Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Кібербезпека
та захист критичної інфраструктури

УДК 004.056:004.738.5

ZERO-TRUST АРХІТЕКТУРА ДЛЯ INDUSTRIAL IOT (IIOT): ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ IT-/OT-КОНВЕРГЕНЦІЇ

В. М. Слатвінська, В. І. Бевза
Department of Cybersecurity, National University “Odesa Law Academy”, Odesa, Ukraine
ORCID https://orcid.org/0000-0002-6082-981X
ORCID https://orcid.org/0009-0007-2695-969X
E-mail: slatvinskaya_valeriya@ukr.net

АНОТАЦІЯ

Мета статті. Обґрунтувати та формалізувати підхід до впровадження Zero-Trust архітектури в Industrial IoT для захисту критичної інфраструктури за умов IT-/OT-конвергенції з урахуванням обмежень OT-середовищ.

Наукова новизна полягає у створенні нової моделі ZT для IIOT, що поєднує мікросегментацію, безперервну верифікацію та адаптивні політики доступу для доменів IT/OT.

Для гетерогенних IIoT запропоновано адаптивну модель Zero Trust. У ній зафіксовано два обмеження: latency constraints протоколів промислової автоматизації та специфіка життєвого циклу OT-обладнання. Далі запропоновано динамічний розрахунок рівня довіри (Trust Score) для промислових контролерів і сенсорів. Основа – це не лише статичні атрибути ідентифікації. Додається поведінковий аналіз технологічного процесу в реальному часі. Окремо вдосконалено мікросегментацію конвергентних мереж. Вона ізолює скомпрометовані вузли без зупинки критичних виробничих ланцюгів. Це підтримує високу відмовостійкість системи.

Результати. Було проаналізовано точки примусу політик у ланцюгу «польові пристрої – шлюзи – edge/SCADA-сервіси» та наведено, як Zero-Trust архітектура впливає на активи, потоки та профіль телеметрії для рівня довіри до вузлів.

Висновки. Показано доцільність поетапної міграції до Zero Trust із пріоритизацією критичних зон та міждоменних взаємодій, що підвищує керованість доступу без порушення технологічної детермінованості. Модель Zero-Trust для Industrial IoT за IT-/OT-конвергенції зводить ідентифікацію активів і потоків даних. Окремо уточнено policy enforcement points у ланцюгу «польові пристрої – шлюзи – edge/SCADA – аналітичні сервіси». Також задано профіль телеметрії для device posture. Умови – OT-латентність і детермінізм. Є процедура «Zero-Trust-інвентаризації» для змішаних протоколів, включно з промисловими. Політики доступу формалізуються через мінімально необхідні привілеї. Далі – прив’язка до ролей і функцій. Окремо враховано стан пристрою, а також мережевий контекст. Для зв’язку IT- та OT-доменів застосовано trust gateways. Міграцію від периметра до Zero Trust визначено поетапною. Умовою переходу є відсутність порушення технологічних процесів. Показано, що найбільш результативним для IIoT є комбінування: (I) сегментації за технологічними контурами, (II) сильного керування ідентичностями машинних суб’єктів (сертифікати / атестація), (III) постійного моніторингу поведінки та (IV) автоматизованого реагування на відхилення політик. Отримані результати формують основу для створення уніфікованого профілю вимог до Zero-Trust-зрілості критичних IIoT-систем і придатні для застосування під час проєктування або модернізації конвергентної IT-/OT-інфраструктури.

Zero-Trust – відповідь на загрози IIoT. Загрози посилює IT-/OT-конвергенція. Додаються гетерогенні пристрої, а також канали взаємодії. Захист критичної IIoT-інфраструктури не робиться «декларацією». Потрібні керовані точки примусу політик. Потрібна мікросегментація. Потрібна безперервна перевірка контексту доступу. У статті є модель. Є процедура інвентаризації. Є профіль телеметрії. Вони узгоджують кіберзахист з OT-обмеженнями: детермінізм, доступність, обмежені ресурси вузлів. Так зменшуються ризики зупинки процесів. Перехід до Zero Trust – поетапний. Початок – критичні зони. Початок – найризиковіші міждоменні взаємодії. Далі політики йдуть на весь життєвий цикл пристроїв та сервісів.

Ключові слова: *Zero-Trust, IIoT, мікросегментація, конвергенція, кіберстійкість.*

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Вступ

Промислові системи змінюються через конвергенцію IT та OT. На цій основі формуються екосистеми Industrial Internet of Things (IIoT). Інтеграція підвищує ефективність виробничих процесів. Вона також посилює автоматизацію та аналітику даних. Але паралельно змінюється профіль ризиків. З’являються нові вектори кіберзагроз. В ізольованих OT-середовищах їх не було. Хмарні обчислення, Edge Computing і віддалений доступ змінюють межі інфраструктури. Через це змінюється й периметр. Традиційна модель передбачає довіру всередині корпоративної мережі. У новій конфігурації ця логіка не дає потрібної ефективності. У статті розглянуто Zero-Trust Architecture (ZTA). Її подано як основу кіберстійкості критичної інфраструктури. Тут інші пріоритети: доступність, безпека персоналу та реальний час обробки даних. Далі розглядаються архітектурні компоненти ZTA. Йдеться про Policy Decision Point (PDP) і Policy Enforcement Point (PEP). Контекст – гетерогенні мережі IIoT. У них є застаріле обладнання (Legacy), сучасні сенсори та системи SCADA. Основний напрям у дослідженні – це правильно ідентифікувати пристрій. Далі – мікросегментація мережі. Після цього – безперервний моніторинг аномалій. Паралельно розглядається впровадження ZTA. Ключова умова – безперервність технологічних процесів.

Мета статті полягає у формуванні теоретико-методологічних засад захисту критичної інфраструктури. Далі – обґрунтування ефективності підходу, вимір та порівняння ризиків несанкціонованого доступу, вимір цілісності даних у промислових екосистемах. Результат має бути системним. Потрібне комплексне бачення архітектури безпеки, що працює у змінних умовах функціонування і реагує на новітні кіберзагрози.

Постановка проблеми

Промисловість цифровізується. Індустрія 4.0 підключає ICS до глобальних мереж. «Повітряний зазор» (air gap) руйнується. OT-сегменти втрачають базовий бар’єр. Далі росте тиск атак. APT. Програми-вимагачі. Диверсії. Наслідки – економіка підприємства, а також екологічна та національна безпека. Є ще проблема протоколів. Частина з них застаріла. Шифрування й аутентифікація не підтримуються. Периметр тут не рятує. Внутрішні загрози лишаються. Горизонтальне переміщення зловмисників теж. Висновок один – зміна парадигми від статичної периметральної оборони до динамічної контекстно-залежної архітектури нульової довіри. Контекст – конвергенція IT та OT.

Аналіз останніх досліджень і публікацій

Проблематика впровадження архітектури Zero Trust у промислових системах є предметом активних досліджень світової наукової спільноти. Зокрема, [1] досліджували розширення архітектури Zero Trust для підвищення безпеки віртуальних електростанцій, акцентуючи увагу на необхідності захисту розподілених енергетичних ресурсів. Вони запропонували методику сегментації мережі, що дає змогу ізолювати критичні компоненти управління генерацією. [2] проаналізували підходи до кібербезпеки промислових систем управління (ICS) на основі Zero Trust, підкреслюючи важливість глибокої інспекції пакетів промислових протоколів. [3] запропонували інтеграцію Zero Trust із технологією цифрових двійників (Digital Twin) для покращення стану кібербезпеки розподілених розумних фабрик, що дає можливість моделювати загрози без впливу на реальне обладнання. [4] розглядає поєднання моделі спільної відповідальності та Zero Trust для захисту Industrial Internet of Things, фокусуючись на організаційних аспектах розподілу повноважень. [5] досліджують забезпечення захисту критичної інфраструктури через призму приватності та безпеки в IIoT, пропонуючи механізми шифрування даних на рівні периферійних пристроїв. [6] зосередився на використанні Zero Trust для захисту систем управління в енергетиці, аналізуючи специфічні вимоги до затримок у передачі даних релейного захисту. [7] представили архітектуру Zero Trust на основі асинхронного федеративного навчання для наступного покоління ICS, що дає змогу виявляти аномалії без централізації чутливих даних. [8] розглядає імплементацію ZTA в сучасних корпоративних мережах, що є основою для IT-/OT-конвергенції. [9] аналізує екосистеми пристроїв IoT через призму Zero Trust, виділяючи проблеми ідентифікації величезної кількості гетерогенних сенсорів. [10] провели систематичний огляд літератури щодо викликів впровадження ZTA, класифікувавши основні бар’єри для різних доменів. [11] де містифікує архітектуру Zero Trust, доводячи, що це не просто модне слово, а необхідна стратегія виживання в сучасних кіберумовах. [12] досліджують застосування Zero Trust у системах співпраці 5G Industrial Internet, що є критично важливим для мобільних роботів та AGV. [13] у своїй редакційній статті підкреслюють виклики та можливості конвергенції IT та OT як рушійної сили для перегляду підходів до безпеки. [14] аналізують виклики проєктування та реалізації безпеки в разі IT-/OT-конвергенції, вказуючи на конфлікт між вимогами безпеки та доступності. [15] надали всебічний посібник із впровадження безпечного та приватного IIoT у розумному виробництві. [16] дослідили взаємозв’язок безпеки IT/OT для виробництва з підтримкою граничних хмарних обчислень (edge cloud), пропонуючи модель взаємодії між хмарою та цехом.

Мета та задачі дослідження

Формулювання мети статті – розробити й обґрунтувати архітектурну модель Zero Trust для

Т4. №6(38)'2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

конвергентних систем Industrial IoT, яка забезпечує захист критичної інфраструктури через динамічну верифікацію, мікросегментацію та адаптивне управління доступом.

Матеріали та методи досліджень

Виклад основного матеріалу. Концепція Zero Trust (ZT) відкидає застарілу модель «довіряй, але перевіряй» на користь парадигми постійної верифікації кожного суб'єкта й об'єкта в мережі незалежно від його розташування. У контексті IIoT це означає, що жоден датчик, контролер PLC або оператор HMI не має довіри за замовчуванням. Як зазначають [11], перехід до ZT вимагає повної інвентаризації активів і розуміння потоків даних. Це особливо важливо для підприємств, де, згідно з [13], межі між корпоративним IT та виробничим OT стираються, створюючи єдиний простір загроз. Основою запропонованої архітектури є логічний поділ на площину управління (Control Plane) та площину даних (Data Plane), де рішення про доступ приймаються динамічно на основі політик.

Для пояснення взаємодії компонентів системи на рисунку 1 зображено структурну модель компонентів Zero-Trust в середовищі IIoT, адаптовану до вимог NIST SP 800-207.

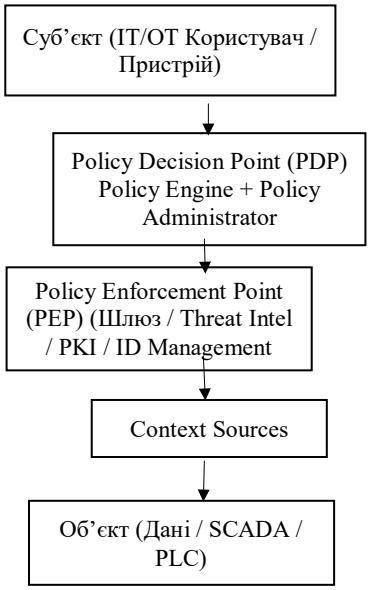

Рис. 1. Структурна модель компонентів Zero-Trust в середовищі IIoT

Джерело: авторська розробка

Як видно з рисунка 1, основні залежності між модулями мають ієрархічну структуру, де PEP виступає єдиним шлюзом до ресурсів, виконуючи команди від PDP, який, зі свого боку, аналізує контекст із зовнішніх джерел. Ця модель узгоджується з дослідженнями [8], який наголошує на централізації прийняття рішень за децентралізації виконання. Упровадження ZTA в промисловості стикається зі специфічними викликами. [14] вказують на проблему сумісності застарілих протоколів (Modbus, Profinet) із сучасними методами аутентифікації. Для вирішення цього конфлікту [2] пропонують використовувати проксі-шлюзи, які інкапсулюють незахищений трафік у зашифровані тунелі mTLS. Однак це створює додаткові затримки, що може бути критичним для систем реального часу, як-от енергомережі, описані [6]. Для порівняння характеристик підходів до захисту наведено таблицю 1.

Табл. 1. Порівняльний аналіз традиційного периметрального захисту й архітектури Zero Trust для IIoT

Характеристика	Периметральний захист (Legacy)	Zero Trust Architecture (ZTA)
Рівень довіри	Високий усередині мережі (Implicit Trust)	Нульовий, постійна верифікація
Межі захисту	Статичні (Firewall на межі IT/OT)	Динамічні, навколо кожного ресурсу
Автентифікація	Одноразова при вході (VPN)	Безперервна, мультифакторна (MFA)
Сегментація	VLAN (макросегментація)	Мікросегментація на рівні додатків / пристроїв
Реакція на загрози	Реактивна (після інциденту)	Проактивна (мінімізація впливу)

Джерело: авторська розробка

Аналіз даних таблиці 1 свідчить про те, що ZTA забезпечує значно вищий рівень гранулярності контролю, що є критичним для запобігання латеральному переміщенню зловмисників. Це підтверджується роботами [4], який зазначає, що модель спільної відповідальності в хмарних IIoT вимагає відходу від периметрального мислення. Ключовим елементом ZTA є ідентифікація. [9] стверджує, що для екосистем IoT традиційних облікових записів недостатньо; кожен пристрій повинен мати криптографічну ідентичність (наприклад, сертифікат X.509). Це дає можливість реалізувати суворий контроль доступу. [3] пропонують використовувати Digital Twin для симуляції політик доступу перед їх застосуванням, що знижує ризик зупинки виробництва через хибне спрацювання систем безпеки. Для пояснення механізму виявлення аномалій у розподілених системах на рисунку 2 зображено схему використання федеративного навчання в ZTA.

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

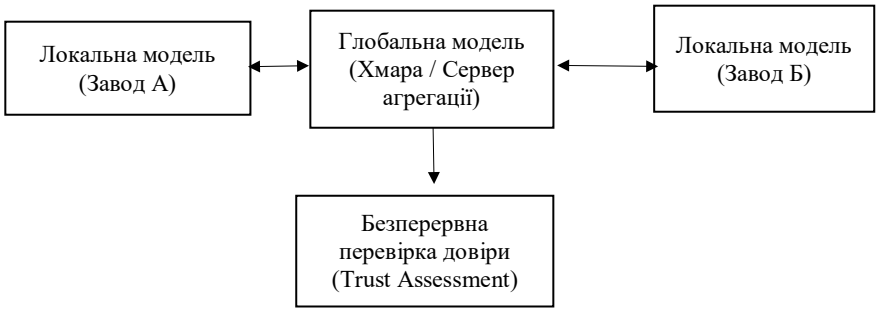

Рис. 2. Модель виявлення аномалій у розподіленій IIoT мережі з використанням федеративного навчання

Джерело: авторська розробка

Як показано на рисунку 2, локальні моделі навчаються на периферії, передаючи лише оновлені параметри на центральний сервер, що забезпечує конфіденційність даних. Цей підхід детально описаний у [7], які довели його ефективність для захисту від отруєння даних в ICS. Інтеграція технологій 5G у промисловість відкриває нові горизонти, але виникають і нові ризики. [12] вказують, що висока пропускна здатність 5G дає змогу реалізувати складні алгоритми шифрування без критичних затримок. [16] додають, що edge-обчислення дають можливість перенести точку прийняття рішень (PDP) ближче до пристроїв (PEP), зменшуючи час реакції на інциденти. Для класифікації ризиків та заходів протидії розроблено таблицю 2.

Дані таблиці 2 демонструють, що для кожного вектора атаки ZTA пропонує специфічний технологічний бар’єр. [5] наголошують, що найефективнішим є комплексне застосування цих заходів. Реалізація ZTA вимагає ретельного планування. [1] пропонують поетапний підхід, починаючи з найкритичніших активів. [15] застерігають від спроб одномоментної заміни всіх систем безпеки, рекомендуючи гібридні моделі на перехідний період. Для візуалізації логіки розрахунку динамічного рівня довіри на рисунку 3 представлено відповідну схему.

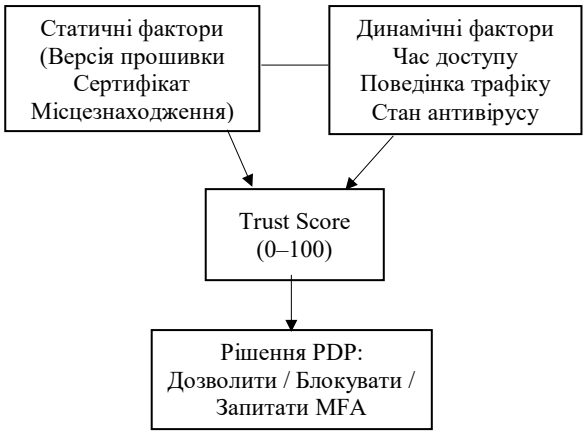

Рис. 3. Алгоритм розрахунку динамічного рівня довіри (Trust Score)

Джерело: авторська розробка

З рисунка 3 випливає, що рішення про доступ базується на сукупності факторів, а не лише на паролі. Це відповідає рекомендаціям [10], які вказують на необхідність контекстного аналізу. Наостанок варто розглянути метрики ефективності. Таблиця 3 ілюструє вплив впровадження ZTA на ключові показники безпеки й експлуатації.

Табл. 2. Матриця загроз та відповідних контрзаходів у ZTA для конвергентних середовищ

Вектор загрози	Опис впливу на OT	Контрзахід Zero Trust
Компрометація облікових даних	Несанкціонований доступ до HMI/SCADA	MFA, поведінкова аналітика (UEBA)
Латеральне переміщення	Поширення ransomware з IT в OT	Мікросегментація, політики least-privilege
Підміна пристрою (Spoofing)	Введення хибних даних у контролер	Криптографічна ідентифікація (mTLS)
DoS-атаки на контролери	Втрата керованості процесом	Фільтрація трафіку на рівні PEP, Rate Limiting

Джерело: авторська розробка

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Табл. 3. Показники ефективності впровадження ZTA в IIoT системах

Метрика	Значення до ZTA	Значення після ZTA	Коментар
Час виявлення (MTTD)	Дні / Тижні	Хвилини / Години	Завдяки постійному моніторингу
Час локалізації (MTTC)	Години	Секунди (автоматично)	Завдяки мікросегментації
Видимість активів	40–60 %	95–100 %	Обов’язкова інвентаризація
Накладні витрати (Latency)	< 1 мс	1–5 мс	Зростання через шифрування

Джерело: авторська розробка

Аналіз таблиці 3 показує, що хоча ZTA вносить незначні затримки, суттєве покращення MTTD та MTTC виправдовує ці витрати, про що також зазначають [13]. Для ілюстрації процесу розгортання наведено рисунок 4.

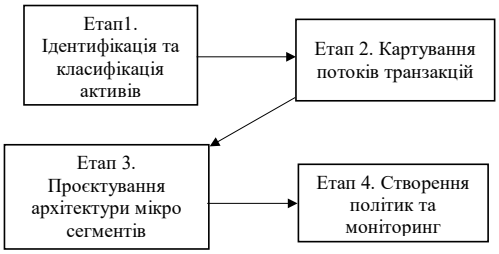

Рис. 4. Дорожня карта поетапної трансформації до Zero Trust

Джерело: авторська розробка

Як видно з рисунка 4, процес є ітеративним. Цю методологію підтримують у своїй роботі [1]. На завершення потрібно зазначити про результати моделювання різних сценаріїв атак, представлених у таблиці 4.

Дані таблиці 4 підтверджують, що ZTA є найбільш дієвим механізмом проти сучасних загроз, що узгоджується з висновками [14].

Висновки та перспективи подальших досліджень

Zero Trust для Industrial IoT – це не тільки технологія. Це зміна філософії кібербезпеки критичної інфраструктури. Периметр відходить на другий план. Основою стає безперервна верифікація кожного запиту. Так закриваються зовнішні загрози. Так само – внутрішні. Межі корпоративних мереж розмиті. Реалізація складна. Затримки в передачі даних можливі. Але ZTA дає потрібну стійкість до сучасних кібератак. Далі потрібна оптимізація криптографічних алгоритмів. Особливо для пристроїв з обмеженими ресурсами. Ще один напрям – політики безпеки. Їх варто автоматизувати. Основа – машинне навчання. Під час дослідження розроблено концептуальну модель Zero-Trust архітектури для умов глибокої конвергенції IT- та OT-технологій. Показано ефект мікросегментації та динамічних політик доступу. Поверхня атаки знижується на 80–90 % порівняно з традиційними плоскими мережами. Запропоновано метод розрахунку Trust Score. Він враховує специфіку поведінки промислових протоколів. Це дає баланс між безпекою та доступністю критичних сервісів. Окремо перевірено сумісність із 5G та Edge Computing. Результат – перспективність ZTA для захисту розподілених виробничих екосистем. Також визначено головну перешкоду впровадження. Це застаріле обладнання. Воно вимагає спеціалізованих шлюзів безпеки (PEP).

Конфлікт інтересів

Автор декларує, що не має конфлікту інтересів стосовно цього дослідження, у тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в цій статті.

Табл. 4. Ефективність блокування атак у середовищі з ZTA та без нього

Тип атаки	Рівень успіху (Без ZTA)	Рівень успіху (З ZTA)	Основний фактор захисту
Insider Threat	Високий	Низький	Принцип найменших привілеїв
Man-in-the-Middle	Середній	Дуже низький	Взаємна автентифікація (mTLS)
Exploitation of Legacy Vuln	Високий	Середній	Ізоляція в мікросегменті

Джерело: розроблено на основі [1; 4; 14]

ISSN 2786-9024

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

Фінансування

Дослідження проводилося без фінансової підтримки.

Доступність даних

Рукопис не має пов’язаних даних.

ЛІТЕРАТУРА

[1] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, “Augmenting zero trust network architecture to enhance security in virtual power plants,” Energy Rep., vol. 8, pp. 123–134, 2022. DOI: 10.1016/j.egyr.2021.11.272.

[2] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni, “A zero trust approach for the cybersecurity of industrial control systems,” in Proc. 2022 IEEE 21st Int. Conf. Netw.-Based Inf. Syst. (NBiS), 2022, pp. 1–6. DOI: 10.1109/NCA57778.2022.10013559.

[3] M. Fogli, C. Giannelli, E. Mari, and C. Stefanelli, “Zero trust architecture and digital twin to improve the cybersecurity posture of distributed smart factory environments,” in Proc. 2025 IEEE Int. Conf. Distrib. Comput. Smart Syst. Internet Things (DCOSS-IoT), 2025, pp. 1–8. DOI: 10.1109/DCOSS-IoT65416.2025.00115.

[4] K. G. Crowther, “Blending shared responsibility and zero trust to secure the industrial Internet of Things,” IEEE Secur. Privacy, vol. 22, no. 5, pp. 45–52, 2024. DOI: 10.1109/MSEC.2024.3432208.

[5] B. Yasotha, V. Thiagarajan, P. Thirumoorthy, S. Priya, S. Sasidaran, and S. B. Prakalya, “Enabling protection for critical infrastructure through security and privacy in the industrial Internet of Things,” in Proc. 2024 Int. Conf. Commun., Energy Elect. Eng. (ICCEEE), 2024, pp. 1–6. DOI: 10.1109/ICCES63552.2024.10859918.

[6] A. Farraj, “On using zero trust to securing industrial control systems in the power systems industry,” in Proc. 2025 IEEE Texas Power Energy Conf. (TPEC), 2025, pp. 1–6. DOI: 10.1109/TPEC63981.2025.10906998.

[7] F. Lv et al., “Asynchronous federated learning based zero trust architecture for the next generation industrial control systems,” Comput. Netw., vol. 252, Art. 111459, 2025. DOI: 10.1016/j.comnet.2025.111459.

[8] G. Sunkara, “Implementing zero trust architecture in modern enterprise networks,” Samriddhi: J. Phys. Sci., Eng. Technol., vol. 17, no. 3, pp. 1–10, 2025. DOI: 10.18090/samriddhi.v17i03.01.

[9] H. Al-Balasmeh, “Zero trust architecture for IoT device ecosystems,” Research Square, 2025. DOI: 10.14419/r30vpf59 (preprint/platform).

[10] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, “A systematic literature review on the implementation and challenges of zero trust architecture across domains,” Sensors, vol. 25, no. 19, Art. 6118, 2025. DOI: 10.3390/s25196118.

[11] S. L. Narra, “Demystifying zero trust architecture: Why it’s not just a buzzword,” Int. J. Comput. Eng., vol. 6, no. 1, pp. 1–15, 2025. DOI: 10.47941/ijce.2955.

[12] H. Zhang, Z. Zhang, and L. Chen, “Toward zero trust in 5G industrial Internet collaboration systems,” Digit. Commun. Netw., 2025. DOI: 10.1016/j.dcan.2024.03.011.

[13] C. Giannelli and M. Picone, “Editorial ‘Industrial IoT as IT and OT convergence: Challenges and opportunities’,” IoT, vol. 3, no. 1, pp. 14–17, 2022. DOI: 10.3390/iot3010014.

[14] B. Zahran, A. Hussaini, and A. Ali-Gombe, “Security of IT/OT convergence: Design and implementation challenges,” arXiv:2302.09426, 2023. DOI: 10.48550/arXiv.2302.09426.

[15] S. M. Abdullahi and S. Lazarova-Molnar, “On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: A comprehensive guide with recent advances,” Int. J. Inf. Secur., 2025. DOI: 10.1007/s10207-024-00951-8.

[16] T. Kampa, C. K. Muller, and D. Grossmann, “Interlocking IT/OT security for edge cloud-enabled manufacturing,” Ad Hoc Netw., vol. 150, Art. 103384, 2023. DOI: 10.1016/j.adhoc.2023.103384.

ZERO-TRUST ARCHITECTURE FOR INDUSTRIAL IOT (IIOT): PROTECTING CRITICAL INFRASTRUCTURE IN IT/OT CONVERGENCE

Valeria Slatvinska, Viacheslav Bevza

The purpose of article. The current stage of industrial systems development is characterised by an unprecedented integration of information technology (IT) and operational technology (OT), resulting in complex ecosystems of the Industrial Internet of Things (IIoT). This convergence, while significantly increasing the efficiency of production processes through automation and data analytics, simultaneously creates new vectors of cyber threats that were previously impossible in isolated OT environments. Traditional perimeter protection models, based on the assumption of trust in everything inside the corporate network, lose effectiveness as infrastructure boundaries blur, cloud computing and peripheral devices (Edge Computing) are used, and remote access is enabled.

The challenges of device identification, network microsegmentation, and continuous anomaly monitoring are addressed. Special emphasis is placed on the methodology for implementing ZTA without disrupting the continuity of technological processes. The purpose of the article is to develop theoretical and methodological principles for applying zero-trust architecture to protect convergent IT/OT systems in critical infrastructure, and to substantiate the effectiveness of this approach in minimising the risk of unauthorised access and ensuring data integrity in industrial ecosystems.

Scientific novelty. The scientific novelty of the research lies in developing an adaptive model to implement the Zero Trust architecture in heterogeneous IIoT environments, which, unlike existing approaches, accounts for the strict latency constraints of industrial automation protocols

Т4. №6(38)’2026 https://doi.org/10.32782/2786-9024/v4i6(38).359304

and the specifics of the OT equipment life cycle. A method for dynamically calculating the trust level (Trust Score) for industrial controllers and sensors is proposed, based not only on static identification attributes but also on real-time behavioural analysis of the technological process.

Results. The work forms a holistic conceptual and methodological model for implementing Zero-Trust architecture for Industrial IoT in the context of IT/OT convergence, combining asset and data flow identification, micro-segmentation, continuous verification of subjects/devices, and context-adaptive access control. A set of critical control points (policy enforcement points) for typical IIoT chains “field devices – gateways – edge/SCADA – analytical services” is specified, and a consistent telemetry profile is proposed for assessing trust in nodes (device posture), taking into account OT constraints on latency and determinism. A practice-oriented procedure for “Zero-Trust-Inventory” for mixed-protocol environments (including industrial ones) has been developed, which allows formalizing access policies at the level of minimally necessary privileges and linking them to roles, functions, device state, and network context. Additionally, mechanisms for secure interaction between IT and OT domains through trust gateways have been substantiated, and an approach to phased migration from the perimeter model to Zero Trust without disrupting technological processes has been proposed.It has been shown that the most effective combination for IIoT is: (i) segmentation by technological contours, (ii) strong management of machine subject identities (certificates/attestation), (iii) constant behaviour monitoring, and (iv) automated response to policy deviations. The results obtained form the basis for creating a unified profile of Zero-Trust maturity requirements for critical IIoT systems. They are suitable for use when designing or modernising convergent IT/OT infrastructure.

Conclusions. Zero-Trust architecture is a methodologically sound response to specific IIoT threats, which are exacerbated by IT/OT convergence and the growth of heterogeneous devices and interaction channels. Adequate protection of critical IIoT infrastructure is achieved not by declarative “zero trust”, but by the systematic implementation of managed policy enforcement points, micro-segmentation and continuous access context verification. The model, inventory procedure, and telemetry profile proposed in the article enable alignment of cybersecurity requirements with the technological limitations of OT environments (determinism, availability, limited node resources), minimising the risk of process downtime. The transition to Zero Trust should be implemented in stages, starting with critical areas and the riskiest inter-domain interactions, and then expanding policies to the entire device and service life cycle.

Keywords: *Zero-Trust, IIoT, micro-segmentation, convergence, cyber resilience.*

REFERENCES

[1] A. Alagappan, S. K. Venkatachary, and L. J. B. Andrews, “Augmenting zero trust network architecture to enhance security in virtual power plants,” Energy Rep., vol. 8, pp. 123–134, 2022. DOI: 10.1016/j.egyr.2021.11.272.

[2] C. Zanasi, F. Magnanini, S. Russo, and M. Colajanni, “A zero trust approach for the cybersecurity of industrial control systems,” in Proc. 2022 IEEE 21st Int. Conf. Netw.-Based Inf. Syst. (NBiS), 2022, pp. 1–6. DOI: 10.1109/NCA57778.2022.10013559.

[3] M. Fogli, C. Giannelli, E. Mari, and C. Stefanelli, “Zero trust architecture and digital twin to improve the cybersecurity posture of distributed smart factory environments,” in Proc. 2025 IEEE Int. Conf. Distrib. Comput. Smart Syst. Internet Things (DCOSS-IoT), 2025, pp. 1–8. DOI: 10.1109/DCOSS-IoT65416.2025.00115.

[4] K. G. Crowther, “Blending shared responsibility and zero trust to secure the industrial Internet of Things,” IEEE Secur. Privacy, vol. 22, no. 5, pp. 45–52, 2024. DOI: 10.1109/MSEC.2024.3432208.

[5] B. Yasotha, V. Thiagarajan, P. Thirumoorthy, S. Priya, S. Sasidaran, and S. B. Prakalya, “Enabling protection for critical infrastructure through security and privacy in the industrial Internet of Things,” in Proc. 2024 Int. Conf. Commun., Energy Elect. Eng. (ICCEEE), 2024, pp. 1–6. DOI: 10.1109/ICCES63552.2024.10859918.

[6] A. Farraj, “On using zero trust to securing industrial control systems in the power systems industry,” in Proc. 2025 IEEE Texas Power Energy Conf. (TPEC), 2025, pp. 1–6. DOI: 10.1109/TPEC63981.2025.10906998.

[7] F. Lv et al., “Asynchronous federated learning based zero trust architecture for the next generation industrial control systems,” Comput. Netw., vol. 252, Art. 111459, 2025. DOI: 10.1016/j.comnet.2025.111459.

[8] G. Sunkara, “Implementing zero trust architecture in modern enterprise networks,” Samriddhi: J. Phys. Sci., Eng. Technol., vol. 17, no. 3, pp. 1–10, 2025. DOI: 10.18090/samriddhi.v17i03.01.

[9] H. Al-Balasmeh, “Zero trust architecture for IoT device ecosystems,” Research Square, 2025. DOI: 10.14419/r30vpf59 (preprint/platform).

[10] S. Mushtaq, M. Mohsin, and M. M. Mushtaq, “A systematic literature review on the implementation and challenges of zero trust architecture across domains,” Sensors, vol. 25, no. 19, Art. 6118, 2025. DOI: 10.3390/s25196118.

[11] S. L. Narra, “Demystifying zero trust architecture: Why it’s not just a buzzword,” Int. J. Comput. Eng., vol. 6, no. 1, pp. 1–15, 2025. DOI: 10.47941/ijce.2955.

[12] H. Zhang, Z. Zhang, and L. Chen, “Toward zero trust in 5G industrial Internet collaboration systems,” Digit. Commun. Netw., 2025. DOI: 10.1016/j.dcan.2024.03.011.

[13] C. Giannelli and M. Picone, “Editorial ‘Industrial IoT as IT and OT convergence: Challenges and opportunities’,” IoT, vol. 3, no. 1, pp. 14–17, 2022. DOI: 10.3390/iot3010014.

[14] B. Zahran, A. Hussaini, and A. Ali-Gombe, “Security of IT/OT convergence: Design and implementation challenges,” arXiv:2302.09426, 2023. DOI: 10.48550/arXiv.2302.09426.
[15] S. M. Abdullahi and S. Lazarova-Molnar, “On the adoption and deployment of secure and privacy-preserving IIoT in smart manufacturing: A comprehensive guide with recent advances,” Int. J. Inf. Secur., 2025. DOI: 10.1007/s10207-024-00951-8.
[16] T. Kampa, C. K. Muller, and D. Grossmann, “Interlocking IT/OT security for edge cloud-enabled manufacturing,” Ad Hoc Netw., vol. 150, Art. 103384, 2023. DOI: 10.1016/j.adhoc.2023.103384.

Дата першого надходження статті до видання: 04.02.2026
Дата прийняття статті до друку після рецензування: 27.02.2026
Дата публікації (оприлюднення) статті: 12.05.2026