DNS на рівні вбудованих AT-команд, спрощується програмування контролера, що відповідає за комунікацію із сервером SCADA. Код модуля обміну написано мовою C++ із використанням POSIX threads, libmodbus, curl, openssl (для захисту даних).

Архітектура серверної частини (рис. 5) містить набір із трьох сервісів – накопичення, обробки та комунікацій. Останній забезпечує зв'язок з оператором (людиною) та з інтеграційно-комунікаційним контролером. Ці сервіси виконуються на базі серверу Intel Core i5 / 32 Gb ОЗП / 2 x 500 Gb HDD.



Рис. 5 – Структура серверної частини системи

Для організації комунікації між сервером та контролером було обрано протокол MQTT, що працює над TCP/IP та забезпечує чотири рівні якості послуг. Взаємодію між клієнтом та сервером організовано на основі архітектури REST, що забезпечує просту інтеграцію у систему Web-сервісів та використання стандартних протоколів.

На етапі досліджень ефективності прийнятих рішень для забезпечення безпеки даних між клієнтом і сервером, сервером та комунікаційним контролером використовується протокол TLS. В подальшому планується додати додаткові рівні безпеки, наприклад двоетапна автентифікація.

За допомогою розробленої системи були реалізовані алгоритми керування антенними пристроями із режимом стеження за джерелом сигналу [11-12].

Висновки:

1. Проведено аналіз вимог до систем на основі систем ІоТ, основними відмінностями таких систем від традиційних систем на основі ІоТ є підвищені вимоги до безпеки та надійності.

2. Традиційні системи SCADA (із використанням клієнта на персональному комп'ютері) не задовольняють вимогам ІоТ у розрізі доступу до даних у будь-якому місці та у будь-який час.

4. Перенесення SCADA у хмари додає проблем із забезпеченням безпеки та надійності даних. Доцільним є організація таких систем на основі ІааS [13]

5. Запропоновано архітектуру інтегрованої універсальної система віддаленого контролю та управління, основаної на використанні архітектури REST. Реалізовано ядро серверної частини системи, а також інтеграційно-комунікаційний контролер.

Перспективами подальших досліджень є аналіз методів побудови ефективних інтерфейсів користувача (HMI [14-15]) та розробка клієнтської частини системи.

Література:

1. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network – Performance evaluation / K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, J. Martin // *Transportation Research Part C: Emerging Technologies*, 2016. – PP. 168-184
2. *Towards 5G: Applications, Requirements and Candidate Technologies.* / R. Vannithamby (ed.), S. Talwar (ed.). – J. Wiley & Sons, 2017. – 466 p.
3. *Machine-to-machine (M2M) Communications. Architecture, Performance and Applications* / C. Anton-Haro (ed.), M. Dohler (ed.). – Woodhead Publishing, 2017. – 410 p.
4. Galloway B. Introduction to Industrial Control Networks / B. Galloway, G. P. Hancke // *IEEE Communications Surveys & Tutorials*. – 2013. – vol. 15, no. 2. – PP. 860-880.
5. Recommendation ITU-T Y.2060. Overview of the Internet of things. – ITU, Geneva, 2013. – 22 p.
6. *The Industrial Internet of Things Volume G1: Reference Architecture.* – IIC, 2017. – 58 p.
7. Implementation of SCADA for multiple telemetry units while using GSM for communication / Q. ul. Ain, M. Shah, M. Khan, S. A. Mahmud // *2015 International Conference on Emerging Technologies (ICET)*. – Peshawar, 2015. – pp. 1-4.
8. How can I ... Select PlantStruxure reference architectures. – Schneider Electric, 2017. – Режим доступу: <https://www.schneider-electric.com.co/documents/News/Ecuador/Scada.pdf>.
9. Fu C. The application of embedded system in Supervisory Control and Data Acquisition System (SCADA) over wireless sensor and GPRS networks / C. Fu, Z. Ni, // *2015 IEEE 9th Int. Conf. on Anti-counterfeiting, Security, and Identification (ASID)*. – Xiamen, 2015. – PP. 81-85.

10. Paul S. Design of SCADA based wireless monitoring and control system using ZigBee / S. Paul, S. Narang, // 2015 Annual IEEE India Conference (INDICON).– New Delhi, 2015. – PP. 1-6.
11. Мнушка О.В. Системы управления позиционированием и слежением мобильных спутниковых антенных установок / О. В. Мнушка / Восточно-европейский журнал передовых технологий. – X., 2013. – Т. 5. – №9(65). – С. 39-45.
12. Мнушка О. В. Адаптивна система керування позиціонуванням супутниковою антеною / Мнушка О.В., Ніконов О.Я., Савченко В.М. // Вісник Національного технічного університету "Харківський політехнічний інститут". Зб. наук. праць. Серія: Інформатика та моделювання. – Харків: НТУ "ХПИ". – 2015. – № 32 (1141). – С. 120-127 с.
13. Church P. Moving SCADA Systems to IaaS Clouds / [P. Church, H. Mueller, C. Ryan et al] // IEEE Int. Conf. on Smart City/SocialCom/SustainCom (SmartCity). – Chengdu, 2015. – PP. 908-914.
14. Scripting engine for SCADA HMI / [M. Tandel, U. Joshi, A. Golhani et al] //2nd Int. Conf. for Convergence in Technology (I2CT). – Mumbai, 2017. – PP. 492-496.
15. Reeser J. Maintaining HMI and SCADA Systems Through Computer Virtualization / J. Reeser, T. Jankowski, G. M. Kemper // IEEE Transactions on Industry Applications. – 2015. – vol. 51. – no. 3. – PP. 2558-2564.

Summary

Mnushka O.V. SCADA based on the industrial Internet of Things: architecture of the system

In this paper the requirements for the construction of distributed monitoring systems (Supervisory Control and Data Acquisition, SCADA) based on technologies of the industrial Internet of Things (IIoT) was analyzed. The architecture of telematics system based on cloud technologies and technologies IIoT is proposed. The main modules of such system, their purpose and technical characteristics are considered.

Keywords: Internet of Things (IoT), protocol, cloud-based services, telematics, technical service, HMI

References

1. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network – Performance evaluation / K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, J. Martin // Transportation Research Part C: Emerging Technologies, 2016. – PP. 168-184
2. Towards 5G: Applications, Requirements and Candidate Technologies. / R. Vannithamby (ed.), S. Talwar (ed.). – J. Wiley & Sons, 2017. – 466 p.
3. Machine-to-machine (M2M) Communications. Architecture, Performance and Applications / C. Anton-Haro (ed.), M. Dohler (ed.). – Woodhead Publishing, 2017. – 410 p.
4. Galloway B. Introduction to Industrial Control Networks / B. Galloway, G. P. Hancke // IEEE Communications Surveys & Tutorials. – 2013. – vol. 15, no. 2. – PP. 860-880.
5. Recommendation ITU-T Y.2060. Overview of the Internet of things. – ITU, Geneva, 2013. – 22 p.
6. The Industrial Internet of Things Volume G1: Reference Architecture. – IIC, 2017. – 58 p.
7. Implementation of SCADA for multiple telemetry units while using GSM for communication / Q. ul. Ain, M. Shah, M. Khan, S. A. Mahmud // 2015 International Conference on Emerging Technologies (ICET). – Peshawar, 2015. – pp. 1-4.

8. How can I ... Select PlantStruxure reference architectures. – Schneider Electric, 2017. – URL: <https://www.schneider-electric.com.co/documents/News/Ecuador/Scada.pdf>.
9. Fu C. The application of embedded system in Supervisory Control and Data Acquisition System (SCADA) over wireless sensor and GPRS networks / C. Fu, Z. Ni, //2015 IEEE 9th Int. Conf. on Anti-counterfeiting, Security, and Identification (ASID). – Xiamen, 2015. – PP. 81-85.
10. Paul S. Design of SCADA based wireless monitoring and control system using ZigBee / S. Paul, S. Narang, // 2015 Annual IEEE India Conference (INDICON).– New Delhi, 2015. – PP. 1-6.
11. Mnushka O.V. Sistemy upravleniya pozicionirovaniem i slezheniem mobil'nyh sputnikovyyh antennyyh ustanovok / O. V. Mnushka / Vostochno-evropejskij zhurnal peredovyh tekhnologij. – H., 2013. – T. 5. – #9(65). – S. 39-45.
12. Mnushka O. V. Adaptyvna systema keruvannya pozytsionuvannyam suputnykovoyu antenoyu / Mnushka O.V., Nikonov O.Ya., Savchenko V.M. // Visnyk Natsional'noho tekhnichnoho universytetu "Kharkivs'kyi politekhnichnyy instytut". Zb. nauk. prats'. Seriya: Informatyka ta modelyuvannya. – Kharkiv: NTU "KhPI". – 2015. – # 32 (1141). – S. 120-127.
13. Church P. Moving SCADA Systems to IaaS Clouds / [P. Church, H. Mueller, C. Ryan et al] // IEEE Int. Conf. on Smart City/SocialCom/SustainCom (SmartCity). – Chengdu, 2015. – PP. 908-914.
14. Scripting engine for SCADA HMI / [M. Tandel, U. Joshi, A. Golhani et al] //2nd Int. Conf. for Convergence in Technology (I2CT). – Mumbai, 2017. – PP. 492-496.
15. Reeser J. Maintaining HMI and SCADA Systems Through Computer Virtualization / J. Reeser, T. Jankowski, G. M. Kemper // IEEE Transactions on Industry Applications. – 2015. – vol. 51. – no. 3. – PP. 2558-2564.