Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2020

(Випуск 2)

[електронне видання]

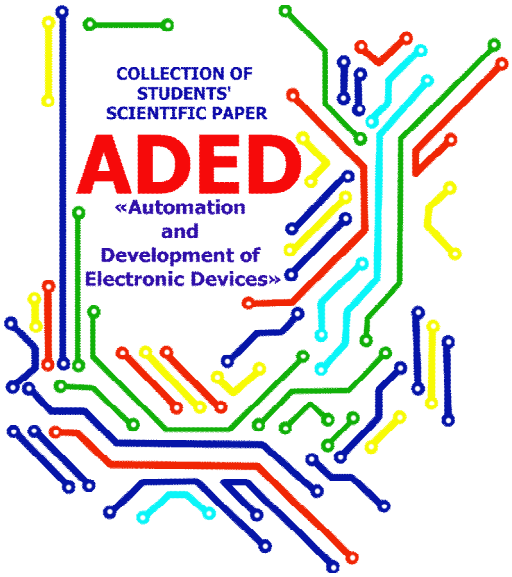
http://nure.ua/department/kafedra-komp-yuterno-integrovanih-tehnologiy-avtomatizatsiyi-ta-mehatroniki-kitam

http://itez.zntu.edu.ua/

http://kafea.kdu.edu.ua

Харків 2020

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
кафедра комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки
(КІТАМ)



ЗБІРНИК

студентських наукових статей

«Автоматизація та приладобудування»

«Automation and Development of Electronic Devices»

ADED-2020

(Випуск 2)

[електронне видання]

Харків 2020

АВТОМАТИЗАЦІЯ ТА ПРИЛАДОБУДУВАННЯ («Automation and Development of Electronic Devices» ADED-2020) [Електронний ресурс] : збірник студентських наукових статей / Харківський національний університет радіоелектроніки ; [редкол.: І.Ш. Невлюдов та ін.]. – Харків : ХНУРЕ, 2020. – Вип. 2. – 298 с.

COLLECTION OF STUDENTS' SCIENTIFIC PAPER «AUTOMATION AND DEVELOPMENT OF ELECTRONIC DEVICES» ADED-2020 Part 2 (Key infrastructure 2020) - Kharkiv/ The Editorial.: Nevlyudov I.Sh. (head), that all. Kharkiv: Kind of Kharkiv National Universitety of Radio Elektronics [electronic edition], 2020.- 298 p with.

Рекомендовано рішенням
Науково-технічної ради
Харківського національного
університету радіоелектроніки
протокол №6 від 29.11.2018

Рекомендовано рішенням Вченої ради
факультету Автоматики і комп'ютеризованих
технологій
Харківського національного
університету радіоелектроніки
протокол № 2 від 23.11.2020

Збірник містить наукові статті студентів кафедри комп'ютерно-інтегрованих технологій, автоматизації та мехатроніки (КІТАМ) Харківського національного університету радіоелектроніки, кафедри Інформаційних технологій електронних засобів (ІТЕД) Запорізького національного технічного університету та кафедри Електронних апаратів (ЕА) Кременчуцького національного університету ім. М. Остроградського які навчаються за спеціальностями: 151 Автоматизація та комп'ютерно-інтегровані технології, 172 Телекомунікації та радіотехніка, 171 Електроніка та 163 Біомедична інженерія, першого (бакалаврського), другого (магістерського) рівнів вищої освіти. Статті надані в авторській редакції.

– підтримка різних операційних систем, включаючи UNIX, Linux, Mac OS X і Windows;

– одночасна робота великої кількості користувачів в рамках одного проекту;

– повнофункціональне рішення для моделювання;

– просунуті інструменти промислового дизайну (вільні форми, параметричні поверхні, динамічний рендеринг;

– глибока інтеграція з PLM-системою Teamcenter.

CATIA

Система автоматизованого проектування від компанії Dassault Systemes, орієнтована на проектування складних комплексних виробів, в першу чергу, в області авіабудування і кораблебудування.

До особливостей можна віднести:

– орієнтація на роботу з моделями складних форм;

– глибока інтеграція з розрахунковими і технологічними системами;

– можливості для колективної роботи тисяч користувачів над одним проектом;

– підтримка міждисциплінарної розробки систем.

ВИСНОВКИ. Таким чином, в ході проведеного аналізу застосування засобів САПР у приладобудуванні, класифікації та види САПР: CATIA, NX, PTC Creo , Компас–3D, SolidEdge, SolidWorks, AutoCAD**.** Були виділені їх основні особливості, що будуть передумовою для вибору систем, які зможуть вирішити поставлені завдання.

ЛІТЕРАТУРА

1. Савёлов И. Н., Довнар, А. С., Плытник Е. А., Савёлов П. И. Применение современных САПР в электронном приборостроении. 2019.
2. Зарипова Р. С., Галямов Р. Р. Применение машиностроительных САПР для проектирования цифровых аналогов приборов. // Наука и образование: новое время. – 2019. – № 1. С. 96–98.
3. Митрофанов А. Н. Сравнительный анализ систем автоматизированного проектирования изделий машиностроения // Дневник науки. – 2020.– № 9.– С.13–14.
4. Бесхлебнов И. В. Классификация САПР и их функциональное назначение // Международный студенческий научный вестник.– 2019.– № 6. С. 6.
5. Нестерова Н. В., Пыхтырев В.С., Сырямкин В.И. Основы приборостроения: учебное пособие. 2018.
6. Ганиева Т. И., Тожикулов Х. Ю. Основы построения автоматизированных информационных систем. // Техника и технологии машиностроения. – 2018. С. 186–189.

Науковий керівник: *Сотник Світлана Вікторівна, к.т.н., доцент кафедри КІТАМ Харківського національного університету радіоелектроніки*

УДК 621.315

ЗВ'ЯЗОК ПРОМИСЛОВОЇ АВТОМАТИЗАЦІЇ І КОНТРОЛЮЮЧИХ СИСТЕМ

Шило Н. Ю.

Харківський національний університет радіоелектроніки

Україна, 61166, Харків, пр. Науки, 14

E-mail: nazar.shylo@nure.ua

Анотація: Системи промислової автоматизації та управління (IACS) були в основному ізольовані від корпоративних систем за допомогою власних протоколів, що сприяло їх захист від кібератак за принципом «безпека через невідомість». Однак широке впровадження нових комунікаційних технологій, таких як Інтернет-протоколи та бездротові комунікації змінили дану ситуацію.

Ключові слова: кібератака, мережа, піраміда автоматизації.

THE COMMUNICATION OF INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

N. Shylo
Kharkiv National University of Radioelectronics
Ukraine, 61166, Kharkiv, Nauky av., 14
E-mail: nazar.shylo@nure.ua

Abstract: Industrial Automation and Control Systems (IACS) were largely isolated from corporate systems by means of proprietary protocols, which facilitated their protection against cyber-attacks under the principle of security through obscurity. However, the widespread adoption of the new communication technologies, such as the Internet protocols and wireless communications has changed this scenario.

Key words: cyberattack, network, automation pyramid.

АКТУАЛЬНІСТЬ РОБОТИ. В останні роки було багато свідчень про кібератаки на промислову автоматизацію і контролюючі системи, особливо на їхні вразливі місця. На жаль, ці атаки значно зросли протягом останніх років, і цілком чітко помітна лише вершина айсберга, яка приходить до відома громадськості.

ВСТУП. Промислова автоматизація і контролюючі системи покривають різні типи контролюючих систем, які включають наглядовий контроль та збір даних і розподілені системи управління, що отримують дані з промислових процесів за допомогою специфічних пристроїв – програмних логічних контролерів, віддалених блоків-терміналів та інших інтелектуальних електронних пристроїв. У свою чергу вони оперують даними з виробничих процесів.

Представлення нових технологій і різних типів систем зв'язку у виробничому середовищі зробило значний прогрес у полі автоматизації та контролю. Вони значно покращили можливості систем наглядового контролю та збору даних для стеження за багатьма критичними структурами у режиму реального часу у різних ділянках – енергії, транспорту, води, хімічних процесів, нафти та газу. Даний «ландшафт» розширюється пропозицією комунікацій і зв'язків для будь якого виробничого пристрою, особливо з представленням інтернет технологій [1].

З повагою до бездротового підключення, за даними Бойєса [3], воно було використане 43% операторів у 2011 році. За прогнозами, їх установка зросте на 20% за три роки.

Представлення так званих інформаційних і комунікаційних технологій у виробничому секторі стало випробовуванням для інженерів і дослідників хто активно шукає та розробляє рішення, які базують на мережі, і в той же час покращує процеси автоматизації у термінах операцій [4], включаючи віддалений контроль і стеження виробничих процесів. Це гарантує точний потік інформації у режимі реального часу [2].

При такому сценарії, нові рішення, які базуються на парадигмі віддалених обчислень, дозволяють дослідникам використовувати сервісно-орієнтовані інтерфейси архітектури. Даний підхід представляє нові концепції й парадигми, ідентифіковані як Інтернет Речей, що націлений на зв'язок інфраструктури інформаційних і комунікаційних технологій з різними пристроями (датчики виробництва, розумні лічильники, радіочастотні ідентифікатори, смартфони) за допомогою бездротового підключення [5].

Такі нові налаштування сприяють модифікаціям у створенні і керуванні промислових мереж. Традиційно автоматизовані системи були ізольовані від навколишнього світу і інтернету так, що кількість офісних мереж була мінімальною [6].

Тим більше зростання попиту на такі сервіси незалежно від точки доступу (тобто віддалено) так само як на загальний зв'язок корпоративних систем порушило безпеку промислової автоматизації і контролюючих систем. Як наслідок, в колишніх системах застосування власного обладнання і програмного забезпечення гарантувало високий ступінь захисту даних.

Сьогодні, навпаки, мережі промислової автоматизації і контролюючих систем повинні зіткнутися з загрозами, які присутні в корпоративних системах, одночасно задовольняючи більш

жорсткі вимоги щодо продуктивності (тобто розподіл сигналізації). На рисунку 1 показано типовий сценарій, де виробничі мережі підключені до мереж корпорацій [7].

Рисунок 1 – Типові зв'язки промислової автоматизації і контролюючих систем з корпоративними мережами й Інтернетом

На жаль, ситуація досить складна і заходи безпеки, потрібні у сучасній промисловій автоматизації і контролюючих системах, не можуть бути такими, як у корпоративних мережевих системах завдяки спеціальним вимогам до реального часу та продуктивності виробництва систем. Наприклад, повна доступність (24/7) до обладнання, яка є типовою вимогою у деяких установках, поєднує певні заходи безпеки – оновлення програмного забезпечення з моменту, ці установки вимагають системних запинок та/або перезавантажень.

Існують також погрози, які викликані неправильним використанням обладнання внутрішнім персоналом. Прикладом цього є зараження ботнетом Maiposa через USB-підключення. На відновлення плану пішло три тижні [8]. Саме тому потрібний комплексний план безпеки, який включає весь персонал компанії.

У наведених секціях ми аналізуємо характерні риси зв'язків промислової автоматизації і контролюючих систем, визначаючи основні ключові вразливості щодо кібератак. Пропонується серія контрзаходів для забезпечення кращого захисту таких систем.

ПРОМИСЛОВІ ЗВ'ЯЗКИ. Промислова автоматизація і контролюючі системи зазвичай структуровані ієрархічно у вигляді декількох шарів відповідно до піраміди автоматизації (рис. 2). Кожен шар повинен гарантувати різні вимоги з точки зору експлуатації та продуктивності як для самих систем, так і для комунікацій. Це встановлено стандартом ISA-95[9], який інтегрує різні типи зв'язків, деякі з них власні – польові і контролюючі мережі (базовані на IP-мережах), локальні мережі й Інтернет [10].

Протоколи комунікацій використовують як посилання основну 7-му архітектуру моделі рівня OSI (Відкритий Взаємозв'язок Систем) [11]. І навпаки, конунікаційні протоколи, що використовуються в промислових системах, як правило, є власницькими та специфічними залежно від рівня піраміди автоматизації, де вони використовуються.

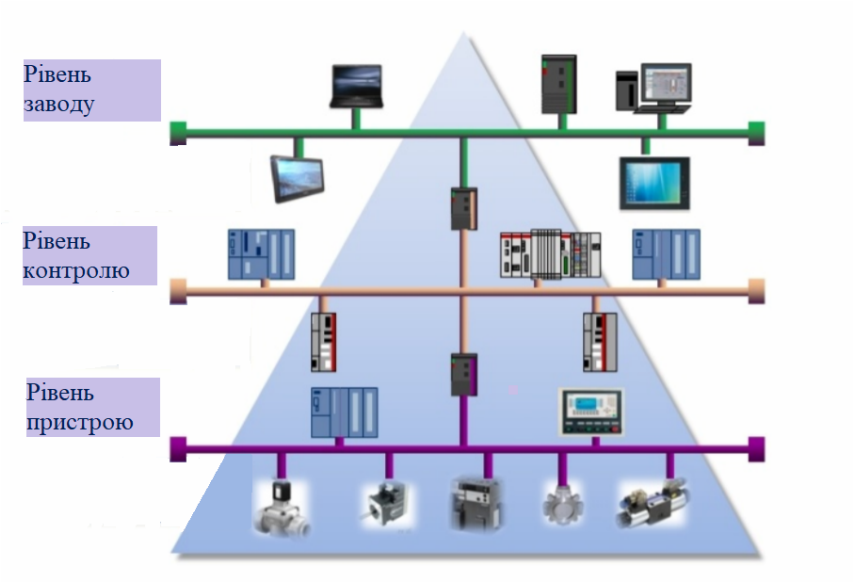


Рисунок 2 – Піраміда автоматизації

Загалом ці протоколи можна класифікувати за такою ієрархією:

1) Рівень заводу. Підключення сегментів мережі на рівні нагляду, моніторинг та корпоративні системи.

2) Рівень контролю. Розповсюдження інформації з поля пристроїв до контролерів та самих драйверів.

3) Рівень пристрою. Розповсюдження інформації від датчиків і приводів до контролерів і польових пристроїв.

Мережева архітектура в промислових автоматизованих системах відрізняється від тієї, яка використовується в офісі. Наприклад, на найнижчих рівнях використовуються безліч протоколів та/або фізичних засобів. Навіть коли вони схожі й ідентичні до офісних, використовують канали для зв'язку з верхніми шарами. З іншого боку в системах управління протоколи і фізичні носії, як правило, менш різноманітні.

ВИСНОВОК. Отож необхідно впровадити глобальні та більш дієві стратегії через політику, яка впливає на обидва рівня мережі та платформи для забезпечення певних заходів безпеки, які можуть допомогти інженерам контролю розробити розумні безпечні системи промислової автоматизації та управління.

Важливо зазначити, що неможливо отримати повністю захищену систему від кібератак. Важливо також врахувати, що багато заходів безпеки вимагають введення складних алгоритмів, таких як шифрування даних, що може впливати на загальну продуктивність системи.

ЛІТЕРАТУРА

1. Calvo, M. Marcos, D. Orive, I. Sarachaga, "A methodology based on distributed object-oriented technologies for providing remote access to industrial plants," Control Engineering Practice, 14 (8), pp. 975-990, 2006. http://dx.doi.org/10.1016/j.conen gprac.2005.05.008.

2. T. Sauter, S. Soucek, W. Kastner, and D. Dietrich, "The evolution of factory and building automation," IEEE Industrial Electronics Magazine, 5 (3), pp. 35-48, 2011. http://dx.doi.org/10.1109/MIE. 2011.942175.

3. W. Boyes, "All quiet on the wireless front," Control, August 2011, http://www.controlglobal.com/articles/2011/all-quite-on-thewireless-front/.

4. M. Jain, A. Jain, and M. Srinivas, "A web based expert system shell for fault diagnosis and control of power system equipment," Proceedings of Intl. Conf. Condition Monitoring and Diagnosis (CMD-08), 2008, pp. 1310–1313. http://dx.doi.org/10.1109/ cmd.2008.4580217.

5. S. Li, L.D. Xu, and S. Zhao, “The internet of things: a survey,” Information Systems Frontiers, 17 (2), pp. 243-259, 2015. http://dx.doi.org/10.1007/s10796-014-9492-7.

6. K. Fischer and J. Gesner, “Security Architecture Elements for IoT enabled Automation Networks,” 17th IEEE Intl. Conf. Emerging Technologies and Factory Automation (ETFA), 2012. http://dx.doi.org/10.1109/etfa.2012.6489651.

7. M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” IEEE Transactions on Industrial Informatics, 9:1, pp. 277-293, 2013. http://dx.doi.org/10.1109/TII. 2012.2198666.

8. P. Sinha, A. Boukhtouta, V.H. Belarde, and M. Debbabi, “Insights from the Analysis of the Mariposa Botnet,” 5th IEEE Intl. Conf. Risks and Security of Internet and Systems (CRiSIS), 2010. http://dx.doi.org/10.1109/crisis.2010.5764915.

9. Невлюдов І. Ш. Трансфер технологій у сучасній науці, освіті та виробництві в умовах четвертої промислової революції «ІНДУСТРІЯ 4.0» / І. Ш. Невлюдов, О. О. Чала, Ю. М. Олександров // Сучасний рух науки: тези доп. VIII міжнародної науково-практичної інтернет-конференції, 3-4 жовтня 2019 р. – Дніпро, 2019. – Т.2 С.: 604-608

10. K. Selivanova, K. Determination of the basic parameters of sensor devices for the implementation of psychoneurological research with the introduction of multitouch technology / K. Selivanova, O. Avrunin, N. Kazimirov // Innovative Technologies and Scientific Solutions for Industries, 2020. No. 1 (11), P. 147-155. DOI: https://doi.org/10.30837/2522-9818.2020.11.147

11. Невлюдов И. Ш., Палагин В. А., Чалая Е. А. Технологии микросистемной техники (часть II) // Технология приборостроения. – 2015. – №. 2. – С. 5-1

12. I. Nevliudov, S. Maksymova, A. Funkendorf, O. Chala and K. Khrustalev, "Using MEMS to adapt ultrasonic welding processes control in the implementation of modular robots assembly processes", IEEE XIV-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH), pp. 223-226, 2018.

13. Основи наукових досліджень: Навч. посібник / І.Ш. Невлюдов, Ю.М. Олександров, А.О. Андрусевич, О.О. Чала. – Кривий Ріг: Криворізький коледж НАУ, 2019. – 396 с.

14. Невлюдов, І. Ш., Демська, Н. П., Чала, О. О., & Демська, А. І. ГРУПОВЕ УПРАВЛІННЯ ГНУЧКИМИ ВИРОБНИЧИМИ СИСТЕМАМИ У ВИГОТОВЛЕННІ МЕМС ВИРОБІВ. ББК: У 290-21, 101.

Науковий керівник: *Чала Олена Олександрівна, старший викладач кафедри КІТАМ Харківського національного університету радіоелектроніки*

УДК: 621.317

РОЗРОБКА СТРУКТУРИ ЦИФРОВОГО ОСЦИЛОГРАФУ НА БАЗІ ARDUINO UNO

Єрмашева А. С.
Харківський національний університет радіоелектроніки
радіоелектроніки
Україна, 61166, Харків, пр. Науки, 14
E-mail: alina.yermasheva@nure.ua

Аннотація: Дана стаття присвячена розробці портативного цифрового осцилографа на базі мікроконтролера ATmega328. Автором було проведено критичний аналіз сучасних публікацій по темі досліджень, в ході яких були виявлені недоліки, до яких можна віднести: великі маса габаритні параметри, не зручність аналізу отриманих даних. Для усунення цих недоліків в статті запропонована структурна схем портативного осцилографа і обрані не обхідні модулі.

Ключові слова: структура, цифровий осцилограф, arduino uno