УДК 621.317.73
DOI: 10.31891/2219-9365-2020-66-2-13

ФОРКУН Ю. В., ФОРКУН І. В.,
МАКАРИШКІН Д. А., ФЕНЕНКО В. О.
Хмельницький національний університет

СУЧАСНИЙ СТАН ПРОБЛЕМ ПРОМИСЛОВИХ БАГАТОРІВНЕВИХ СИСТЕМ КЕРУВАННЯ НА ОСНОВІ КОНЦЕПЦІЇ SCADA-СИСТЕМ

В статті наведено сучасний стан проблеми промислових багаторівневих систем керування на основі програмно-технічних комплексів SCADA-систем. Проведено аналіз концепції SCADA-систем. Наведені їх переваги та недоліки, а також досліджено архітектури та компоненти SCADA-систем. Встановлено, що з урахуванням концепції Індустрії 4.0 та розвитком кіберфізичного виробництва, сучасні SCADA-системи представляють собою відкриті системи промислового Інтернету речей, а тому для забезпечення ефективного проєктування промислових багаторівневих систем керування необхідно використовувати новий підхід до кібербезпеки SCADA-систем, який пов'язаний з взаємозв'язком різних областей безпеки, враховуючи різні її аспекти. Набули подальшого розвитку промислові багаторівневі системи керування з використанням хмарних SCADA-систем.

Ключові слова: промислові багаторівневі системи керування, SCADA-системи, Інтернет речей, безпека SCADA-системи, архітектура та компоненти SCADA-систем.

FORKUN Y., FORKUN I.,
MAKARYSHKIN D., FENENKO V.
Khmelnitsky national university

CURRENT STATE OF PROBLEMS OF INDUSTRIAL MULTILEVEL CONTROL SYSTEMS BASED ON THE CONCEPT OF SCADA-SYSTEMS

Modern development of multilevel control systems is extremely important for the field of industrial automation. Industrial multilevel control systems include components such as control and data acquisition systems (SCADA), distributed control systems, and other control system configurations, such as programmable logic controllers in the industrial sector and critical infrastructure. At the same time, these components of multilevel control systems must meet the unique requirements of a complete integrated automation system, such as performance, reliability and safety. When designing multilevel control systems, it is necessary to take into account their types for a specific task of industrial automation and typical system topologies, identify typical threats and vulnerabilities of such systems and propose solutions and safety measures to reduce associated risks.

The industrial multilevel control system consists of a combination of the following controls, such as electrical, mechanical, hydraulic, pneumatic and other elements. The controls of industrial multi-level control systems work together to achieve industrial goals (eg, fabrication, transportation of materials or energy). A typical industrial multilevel control system may include multiple control cycles, human-machine interfaces (HMIs), and remote diagnostics and maintenance tools built using a number of network protocols. Industrial control processes apply to electricity, water and wastewater, oil and gas, chemicals, transportation, pharmaceuticals, pulp and paper, food and beverages, and discrete manufacturing (such as automobiles, aerospace, and durable goods). The actual implementation of industrial multi-level control systems can be a hybrid that blurs the boundaries between distributed systems and SCADA systems.

The article presents the current state of the problem of industrial multilevel control systems based on software and hardware SCADA-systems. The analysis of the concept of SCADA-systems is carried out. Their advantages and disadvantages are given, as well as the architectures and components of SCADA-systems are studied. It is established that taking into account the concept of Industry 4.0 and the development of cyberphysical production, modern SCADA-systems are open systems of industrial Internet of Things, and therefore to ensure effective design of industrial multilevel control systems it is necessary to use a new approach to cybersecurity SCADA-systems. the relationship of different areas of security, taking into account its various aspects. Industrial multilevel control systems using cloud SCADA systems have been further developed.

Key words: industrial multilevel control systems, SCADA-systems, Internet of Things, security of SCADA-systems, architecture and components of SCADA-systems.

Вступ. Сучасний розвитку багаторівневих систем керування є надзвичайно важливим для галузі промислової автоматизації. До складу промислових багаторівневих систем керування входять такі компоненти як системи керування та збору даних (SCADA), розподілені системи керування та інші конфігурації систем керування, такі як програмовані логічні контролери у промисловому секторі та критичній інфраструктурі. При цьому ці компоненти багаторівневих систем керування мають задовольняти унікальним вимогам цілої комплексної системи автоматизації, таким як, продуктивність, надійність та безпека. Під час проєктування багаторівневих систем керування необхідно враховувати їх типи для конкретної задачі промислової автоматизації та типових топологій системи, визначати типові загрози та вразливості таких систем та пропонувати рішення і рекомендаційні заходи безпеки для зменшення пов'язаних із ними ризиків [1, 2].

Промислова багаторівнева система керування складається з комбінації наступних елементів керування, таких як електричні, механічні, гідравлічні, пневматичні та інші елементи. Елементи керування промислових багаторівневих систем керування працюють разом для досягнення промислових цілей (наприклад, виготовлення, транспортування матеріалів або енергії). Типова промислова багаторівнева

система керування може включати безліч циклів керування, людино-машинні інтерфейси (HMI) та засоби віддаленої діагностики та обслуговування, побудовані з використанням ряду мережевих протоколів. Промислові процеси керування застосовуються для електроенергії, води та стічних водах, нафті та газі, хімічних речовинах, транспорті, фармацевтиці, целюлозі та папері, продуктах харчування та напоях та дискретному виробництві (таких як автомобілі, аерокосмічна промисловість та товари тривалого користування). Фактична реалізація промислових багаторівневих систем керування може бути гібридом, який стирає межі між системами розподіленим та SCADA-системами.

На основі інтеграції IT-можливостей в існуючі фізичні системи, що в свою чергу доповнює або замінює фізичне керування було розроблено багато сучасних промислових багаторівневих систем керування. Наприклад, вбудовані цифрові елементи керування замінили аналогові механічні елементи керування в обертових машинах та двигунах. Зростання вартості та продуктивності зумовило цей розвиток і призвело до багатьох сучасних «розумних» технологій, таких як розумні мережі, розумне транспортування, розумні будівлі та розумне виробництво. Однак незважаючи на те, що це збільшує зв'язок та важливість таких систем, це також ставить більш високі вимоги до їхньої пристосованості, стійкості та безпеки. Інженерна технологія промислових багаторівневих систем керування продовжує розвиватися, надаючи нові функції, зберігаючи типовий тривалий життєвий цикл цих систем. Впровадження IT-функцій у фізичні системи представляє нову поведінку, яка впливає на безпеку. У теперішній час розробляються інженерні моделі та аналіз для вирішення цих нових особливостей, включаючи взаємозалежність безпеки, конфіденційності та впливу на навколишнє середовище.

Аналіз останніх досліджень та публікацій. Основні операції та компоненти, які виконуються промисловими багаторівневими системами керування представлені на рисунку 1 [1]. Типова промислова багаторівнева система керування включає безліч циклів керування, людино-машині інтерфейси, засоби віддаленої діагностики та обслуговування, які побудовані з використанням масиву мережевих протоколів на багатошаровій архітектурі мережі. Шлейф керування використовує датчики, виконавчі механізми та контролери (наприклад програмований логічний контролер) для маніпулювання певними керуючими процесами. Датчик - це пристрій, який вимірює певні фізичні властивості, а потім надсилає цю інформацію контролеру як керовану змінну. Контролер інтерпретує сигнал відповідно до алгоритму керування і заданого значення цілі, генерує відповідну маніпульовану змінну і передає його на привід. Пускачі, такі як, регулюючі клапани, вимикачі, автоматичні вимикачі та двигуни використовуються для безпосереднього керування керованим процесом на основі команд контролера.

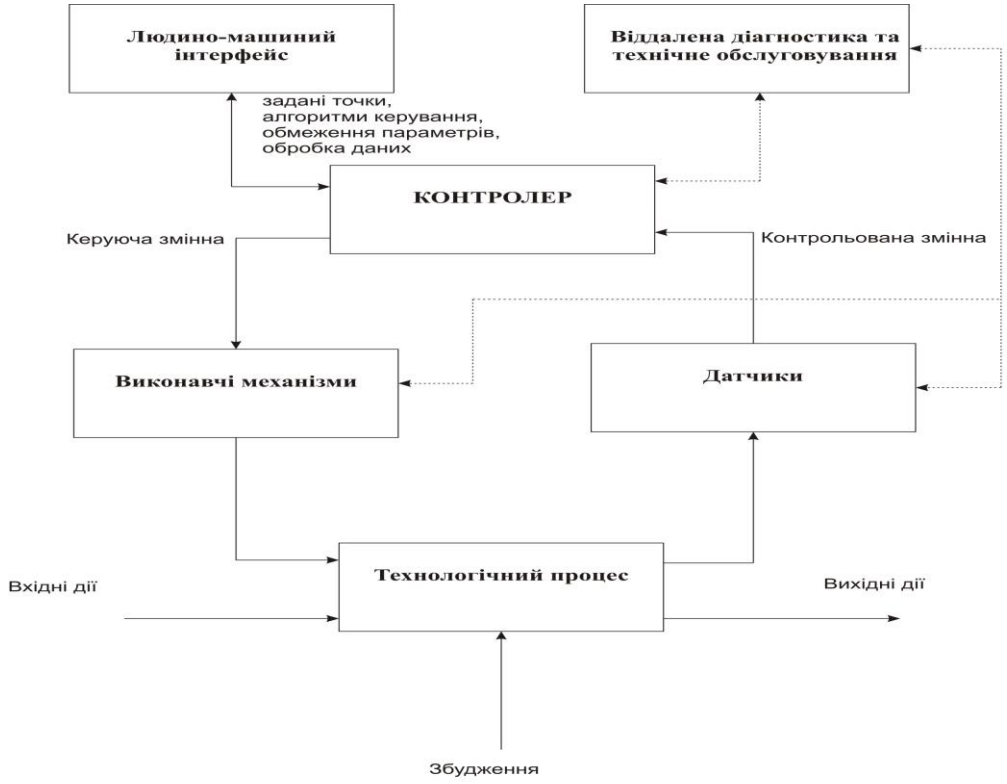

Рис. 1. Операції та компоненти промислових багаторівневих систем керування

Оператори та інженери використовують людино-машині інтерфейси для моніторингу та регулювання заданих значень, алгоритмів керування та налаштування параметрів в контролері. Людино-

машині інтерфейси також відображають інформацію про стан процесу та історичну інформацію. Службові програми діагностики та обслуговування використовуються для запобігання, виявлення та відновлення після ненормальних операцій або збоїв. Іноді ці цикли керування вкладені та/або каскадно – задана точка в одному циклі базується на змінній процесу, яка визначена іншим циклом. Цикл рівня керування та цикл низького рівня працюють безперервно протягом усього процесу, а час циклу становить мілісекунди до хвилин.

Під час проєктування промислової багаторівневої системи керування, є необхідним, визначення ключових факторів, що пов'язані з атрибутами керування, зв'язку, надійності та надмірності промислової багаторівневої системи керування. Оскільки ці фактори значною мірою впливають на розробку промислову багаторівневу систему керування, вони також допоможуть визначити вимоги до безпеки системи. Тому при проектуванні промислової багаторівневої системи керування враховуються наступні вимоги до: контролю часу, географічного розподілу, ієрархії, складності керування, доступності та надійності системи, впливу нестабільності і безпеки [1, 2].

На сьогодні критична інфраструктура зазвичай описується як інфраструктура, яка забезпечує та обслуговує основні послуги системи безпеки, економіки та охорони здоров'я будь-якої країни. Кіберфізична система та Інтернет речей доповнюють традиційну критичну інфраструктуру операціями з великими даними. Список галузей, що належать до критичної інфраструктури зазвичай включають у себе сільське господарство, охорону здоров'я, ядерні реактори, транспорт, енергетичний сектор, цивільна та хімічна інженерія, структура води, дослідження тощо, як представлено на рис. 2. Системи диспетчерського керування та обробка даних (SCADA-системи) при проєктуванні промислових багаторівневих систем керування відіграють ключову роль в управлінні та контролю критичної інфраструктури.

Система SCADA здійснює керування та моніторинг географічно розподілених активів. Історично склалося, що SCADA-системи були обмежені такими системами, як системами передачі енергії, транспортуванням природного газу та керування водою. Сучасний розвиток технологій привів до того, що SCADA-системи використовуються у таких промислових секторах, як металургія, хімічна обробка (переробка), телекомунікації, експериментальне та виробниче обладнання [2]. З розвитком концепції Індустрії 4.0 та промислового Інтернету Речей, сучасні SCADA-системи включають у себе такі компоненти, як CPS / IoT, хмарні технології, аналіз великих даних, штучний інтелект та машинне навчання. Інтеграція цих технологій значно покращує сумісність та спрощує обслуговування і зниження витрат на інфраструктуру.

Рис. 2. Сфера застосувань SCADA-систем

SCADA-системи можуть підвищити ефективність ключових промислових систем і забезпечити більш високу ефективність захисту обладнання. Дайте структуру SCADA. SCADA- системи розроблені для роботи в автономному режимі, а сама SCADA-система була захищена через мережу повітряного зазору та власний протокол. Ось чому оригінальний проєкт SCADA-система, ніколи не включала до свого складу функції безпеки [3, 4]. Однак в останні роки через розширення бізнесу та центральний попит на розподілений програмний моніторинг, система SCADA-система перетворилася на складну відкриту систему, яка є з'єднаною з Інтернетом за допомогою передових технологій. Однак це призвело до того, що система SCADA стала більш вразливою для цілей зловмисників з будь-якої точки світу [5].

Виклад основного матеріалу дослідження. Зазвичай SCADA – це комп'ютерна система, яка широко застосовується для дистанційного керування та моніторингу об'єкту керування. SCADA-система збирає інформація та дані про технологічні процеси, які аналізуються в режимі реального часу. SCADA-

система складається з таких елементів: головний термінал master terminal unit (MTU), комунікація, віддалений термінал remote terminal unit (RTU) та людино-машиний інтерфейс Human-machine-interface (HMI).

Апаратна архітектура SCADA використовує програмовані логічні контролери (PLC) та віддалені термінальні блоки (RTU). Архітектура програмного забезпечення SCADA включає людино-машиний інтерфейс (HMI), центральна база даних та інші користувачі програмне забезпечення [6]. ПЛК і RTU є мікрокомп'ютерами, які взаємодіють з масивом об'єктів, таких як промислові машини, HMI, датчики та кінцеві пристрої, а потім передають інформація від цих об'єктів до комп'ютерів із програмним забезпеченням SCADA. Програмне забезпечення SCADA обробляє, розповсюджує та відображає дані, допомагаючи операторам та іншим працівникам аналізувати дані та приймати важливі рішення. SCADA-системи здатні повідомляти оператора про проблему допомагає йому для її усунення та запобігання подальшій втраті продукту. Найбільший контроль дії виконуються RTU або PLC.

Апаратна система SCADA класифікується на дві основні частини: шари клієнта та сервер даних. Шар клієнта – це шар, який обслуговує людину і машинну взаємодію. Рівень сервера даних – це той, який обробляє більшу частину процесів даних. Програмовані логічні контролери є підключеними до серверів даних безпосередньо або через мережі або шини. SCADA-система використовує, як глобальну мережу (WAN) так, і локальну мережу (LAN), яка складається з Інтернет-протоколів, що використовуються для зв'язку між головною станцією та пристроями, фізичним обладнанням, датчиками, які є підключеними до ПЛК або RTU. RTU перетворює сигнали датчика в цифрові дані і передає цифрові дані MTU. Більшість операцій з моніторингу та контролю виконуються RTU або PLC.

Більшість серверів використовуються для багатозадачності та бази даних у режимі реального часу. Сервери здійснюють збір та обробку даних. SCADA-система складається з програмного забезпечення для забезпечення тенденцій, діагностики даних та керування такою інформацією, як запланований порядок технічного обслуговування, логістичної інформації, детальні схеми для конкретного датчика або машини та за усунення несправностей системи. Взаємозв'язок компонентів зв'язку системи MTU, RTU, HMI, Historian та SCADA є представлені на рис. 3.

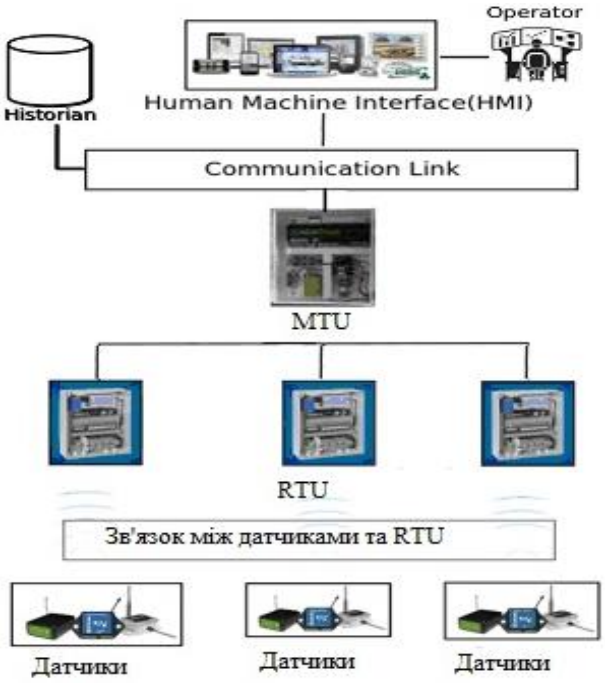

Рис. 3. Взаємозв'язок компонентів зв'язку SCADA-системи

Існують різні типи SCADA-систем, які розглядаються як архітектури SCADA чотирьох різних поколінь: монолітні або ранні системи SCADA (перше покоління); розподілені SCADA-системи (друге покоління); мережеві SCADA-системи (третє покоління); Інтернет речей.

Монолітні або ранні SCADA-системи були незалежними системами без зв'язку з іншими системами. Усі використані протоколи зв'язку були на той час власністю. Функції монолітні системи SCADA на початку першого покоління обмежується лише датчиками моніторингу в системі та позначенням будь-яких операцій у разі перевищення запрограмованих рівнів тривоги. У таких SCADA-системах резервування було досягнуто за допомогою резервної системи мейнфреймів, підключеної до всіх сайтів RTU, і використовувалася лише у випадку виходу з ладу первинної системи мейнфреймів, у цій архітектурі RTU зв'язується з MTU з використанням глобальних мереж (WAN), як показано на рис. 4 [7].

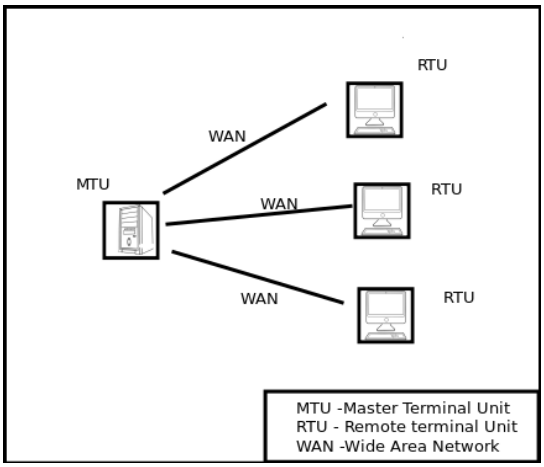

Рис. 4. Мережева архітектура монолітної SCADA-систем

Розподілені SCADA-системи (керування), архітектура, якої представлена на рис. 5, мають спільний доступ до функцій керування розподілений між декількома системами, які підключені один з одним за допомогою локальної мережі LAN [8]. При цьому кожна станція використовувалася для обміну інформацією в режимі реального часу між системами та її обробки для виконання контрольних завдань для спрацювання сигналізації, пр. певних рівнях можливих проблем, тим самим зменшуючи витрати у порівняні з попереднім поколінням SCADA-систем. Мережеві протоколи все ще не стандартизовані в розподілених SCADA-системах, а безпека установки SCADA-систем ігнорується.

У третьому поколінні SCADA-система може бути зведена до найпростішої компоненти, яка утворюються шляхом з'єднання його за допомогою протоколів зв'язку. У SCADA-системах цього типу, мережа може бути географічно розподілена та зв’язуватися за допомогою глобальної мережі WAN через лінії передачі даних або мобільний зв’язок. Такий тип SCADA-систем використовує Ethernet або оптично волоконний з’єднувач для постійної передачі даних між вузлами. Архітектура мережевих SCADA-систем представлена на рис. 6.

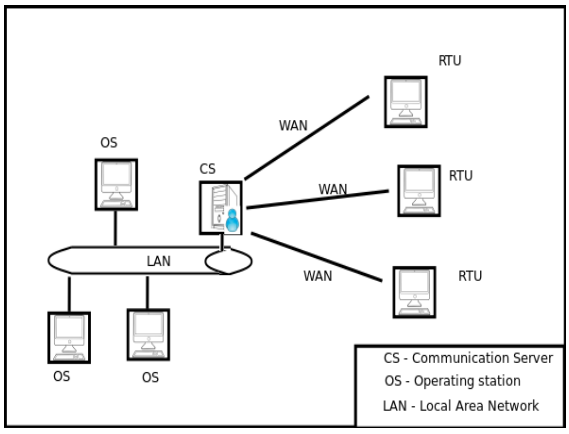

Рис. 5. Мережева архітектура розподіленої SCADA-системи

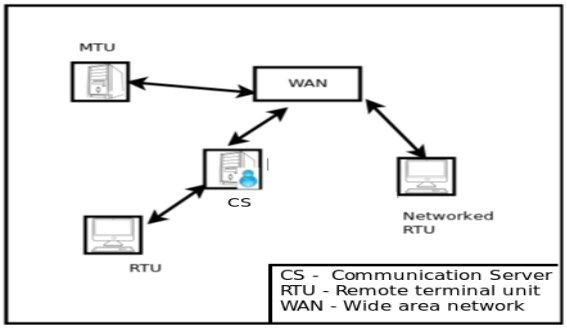

Рис. 6. Мережева SCADA-система

У четвертому поколінні SCADA-систем, за рахунок впровадження Інтернет-технологій (веб-технологій) з'являється можливість користувачам переглядати дані, обмінюватися інформацією та керувати процесами з будь-якої точки світу. Вартість інфраструктури та розгортання SCADA-систем зменшуються шляхом інтеграції технологій Інтернету речей з комерційно доступними хмарними обчисленнями. Технічне обслуговування та інтеграція з попередніми SCADA-системи є більш простим. Це мережа пристроїв зі значним зосередженням на передачі, контролі критичної інформації, отриманні статистичних даних з big data, тому для створення промислового Інтернету речей є необхідними інтегрувати зовнішні системи з існуючими на той момент SCADA-системами, серверними пристроями, протоколами і т.д. [7]. Архітектура четвертого покоління представлена на рис. 7.

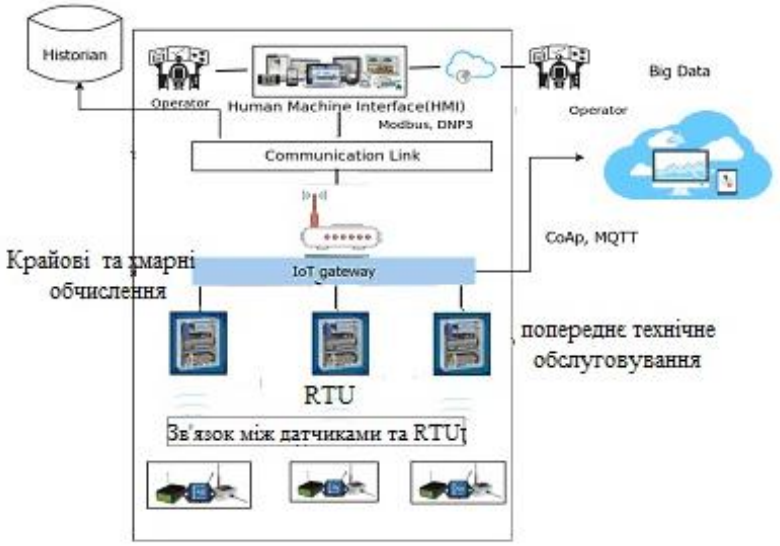

Рис. 7. Мережева архітектура Інтернету речей-четверте покоління SCADA-систем

SCADA-системи четвертого покоління здатні звітувати про стан об'єкту керування у реальному масштабі часу, при цьому використовуючи горизонтальну шкалу з хмарних обчислень. За рахунок цього можуть бути реалізовані більш складні алгоритми керування, для реалізації яких є достатніми традиційні програмовані логічні контролери. Концепція Індустрія 4.0 – це приклад четвертого покоління SCADA-системи, в яких є розподіленими когнітивні обчислення, CPS, Інтерент-речей та хмарні обчислення, які використовуються для керування дії [9].

При проектуванні промислових багаторівневих систем керування різної складності використовується концепція SCADA-систем. Ці системи можуть варіюватися від десятків до тисяч контурів керування в залежності від програми. SCADA-системи використовуються для моніторингу різноманітних даних, таких як потоки, струми, напруги, тиск, температури, рівні води та тощо, в різних галузях промисловості. У виробничих галузях SCADA-системи [8] використовуються для керування виробництвом системи для досягнення цілей продуктивності, перевіряючи кількість вироблених одиниць та підрахунок завершених етапів операцій з температурами на різних стадіях виробничого процесу.

SCADA-системи використовуються для очищення промислових стічних вод. Очисні споруди для обробки поверхневих вод бувають різного типу. Однак, це в основному системи очищення води, в яких багаторівнева система керування, процеси автоматизації та розподілені системи беруть участь в обробці води. Вирішуючи такі задачі, SCADA-системи використовуються для керування автоматичними роботами, обладнанням користувача та зворотнім промиванням фільтрів на основі годин роботи або кількості потоку води, яка проходить через фільтри. Рівні резервуару для води, тиск системи, температуру рослин, седиментація, фільтрація, хімічна обробка та інші параметри або процеси контролюються за допомогою програмно-технічних комплексів SCADA-систем, програмованих логічних контролерів, робочих станцій на базі комп'ютерної техніки, які зв'язані між собою за допомогою локальної мережі LAN, використовуючи наприклад технологію Ethernet. SCADA-системи застосовуються в телекомунікаційних та IT-системах для керування різними радіочастотними системами, засобами та системами зв'язку [10]. Наприклад, реєстрацію даних через антені системи, можна легко здійснити за допомогою SCADA-систем.

SCADA-система може використовуватися разом із програмним забезпеченням MATLAB для керування об'єктами. SCADAMATLAB представляє собою платформу, яка з'єднує звичайну SCADA-систему з програмним забезпеченням MATLAB для досягнення надійності та ефективності керування, при необхідності обробки складних алгоритмів керування.

Віддалені місця розташування та власні промислові мережі використовуються для того, щоб надати SCADA-системам значний ступінь захисту через ізоляцію. Зараз більшість промислових підприємств використовують мережеві сервери історичних процесів для зберігання даних про процеси та інші можливі інтерфейси бізнесу та процесів. Прийняття Ethernet та протоколу керування передачею/Інтернет-протоколу TCP/IP для мереж керування процесами та бездротових технологій, таких як IEEE 802.x та Bluetooth, ще більше зменшило ізоляцію мереж SCADA-систем. Зв'язок та деізоляція SCADA-системи представлено на рис. 8.

Рис. 8. Типові компоненти SCADA-систем

Кіберфізична безпека неперервних систем у режимі реального часу вимагає всебічного уявлення та цілісного розуміння мережевої безпеки, теорії управління та фізичної системи. Зрештою, будь-які життєздатні технічні рішення та напрямки досліджень щодо забезпечення систем SCADA-систем повинні бути у поєднанні з комп'ютерною безпекою, мережею зв'язку та керування. Ідея розглянути проблему в контексті ефективності керуванні має міцні напрямки. Однак дуже велика встановлена база таких систем означає, що в багатьох випадках ми повинні довгий час покладатися на реконструйовані механізми безпеки, а не мати можливість проектувати їх з нуля. Це призводить до нагальної потреби надійних SCADA-систем у виявленні вторгнень (IDS) та еластичному керуванні.

Такі міжнародні інститути, як IEEE, CPNI, AGA, ISA, NERC, NIST публікують рекомендації щодо безпечного використання SCADA-систем [11]. На рис. 9 представлено взаємозв'язок між різними областями безпеки SCADA-системи, такими як архітектура самої системи, вразливості, атаки, виявлення вторгнень та випробувальних стендів. На сьогодні, наукові праці у цьому напрямку, досліджують лише один аспект безпеки SCADA-системи, а отже недоліком є, те що, вони не розглядають взаємозв'язок між різними областями безпеки SCADA-систем, що є дуже значним при створені механізмів безпеки для складних систем промислового Інтернет речей. Таким чином, актуальною задачею, є огляд який враховує різні аспекти безпеки SCADA-систем.

Рис. 9. Взаємозв'язок між різними областями безпеки SCADA-системи

Пропонується використовувати запропоновану у роботі [12] таксономію для вивчення аспекту архітектури та безпеки SCADA-систем, що є необхідним враховувати при проектуванні промислових багаторівневих систем керування. Така таксономія представлена на рис. 10.

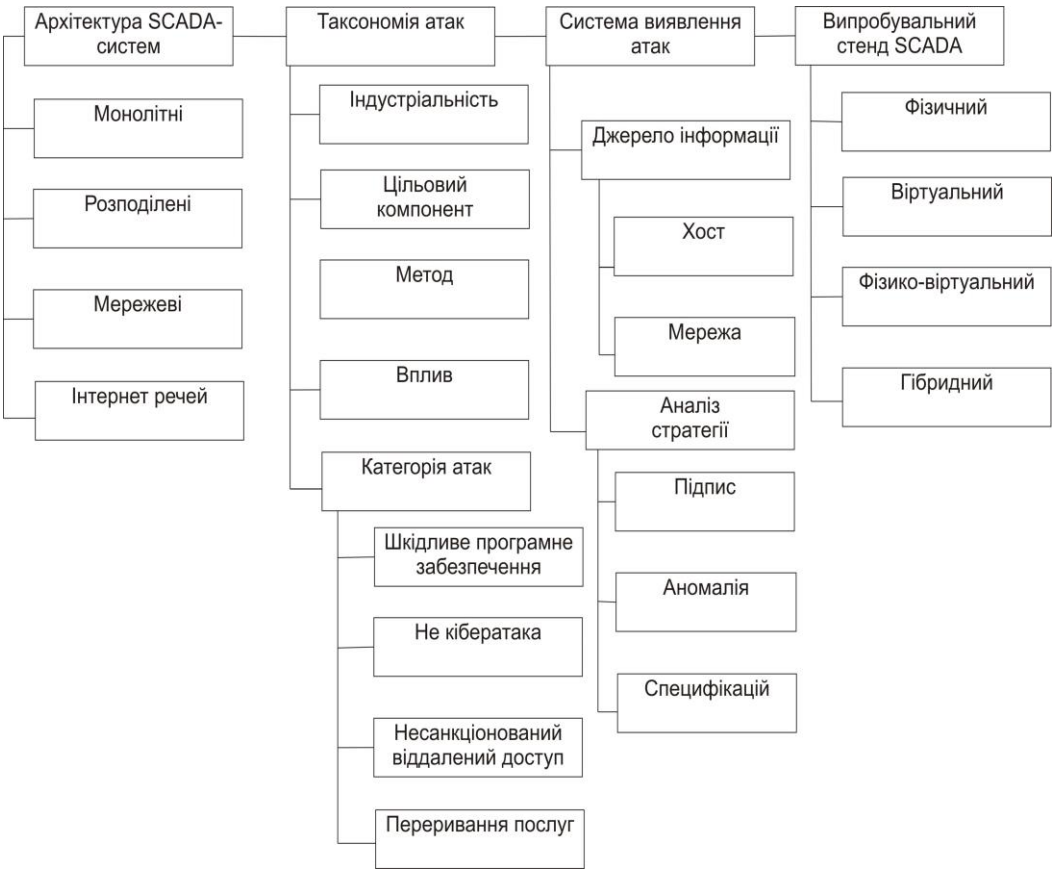

Рис. 10. Взаємозв'язок між різними областями безпеки SCADA-системи

Сучасний стан наукових досліджень, показує, що навіть із вдосконаленим алгоритмом безпеки було виявлено багато атак на SCADA-системи, а це підкреслює майбутній обсяг досліджень, що має зменшити розрив між сучасним станом SCADA-систем та передовими і надійними SCADA-системи для проектування промислових багаторівневих систем керування. Тому при проектуванні промислових багаторівневих систем керування є необхідним враховувати:

1. Бази даних атак: база даних інцидентів безпеки необхідна для аналізу різних вимірів атак для розробки стратегій запобігання подібним атакам у майбутньому. Набори даних KDD99, NSS-KDD, DARPA застарілі і не синхронізовані з сучасною архітектурою SCADA-системи. Набір даних NVD містить загальні вразливості у всіх доменах, які не фокусуються на специфічних вразливостях SCADA-систем. З 2015 року немає оновлення до бази даних RISI. Тому немає належної бази даних, яка охоплювала б всю безпеку інцидентів. Слід створити одне глобальне сховище для всіх цих інцидентів. Це сховище має бути загальнодоступним, доступні дослідникам для аналізу цих атак. Тоді можна обробляти лише атаки нульового дня.

2. Масштабовані тестові стенди та методи перевірки: на основі аналізу огляду існуючих джерел тестових стендів, можна зробити висновок, що як для фізичних, так і віртуальних тестових стендів, було досліджено програмне забезпечення та гібридний тест. Розробка випробувального стенду – це дорогий процес, який потребує величезного обсягу фінансування. Не існує такого випробувального стенду, який був би економічно вигідним, масштабованим і мав високі показники ефективності. Дослідник повинен зосередитись на масштабованості, вищому ступені ефективності, економічності та інтерполяції. Необхідними є нові протоколи зв'язку, нові методи оцінки ризику, а також перевіряти IDS. Існує нагальна вимога щодо достовірної перевірки, підходи до оцінки надійності нових методів безпеки та безпеки SCADA-систем [13].

3. IDS для SCADA-систем: у роботі [14] запропоновані дослідження для визначення показників продуктивності перевірки IDS. У більшості аналізів враховуються лише показники виявлення атак, такі, як хибнопозитивні та хибнонегативні. Час, необхідний для виявлення нападу, є важливим стандартом для вимірювання продуктивності. Отже, навіть якщо гарантовано, що IDS виявлять атаку, а затримка велика, зловмисник матиме достатньо часу, щоб пошкодити систему. Дослідницька робота зосереджена на розробці

системи виявлення для конкретних типів атак, тобто маршрутизації та атаки DOS. Різні атаки схеми виявлення, які працюють за подібних робочих параметрів, мають бути оцінені в подальших дослідженнях і при проектуванні промислових багаторівневих систем керування. Проведено значну роботу в галузі знань, що базується на IDS. Однак ці системи все ще не здатні до обробки атак нульового дня. Визначити прийнятну поведінку при зміні середовища є складним завданням. Засновані на знаннях IDS не є надійними для невідомих атак. Поведінка кожної атаки відрізняється від інших, тому дослідник повинен зосередитись на виявленні моделі нападу. Тому дослідникам слід розробляти підходи для подальшого вдосконалення порогових методів моніторингу. У роботі [15] запропонована модель для динамічного формування правил для виявлення вторгнень у SCADA-системи. Ця порогова модель повинна бути динамічною, яка розпізнає за ступенем тяжкості минулих нападів.

4. Новий комунікаційний протокол: у комунікаційних протоколах основна увага приділяється додатку та захисту мережевого рівня. Протоколи мережевої безпеки повинні бути інтегровані в ці протоколи зв'язку. Протокол зв'язку для SCADA-систем на базі IoT-хмари, тобто надійний, безпечний, масштабований, відкритий, низька затримка протоколу зв'язку – це новий напрямок для дослідника. З концепцією Індустрії 4.0 протоколи IoT використовуються в SCADA-системах. Недоліком таких протоколів є надійність, що викликає потребу в надійному зв'язку. У випадку SCADA-систем, мережевих криптографічних рішень недостатньо для блокування атак. Тому актуальною проблемою є потреба у дослідженнях для більш надійних криптографічних рішень, методів аутентифікації, що входять до протоколу, механізми безпеки, які застосовуються до SCADA-систем.

5. Безпечна архітектура та операційна система: операційні системи DOS, VMS та UNIX, які мають різні уразливості, в основному використовувались у SCADA-системах. На сьогоднішній день працює операційна система Linux та MicrosoftWindows системи витіснили DOS із SCADA-систем на основі UNIX. Однак Linux і Windows страждають від своїх вразливостей, через великий вихідний код для операційних систем. Операційна система заснована на архітектурі мікроядра системи може бути використана для зменшення поверхні атаки для SCADA-систем. Окрім безпеки, безпеки рекомендацій завжди слід дотримуватися в максимальній мірі, щоб уникнути прийнятних ризиків. SCADA-системи можна захистити, використовуючи більш стійку до помилок архітектуру, безпечну та надійну операційну систему і використання захищених мов програмування. Безпека операційної системи є важливою проблемою. Протоколи безпеки повинні бути обов'язковими.

6. Фокус досліджень для IoT-Cloud SCADA-систем: у роботі [16] запропоновано декілька дослідницьких пропозицій щодо безпечного IoT-cloud SCADA-систем. Інтеграція IoT-хмари в традиційну SCADA-систему відкриває нові загрози та можливості обміну даними / інформацією / послугами через Інтернет. Існує гостра необхідність вирощувати нові стратегії, придатні для керування складними та масштабними структурами. Дослідження повинні бути зосереджені на постійну безпеку цих систем. У системі хмарних технологій IoT перевантаження смуги пропускання – це велика проблема. Ці параметри залежать від постачальників хмарних послуг. Затримка з прийняттям рішень може призвести до втрати виробництва. Тож дослідження слід зосередити, щоб зробити цю систему надійною та ефективною. Слід використовувати велику пропускну здатність та низьку затримку. Потенціал цих систем залежить від взаємозв'язку відповідальних платформ. У системі, що базується на Інтернеті речей, величезна кількість даних генерується. Отже, безпека, аналітика, зберігання та складність цих даних є головною проблемою.

Висновки. Встановлено, що для проєктування сучасних промислових багаторівневих систем керування використовуються програмно-технічні комплекси SCADA-системи, що представляють собою централізовані системи для моніторингу та керування всього технологічного процесу за допомогою програмного-апаратних компонентів. У сучасних промислових багаторівневих систем керування SCADA-системи проводять збір даних з віддаленого місця за допомогою датчиків та відправляють команди для керування технологічним процесом до програмованого логічного контролеру або людино-машинного інтерфейсу. Основна перевага SCADA-систем полягає, у тому, що вони конструктивно реалізовуються у різних галузях, а це в свою чергу призводить до зменшення людських зусиль та підвищення точності вимірювання, моніторингу та контролю даних об'єкта керування в режимі реального часу і з будь-якої точки світу.

Сучасні SCADA-системи четвертого покоління представляють собою складні відкриті системи, які є підключеними до Інтернету. Такий підхід робить SCADA-системи, вразливими для різних зловмисників, які здійснюють напади на системи промислових багаторівневих систем керування. Безперебійна та ефективна робота SCADA-систем є однією з актуальних та найважливіших проблем для сучасного виробництва, оскільки наслідки виходу з ладу сучасної промислової багаторівневої системи керування можуть варіюватися від фінансової катастрофи до природного збитку та втрати людського життя.

Для забезпечення ефективного проєктування промислових багаторівневих систем керування необхідно використовувати новий підхід до безпеки SCADA-систем, який поєднує різні аспекти безпеки, комплексний аналіз бази даних атак RISI, систем виявлення вторгнень та тестових стендів SCADA-систем, а також необхідно враховувати, те що, IoTization та хмарні SCADA-системи, розширили спектр проблем дослідження безпеки промислових багаторівневих систем керування.

На сьогодні підходи проектування промислових багаторівневих систем керування переходять до хмарних SCADA-систем. Переваги хмарних SCADA-систем є їх економічність, простота та масштабованість. Однак, незважаючи на ці переваги хмарні SCADA-системи мають ряд недоліків, такі як продуктивність, висока затримка та низька пропускна здатність, що призводить до погіршення ефективності промислових багаторівневих системах керування, тому існує актуальна потреба у розробці ефективних системних архітектур і систем для моделювання таких проблем.

References

1. Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) / [K. Stouffer, V. Pillitteri, S. Lightman and other]. – Gaithersburg: National Institute of Standards and Technology Special Publication 800-82, Revision 2 Natl. Inst. Stand. Technol. Spec. Publ. 800-82, 2015. – 247 c.

2. Nasr P. M. An alarm based access control model for scada system / P. M. Nasr, A. Y. Varjani // Smart Grid Conference (SGC 2015), 2015. – p. 23–24.

3. Rezai A. Key management issue in scada networks: A review / A. Rezai, P. Keshavarzi, Z. Moravej // Engineering Science and Technology, an International Journal, 20(August). - 2016. – p.354–363.

4. Papa S. Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis. / S. Papa, W.Casper, T. Moore // International Journal of Critical Infrastructure Protection. - 013p. 96 – 106.

5. Miller B. A survey scada of and critical infrastructure incidents / B. Miller, D. Rowe. // In Proceedings of the 1st

6. Annual Conference on Research in Information Technology, RIIT '12 - New York: NY, USA, 2012.- p. 51–56.

7. The scada review: System components, architecture, protocols and future security trends / A.Shahzad, S. Musa, A. Aborujilah, M. Irfan. // American Journal of Applied Sciences. – 2014. – №11. – p.1418–1425.

8. Yadav G. Architecture and Security of Scada System: A Review / G. Yadav, K. Paul // arXiv:2001.02925v1 [cs.CR]. - 2020.

9. https://www.watelectronics.com/scada-systemarchitecture-types-applications.

10. Industry 4.0: the fourth industrial revolution –guide to industrie 4.0. / [Y. Yang, K. McLaughlin, S. Sezer and other]. // Multiattribute scadaspecific. – 2017.

11. https://instrumentationtools.com/applications-of-scada/.

12. Sommestad T. Scada system cyber security x2014; a comparison of standards. / T. Sommestad, G. Ericsson, J. Nordlander // Power and Energy Society General Meetingю - 2010 IEEE, 2010. - p.1–8.

13. Papa S. Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis. / S. Papa, W. Casper, T. Moore. // International Journal of Critical Infrastructure Protection.- 2013. - №6. – p. 96 – 106.

14. Lyu X. Safety and security risk assessment in cyber-physical systems. / X. Lyu. // IET Cyber-Physical Systems: Theory & Applications. - 2019. - №4. – p.221–232.

15. Mitchell R. A survey of intrusion detection techniques for cyber-physical systems / R. Mitchell, I. Chen // ACM Comput. Surv.- 2014. -№46. p. 1–29.

16. Zhu B. Scada-specific intrusion detection/prevention systems: A survey and taxonomy / B. Zhu, S. Sastry. - 2010.

17. Sajid A. Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges / A. Sajid, H. Abbas, K. Saleem. // IEEE SPECIAL SECTION ON THE PLETHORA OF RESEARCH IN NTERNET OF THINGS (IoT). - 2016. – №4.

Надійшла / Paper received: 05.10.2020 Надрукована / Paper Printed : 01.12.2020