УДК 681.518.5
DOI https://doi.org/10.32782/IT/2021-2-5

Олена СИРОТКІНА
кандидат технічних наук, доцент кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49000
***ORCID:** 0000-0002-4069-6984*

Павло ІЩУК
асистент кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49000, yshchuk.p.o@nmu.one
***ORCID:** 0000-0001-6399-6771*

Ярослав ЖУРАВЛЬОВ
студент спеціальності 121 «Інженерія програмного забезпечення» другого (магістерського) рівня вищої освіти, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49000

Бібліографічний опис статті: Сироткіна, О., Іщук, П., Журавльов, Я. (2021). Діагностика працездатності сервера розподіленої SCADA системи. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2, 34–41, doi: https://doi.org/10.32782/IT/2021-2-5

ДІАГНОСТИКА ПРАЦЕЗДАТНОСТІ СЕРВЕРА РОЗПОДІЛЕНОЇ SCADA СИСТЕМИ

В даний час існує актуальне завдання створення автоматичних необслуговуваних автоматизованих систем та апаратно-програмних комплексів відповідального призначення. У зв'язку з цим, доцільним є завдання діагностики працездатності таких систем із можливістю їх подальшого самовідновлення. Отже, такі системи повинні працювати в цілодобовому режимі реального часу без участі експлуатаційного персоналу. ***Метою*** *статті є створення та застосування методів автоматичної діагностики та автовідновлення після оборотних відмов сервера, що працює в складі апаратно-програмного комплексу розподіленої SCADA системи для підвищення надійності та відмовостійкості роботи SCADA. Проведено огляд сучасних методологій, що застосовуються при вирішенні завдань даного класу. Розглянуто основні причини виникнення несправностей в розподіленої SCADA системі на стадії промислової експлуатації. Наведена діаграма основних станів системоутворюючого вузла сервера SCADA, де кожному з станів відповідають свої характерні види відмов. Для опису взаємодії структурних компонентів серверного вузла SCADA застосована методологія моделювання з використанням Unified Modeling Language. Наведено модель одного з сценаріїв зміни станів системоутворюючого вузла сервера SCADA в часі. У сценарії наведені методи профілактики відмов системи в зв'язку зі зникненням напруги живлення в електромережі, а також методи автовідновлення після оборотних відмов, що працюють навіть при відмові призначеного для користувача інтерфейсу.* ***Наукова новизна*** *запропонованого методу автоматичної діагностики сервера SCADA полягає в формуванні критеріїв та функціональних залежностей виявлення та розмежування оборотних і необоротних відмов. Як* ***висновок****, результатом розробки методів профілактики та автовідновлення працездатності системи після відмов є істотне підвищення її надійності та відмовостійкості в процесі промислової експлуатації, що особливо істотно для об'єктів відповідального призначення та підвищеної небезпеки.*

Ключові слова: *SCADA система, діагностика відмов, рівні ієрархії ПЗ SCADA, діаграма взаємодії структурних компонентів, методи автовідновлення працездатності SCADA.*

Olena SYROTKINA
Ph.D in Mathematical Modeling and Computational Methods, Associate Professor at the Department of Software Engineering, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49000
***ORCID:** 0000-0002-4069-6984*

Pavlo ISHCHUK
Assistant lecturer at the Department of Software Engineering, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49000, yshchuk.p.o@nmu.one
***ORCID:** 0000-0002-4069-6984*

Yaroslav ZHURAVLOV
Student of specialty 121 "Software Engineering" of the second (master's) level of higher education, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005

To cite this article: Syrotkina, O., Ishchuk, P., Zhuravlov, Ya. (2021). Diahnostyka pratsezdatnosti servera rozpodilenoi SCADA systemy [Server Diagnostic Performance of the Distributed SCADA]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 2, 34–41, doi: https://doi.org/10.32782/IT/2021-2-5

SERVER DIAGNOSTIC PERFORMANCE OF THE DISTRIBUTED SCADA

At the present time, the primary task is to create automatic, maintenance-free systems as well as hardware and software systems. In this regard, it is advisable to diagnose the efficiency of such systems with the possibility of their further self-recovery. Therefore, such systems should function 24/7 in real-time without the involvement of personnel to operate them. ***The aim*** *of the article is to create and apply methods for automatic diagnostics and auto-recovery after reversible server failures. The server works as part of the hardware and software complex of the distributed SCADA system. This will increase SCADA reliability and fault tolerance. We conducted a review of modern methodologies used in solving problems of this class. This paper considers the main causes of malfunctions in the distributed SCADA system at the stage of industrial operation. The diagram of the main states of the SCADA server backbone node is given, where each of the states corresponds to its characteristic types of failures. We applied the modeling methodology using the Unified Modeling Language to describe the interaction of the structural components of the SCADA server node. This resulted in the creation of the model for one of the scenarios of state changes in the SCADA server backbone node in real-time. The scenario provides methods for preventing system failures due to power outages, as well as methods of auto-recovery after reversible failures which work even if the user interface fails.* ***The scientific novelty*** *of the proposed method of automatic diagnostics of the SCADA server is in the formation of criteria and functional dependencies for the detection and differentiation of reversible and irreversible failures. In* ***conclusion****, the result of the method development for prevention and self-recovery of the system after failures lies in a significant increase of its reliability and fault tolerance in the process of industrial operation. This is especially important for critical objects and increased danger.*

Key words*: SCADA system, failure diagnostics, levels of SCADA software hierarchy, diagram of interaction between structural components, methods of auto-recovery of SCADA performance.*

Актуальність проблеми. В даний час в усьому світі відбувається розвиток нових технологій в різних областях промислового виробництва, енергетики, військовій сфері. Контроль і оперативне диспетчерське управління в галузі промислової автоматизації забезпечують сучасні SCADA (Supervisory Control and Data Acquisition) системи відповідального призначення, які отримують все більш широке розповсюдження [1–5]. Галузі застосування SCADA систем зумовлюють підвищені вимоги до надійності їх роботи, безпеки використання, живучості та відмовостійкості в процесі експлуатації на об'єктах відповідального призначення. Дана проблема стає все більш значущою в процесі вдосконалення та ускладнення самих SCADA систем – розподілених багаторівневих і багатозадачних апаратно-програмних комплексів (АПК), які працюють в режимі реального часу. На сьогодні практично всі застосовувані SCADA системи вимагають для експлуатації та обслуговування постійної цілодобової присутності висококваліфікованого персоналу на об'єктах експлуатації. Таким чином, актуальною є задача створення методики автоматичної самодіагностики працездатності SCADA з можливістю автовідновлення роботи системи після оборотних відмов.

Аналіз останніх публікацій показав основні напрями досліджень в цій галузі.

В роботі [1] представлена системна інформація для аналізу поведінки спеціалізованих процесів з метою діагностики та налагодження підсистем SCADA, включаючи основне обладнання,

програмне забезпечення та системи зв'язку, які з'єднують системоутворюючі вузли та автоматизовані робочі місця операторів SCADA.

Робота [2] присвячена питанню автоматизації завдань, пов'язаних з моніторингом конкретних виробничих процесів, зі зменшенням складової диспетчерського управління, а також координацією операцій з технічного обслуговування. Це надає програмованим логічним контролерам (ПЛК) можливість приймати рішення та виконувати дії, виходячи тільки з інформації, що надається ПЛК іншими системоутворюючими вузлами. Таким чином, технологія SCADA модернізується та виходить на новий рівень управління виробничими процесами, а також бізнес-операціями зі збільшенням складової автоматичної діагностики працездатності та відновлення системи. Це дозволяє підвищити швидкість, ефективність і якість виробничих процесів.

У статті [3] представлена інтегрована система управління розподілом ресурсів (Integrated Distribution Management System – IDMS). Вона забезпечує структуру інтеграції, що легко настроюється і в даний час включає в себе один інструментальний засіб підтримки прийняття рішень – компонент діагностики. Цей компонент діагностики називається сервером управління відновленням після збою (Outage Restoration Management Server – ORMS). Він інтегрований з іншими інформаційними системами через гнучку розширювану структуру інтеграції (Integration Framework – IF), що заснована на технології інтегрованих обчислювальних моделей (Model Integrated Computing Technology – MIC), яка розроблена в Інституті програмних інтегрованих систем (The Institute for Software Integrated Systems – ISIS). Структура IF була розроблена таким чином, щоб можна було легко підтримувати інтеграцію між інструментальними засобами підтримки прийняття рішень та інформаційною системою промислового підприємства, а також можна було б швидко і недорого створити та інтегрувати в IDMS додаткові інструментарії підтримки прийняття рішень. Структура IF на базі MIC надає гнучку і розширювану інтеграційну платформу, на якій можна побудувати набір інструментаріїв підтримки прийняття рішень. Такий підхід сприяє підвищенню ефективності та результативності роботи технологічних процесів промислових підприємств.

У статті [4] описується еталонна архітектура для розробки та впровадження програмних додатків, що виконують віддалену діагностику та прогнозування роботи інформаційних систем. Еталонна архітектура включає нові стандартні серверні технології на рівні додатків, щоб гарантувати переносимість між широким спектром серверних платформ і сприяти повторному використанню основних компонентів додатка в різних доменах кінцевих користувачів. Основні програми включають додаток для управління діагностикою в реальному часі, набір інструментарію для діагностичного аналізу, а також середу аналізу і розробки для створення діагностичних / прогностичних додатків. Набір інструментарію для діагностичного аналізу використовує компоненти додатків на основі Java в рамках загальної структури, що дозволяє гнучку інтеграцію різноманітних поєднань методів міркувань та методів, що засновані на правилах, в діагностичні та прогностичні додатки. Ці ж компоненти також використовуються в серверній середовищі реального часу для виконання діагностичних і прогностичних стратегій.

В роботі [5] описана методика, яка використовує багаторівневу архітектуру відкритих мережевих сервісів (Open Grid Services Architecture – OGSA) для побудови експертної системи діагностики несправностей (Grid-based Fault Diagnosis Expert System – GFDES). На основі ряду моделей були розроблені програми суспільного телебачення та паралельного сервісу для сервера. Спроєктована архітектура мережі даних (Data Grid Market-based Architecture – DGMA) представлена незалежними розподіленими вузлами мережі, що відповідають експертній системі діагностики несправностей.

Метою досліджень є підвищення надійності та відмовостійкості роботи сервера розподіленої SCADA системи шляхом розробки методики діагностики його працездатності з можливістю автовідновлення після оборотних відмов.

Виклад основного матеріалу. Розглянемо основні причини виникнення несправностей в АПК розподіленої SCADA системи, що знаходиться на стадії промислової експлуатації, які призводять до часткової або повної втрати її працездатності. До них відносяться:

– несправності апаратних засобів, що виникають у разі відсутності прогнозування їх старіння, зносу та, як наслідок, вихід з ладу. При цьому, таких несправностей вузлів системи можна було б уникнути в разі проведення своєчасної та якісної діагностики всіх вузлів SCADA системи в процесі її експлуатації;

– несанкціоноване втручання або навмисно шкідливий вплив на системоутворюючі вузли або мережеві комунікації SCADA системи, з метою отримання доступу до даних або

з метою спотворення даних і / або зміни будь-яких функцій системи;

– фізичне пошкодження електронного обладнання системи, каналів зв'язку та каналоутворюючої апаратури, що виникає внаслідок впливу будь-яких зовнішніх факторів, перенапруги з боку мережі живлення, грозової активності, пошкодження заземлення та ін.

– оборотні апаратні збої, що не призводять до виходу з ладу обладнання, однак викликають збій та повну, або часткову відмову програмних засобів SCADA системи, що, в свою чергу, призводить до втрати функціональності будь-яких окремих її вузлів, або ж всієї системи;

– помилкові дії експлуатаційного персоналу підприємства.

Крім того, в процесі експлуатації SCADA системи, топологія, структура та функціональність генеруємої run-time SCADA постійно зазнає змін відповідно до змін, що відбуваються на об'єкті впровадження. В тому числі, зміни зазнає парк використовуваного в складі SCADA системи працездатного обладнання, середовище передачі даних, модифікується ПЗ в зв'язку з модернізацією обладнання, резервуванням, ремонтними або профілактичними заходами. Також додаються нові об'єкти контролю, змінюється набори параметрів, що контролюються, тривог, види звітних форм SCADA системи та ін.

Таким чином можна стверджувати, що SCADA система, як розподілений багаторівневий та багатозадачний АПК, що працює в режимі реального часу – складний, динамічний об'єкт діагностики зі змінною структурою та функціональністю в процесі періоду експлуатації. Надійність роботи SCADA системи, достовірність даних на всіх рівнях ієрархії залежить від працездатності системоутворюючих вузлів, каналів передачі даних, периферійного обладнання та узгодженості роботи програмного забезпечення системи в цілому.

На рис. 1 приведена діаграма рівнів ієрархії (PI) середовища розробки та виконання SCADA системи.

На кожному системоутворюючому вузлі SCADA присутній деякий набір з наведених на діаграмі PI (див. Рис. 1). Найбільш повний набір PI мають сервера SCADA системи.

На рис. 2 приведена діаграма станів системоутворюючого вузла сервера SCADA.

Run-time сервера SCADA – це набір виконуваних процесів, кожен з яких проходить через три стани: початкова ініціалізація, основний алгоритм, завершення. У багатьох процесах основний алгоритм являє собою нескінченний цикл очікування команди на обслуговування,

Рис. 1. Діаграма рівнів ієрархії середовища розробки та виконання SCADA системи

що отримується через призначений для користувача інтерфейс або від іншого процесу. Такі процеси завершуються штатно, тільки отримавши сигнал на завершення роботи.

У складі згенерованого run-time сервера SCADA присутні як резидентні програми, що працюють у real-time 24/7, так і тимчасові, що запускаються з резидентних у відповідь на запит клієнта SCADA або згідно з алгоритмом роботи процесів сервера SCADA.

Тимчасова програма проходить свої три стани послідовно або взаємодіє з користувачем через вікна інтерфейсу. Штатне завершення тимчасового процесу здійснюється після закінчення виконання деякого алгоритму або через інтерфейс користувача про завершення роботи.

Резидентні процеси run-time сервера SCADA після початкової ініціалізації входять в цикл очікування запиту, команди, повідомлення або сигналу від клієнта SCADA або будь-якого іншого процесу системи згідно з алгоритмом взаємодії процесів системи. Штатне завершення роботи run-time сервера SCADA відбувається через інтерфейс користувача спеціалізованого резидентного процесу або шляхом запуску командного файлу на завершення роботи run-time сервера SCADA системи. При цьому всі резидентні процеси отримують сигнал про примусове

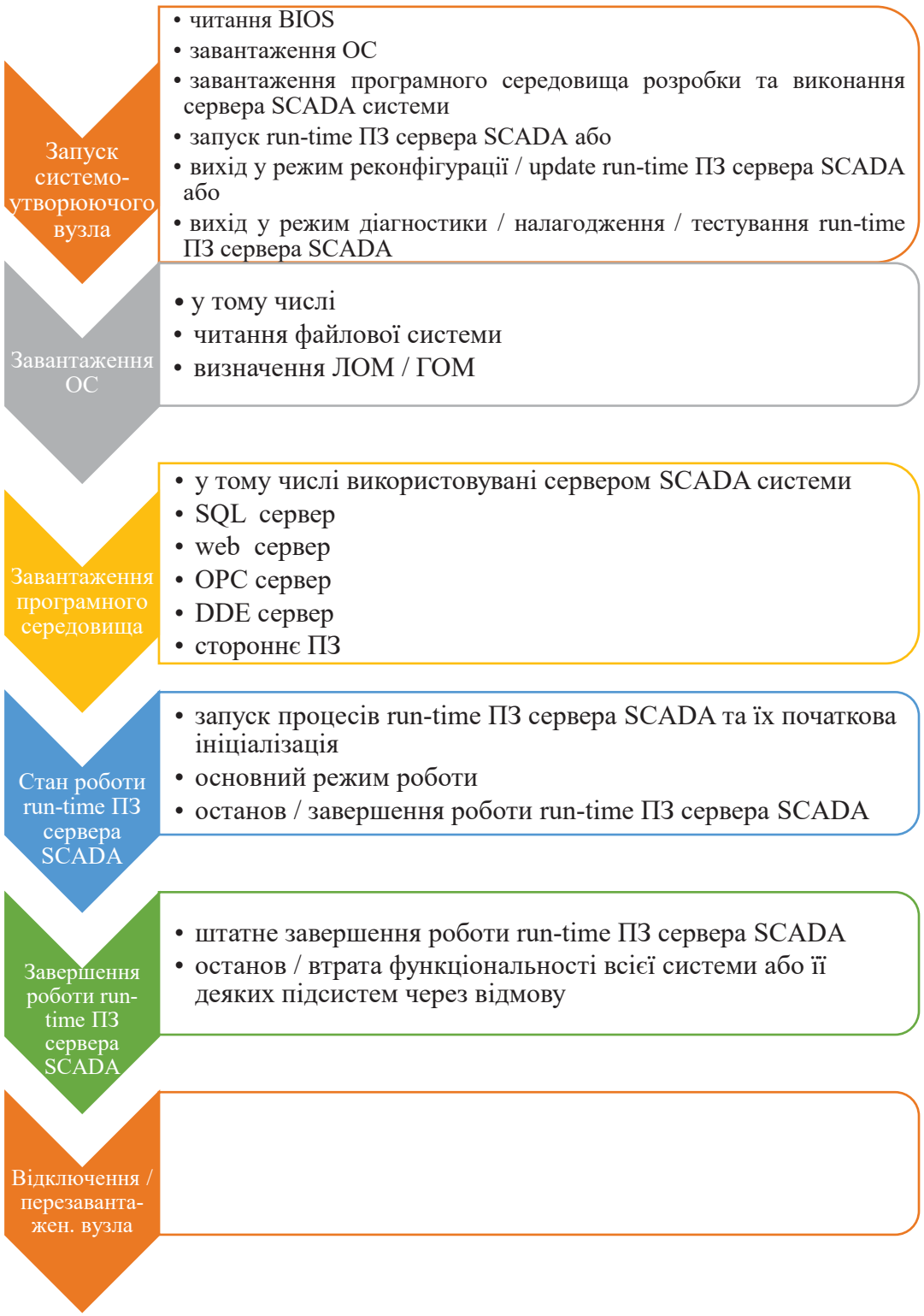

Рис. 2. Діаграма станів системоутворюючого вузла сервера SCADA

завершення та тільки тоді переходять в свій третій стан.

Будь-який з процесів run-time сервера SCADA може завершитися позаштатно з деяким кодом завершення, що дозволяє діагностувати проблему. Якщо даний вид несправності не був заздалегідь передбачений, та його обробка не була прописана в коді програми, то такий процес зніметься аварійно. Аварійне завершення процесу можливо в будь-якому місці (на будь-якому етапі виконання програми).

Крім того, нештатне завершення або аварійне зняття процесу в складі run-time ПЗ сервера SCADA може бути пов'язано з нештатним

завершенням процесу /процесів будь-якого з PI (див. Рис. 1), які повинні взаємодіяти з даним процесом.

Позаштатне завершення або аварійне зняття тимчасового процесу в складі run-time ПЗ сервера SCADA не обов'язково буде критично для працездатності системи в цілому. Перезапуск процесу з інтерфейсу сервера SCADA у багатьох випадках вирішує проблему. Проте, можлива часткова втрата функціональності сервера SCADA, особливо, якщо цей процес не перезапускається. У зв'язку з цим необхідно вести журнал діагностики, в якому будуть зафіксовані коди завершення процесів.

Позаштатне завершення або аварійне зняття резидентного процесу, як правило, є показником виникнення серйозної проблеми в роботі сервера SCADA. Іноді можливо повне або часткове автовідновлення працездатності серверного вузла системи після перезавантаження. Для цього в підсистемі діагностики повинен бути передбачений менеджер процесів, що відслідковує склад і стан резидентних процесів, а також watchdog timer – спеціалізований пристрій для автоматичного перезавантаження системного вузла.

Watchdog timer має вбудований таймер, який налаштовується на T_{wdt} секунд. Кожну секунду значення вбудованого таймера зменшується на одиницю. По закінчення заданого часу T_{wdt}, коли вбудований таймер зможе обнулитися, watchdog timer автоматично виконає перезавантаження системного вузла. Щоб уникнути перезавантаження вузла, необхідно його звести, тобто прописати значення T_{wdt} у вбудованому таймері пристрою до того як він встигне обнулитися.

У разі штатної роботи всіх резидентних процесів в складі run-time ПЗ сервера SCADA зведенням watchdog timer займається менеджер процесів підсистеми діагностики з періодичністю $T < T_{wdt}$. У разі несанкціонованого завершення або нештатної поведінки хоча б одного резидентного процесу watchdog timer НЕ зводиться та після закінчення T_{wdt} з моменту останнього зведення відбувається перезавантаження системного вузла.

Якщо після автоматичного перезавантаження з використанням watchdog timer працездатність сервера SCADA не змогла бути відновлена, тоді watchdog timer деактивується щоб уникнути циклу перезавантажень і системний вузол вважається неробочим. Підсистема аварійної сигналізації (якщо знаходиться в працездатному стані) сповіщає диспетчера SCADA та відповідний обслуговуючий персонал про відмову серверного вузла. Якщо підсистема аварійної сигналізації на даному вузлі непрацездатна, то відмова серверного вузла виявляється досить швидко при першому ж зверненні до нього користувача або процесу з іншого вузла згідно закладеному в розподілену систему алгоритму взаємодії процесів.

Слід зазначити, що для успішного запуску run-time ПЗ сервера SCADA важливим аспектом є попереднє коректне штатне завершення всіх працюючих процесів при закритті системи на серверному вузлі. Штатне завершення всіх процесів вимагає деякого інтервалу часу Δt_{close} після отримання менеджером процесів сигналу на закриття системи. Сигнал на закриття може надходити:

– від адміністратора системи або правомочного експлуатаційного персоналу (в зв'язку з діагностикою, профілактикою або модернізацією серверного вузла);

– від драйвера джерела безперебійного живлення (UPS – Uninterruptible Power Supply) (в зв'язку з відсутністю напруги в електромережі та низьким рівнем зарядки батареї живлення UPS для підтримки роботи серверного вузла);

– від процесу, що працює з watchdog timer, (в зв'язку з необхідністю перезавантаження) та ін.

Якщо сталося зникнення напруги в електромережі та UPS, що працює від батареї, це відключить серверний вузол до повного закриття системи Δt_{close} або ж watchdog timer спрацює та перезавантажить вузол до Δt_{close}, тоді при наступному завантаженні можуть виникнути проблеми в зв'язку з частковою або повною втратою функціональності серверного вузла.

Для запобігання відмов системи, пов'язаних з відключенням живлення або перезавантаженням серверного вузла, необхідна розробка безпечних алгоритмів закриття системи з визначенням часу реакції та синхронізацією взаємодії відповідальних процесів.

На рис. 3 приведена діаграма взаємодії структурних компонентів серверного вузла SCADA.

На діаграмі взаємодії (див. Рис. 3) наведено один з можливих сценаріїв роботи серверного вузла SCADA. При наявності напруги в електромережі та коректному самотестуванні UPS подається напруга живлення від електромережі через UPS на серверний вузол SCADA. Виконується запуск серверного вузла згідно діаграмі, наведеної на рис. 2.

В процесі роботи run-time ПЗ сервера SCADA сталося аварійне зняття резидентного процесу сервера SCADA. Результатом реакції на цю подію є спроба автоматичного завершення роботи системи (наскільки це можливо в конкретній ситуації). За сигналом від watchdog timer серверний вузол йде на перезавантаження.

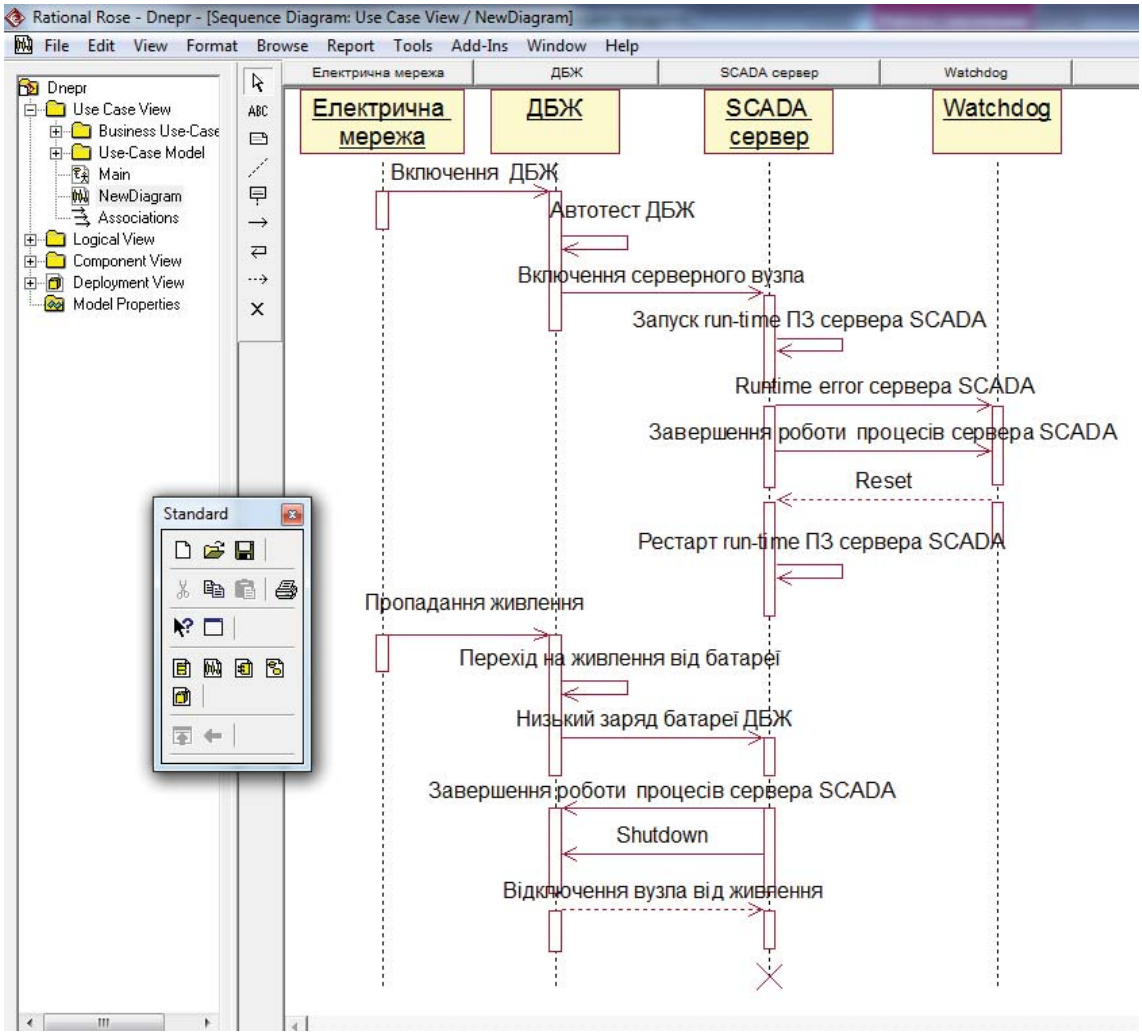

Рис. 3. Діаграма взаємодії структурних компонентів серверного вузла SCADA

Згідно зі сценарієм на діаграмі (рис. 3) запуск системи після перезавантаження відбулося коректно. Таким чином, було виконано автовідновлення працездатності системи. Слід зазначити, що ймовірність успішного автовідновлення системи після перезавантаження не перевищує 30%.

В деякий момент часу відбулося зникнення напруги в електромережі. UPS переходить на батарею, яка з часом розрядиться. При досягненні деякого настроюваного значення заряду батареї U_{lim} драйвер UPS в складі ПЗ сервера SCADA посилає сигнал на закриття системи, після чого відключає UPS. При коректному закритті системи до відключення живлення черговий запуск системи на серверному вузлі, як правило, виконується успішно. Якщо ж через розряджену батарею UPS відключився до завершення закриття SCADA системи на серверному вузлі, то ймовірність відмови при черговому запуску становить близько 50%.

Висновки та перспективи подальших досліджень. Відмови SCADA системи та тривалість часу відновлення працездатності обслуговуючим персоналом SCADA істотно впливають на зниження якості управління технологічним процесом на промисловому підприємстві в режимі реального часу. Тому особлива увага приділяється розробці методів профілактики відмов та автовідновлення системи після оборотних відмов.

У даній статті були розглянуті деякі з цих методів, пов'язані з проблемами зникнення напруги живлення в електромережі, низького заряду батареї UPS, некоректного завершення процесів при закритті системи. Був показаний метод автовідновлення системи шляхом виявлення відмови з наступним автоматичним перезавантаженням серверного вузла. Цей метод може бути ефективний для цілого спектра різноманітних оборотних відмов.

Враховуючи жорсткий графік експлуатації SCADA систем (24/7 в режимі реального часу), дослідження причин виникнення відмов в SCADA, напрацювання банку методів автовідновлення працездатності системи дозволять істотно підвищити її надійність та відмовостійкість.

ЛІТЕРАТУРА:

1. Bailey D., Wright E. Practical SCADA for Industry. Australia: Newnes, 2003. 304 p.
2. Hunzinger R. SCADA Fundamentals and Applications in the IoT. Internet of Things and Data Analytics: Handbook, Wiley Telecom, 2017. 293 p.
3. Moore M. S., Monemi, S., Jianfeng W. Integrating information systems in electric utilities. *SMC 2000 Conference Proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics "Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions"*. 2000. № 1. pp. 399–404.
4. Campos, F.T., Mills, W.N., Graves, M.L. A reference architecture for remote diagnostics and prognostics applications. *Proceedings, IEEE AUTOTESTCON*. 2002. pp. 842–853.
5. Mingzan, W., Ziye, Z. Service Architecture of Grid Faults Diagnosis Expert System Based on Web Service. *2007 8th International Conference on Electronic Measurement and Instruments*. 2007. pp. 3–413.

REFERENCES:

1. Bailey D., Wright E (2003). Practical SCADA for Industry. Australia: Newnes.
2. Hunzinger R (2017). SCADA Fundamentals and Applications in the IoT. Internet of Things and Data Analytics: Handbook, Wiley Telecom.
3. Moore M. S., Monemi, S., Jianfeng W (2000). Integrating information systems in electric utilities. *SMC 2000 Conference Proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics "Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex Interactions"*. 1, 399-404.
4. Campos, F.T., Mills, W.N., Graves, M.L (2002). A reference architecture for remote diagnostics and prognostics applications. *Proceedings, IEEE AUTOTESTCON*.
5. Mingzan, W., Ziye, Z (2007). Service Architecture of Grid Faults Diagnosis Expert System Based on Web Service. *2007 8th International Conference on Electronic Measurement and Instruments*, 3–413.