СРАВНИТЕЛЕН АНАЛИЗ НА АРХИТЕКТУРНИ МОДЕЛИ ЗА СИГУРНА КОМУНИКАЦИЯ МЕЖДУ ERP И SCADA СИСТЕМИ В IOT-БАЗИРАНИ ПРЕДПРИЯТИЯ

Христо Светославов Христов
Технически университет - Варна, Докторант

Резюме: *Настоящата статия разглежда проблема за сигурната комуникация между системите за планиране на ресурсите на предприятието (Enterprise Resource Planning - ERP) и системите за надзорно управление и събиране на данни (Supervisory Control and Data Acquisition - SCADA) в предприятия, базирани на Интернет на нещата (Internet of Things - IoT). Извършен е сравнителен анализ на три широко използвани архитектурни модела - референтния модел на Пърдю (Purdue Enterprise Reference Architecture - PERA), модел с индустриална демилитаризирана зона (Industrial Demilitarized Zone - IDMZ) и архитектурата „Нулево доверие“ (Zero Trust Architecture - ZTA). Анализът е проведен по критерии, свързани със сигурността, мащабируемостта, оперативната съвместимост и производителността на комуникационната инфраструктура. За оценяване на архитектурните модели е разработена методика, основана на качествен анализ на техните характеристики и комплексна оценка по предварително дефинирани критерии. Получените резултати показват, че архитектурите, базирани на принципите на „Нулево доверие“, осигуряват по-високо ниво на защита и по-добра адаптивност към динамичните изисквания на индустриалните IoT среди. На тази основа са формулирани изводи относно приложимостта на разглежданите архитектурни модели при интеграцията между ERP и SCADA системи в съвременните предприятия.*

Ключови думи: *сравнителен анализ, архитектурни модели, сигурна комуникация, системи за планиране на ресурсите на предприятието, системи за надзорно управление и събиране на данни, интернет на нещата*

COMPARATIVE ANALYSIS OF ARCHITECTURAL MODELS FOR SECURE COMMUNICATION BETWEEN ERP AND SCADA SYSTEMS IN IOT-BASED ENTERPRISES

Hristo Svetoslavov Hristov
Technical University - Varna, PhD Student

Abstract: *This paper addresses the problem of secure communication between Enterprise Resource Planning (ERP) systems and Supervisory Control and Data Acquisition (SCADA) systems in enterprises based on the Internet of Things (IoT). A comparative analysis of three widely adopted architectural models is conducted, namely the Purdue Enterprise Reference Architecture (PERA), the Industrial Demilitarized Zone (IDMZ) model, and the Zero Trust Architecture (ZTA). The analysis is performed using criteria related to security, scalability, interoperability, and communication infrastructure performance. To evaluate the architectural models, a methodology*

based on qualitative analysis of their characteristics and a comprehensive assessment using predefined criteria is developed. The results indicate that architectures based on Zero Trust principles provide a higher level of security and greater adaptability to the dynamic requirements of industrial IoT environments. Based on these findings, conclusions are drawn regarding the applicability of the examined architectural models for the integration of ERP and SCADA systems in modern enterprises.

Keywords: *comparative analysis, architectural models, secure communication, Enterprise Resource Planning systems, Supervisory Control and Data Acquisition systems, Internet of Things*

1. Увод

С нарастващото използване на Интернет на нещата (Internet of Things – IoT) в индустриалните предприятия се увеличава необходимостта от надежден и сигурен обмен на данни между корпоративните и производствените информационни системи. В тази среда интеграцията между корпоративните и производствените информационни системи, включително ERP, MES и SCADA, има ключова роля за осигуряване на ефективно управление на производствените процеси и обмен на информация между отделните нива на индустриалната инфраструктура (Mičieta et al., 2026; HaddadPajouh et al., 2021).

Вертикалната интеграция между корпоративните и производствените информационни системи позволява автоматизирано взаимодействие между бизнес процесите и производствените операции, като осигурява своевременен обмен на данни и подпомага вземането на управленски решения (Mičieta et al., 2026). Същевременно свързаността между корпоративните и индустриалните мрежи поражда редица предизвикателства, свързани със сигурността на комуникацията, защитата на данните и надеждността на информационния обмен (Rose et al., 2020; Santos Jr. et al., 2024). За осигуряване на сигурна комуникация между ERP и SCADA системите в практиката се използват различни архитектурни модели. Сред най-разпространените са референтният модел на Пърдю (Purdue Enterprise Reference Architecture – PERA), моделът с индустриална демилитаризирана зона (Industrial Demilitarized Zone – IDMZ) и архитектурата „Нулево доверие“ (Zero Trust Architecture – ZTA) (Schachinger et al., 2026; Mosteiro-Sanchez et al., 2020; Rose et al., 2020). Тези модели предлагат различни подходи за сегментация на мрежата, защита на комуникационните потоци и управление на достъпа до информационни ресурси (Sain et al., 2026; Plattform Industrie 4.0, 2024).

През последните години архитектурите, базирани на принципа „Нулево доверие“, се утвърждават като перспективен подход за защита на индустриалните IoT среди, благодарение на механизмите за непрекъсната автентикация, контрол на достъпа и ограничаване на латералното придвижване на потенциални нарушители в мрежата (Liu et al., 2024; Cao et al., 2024; Rose et al., 2020). Независимо от широкото им приложение, между

отделните архитектурни решения съществуват съществени различия по отношение на сигурността, мащабируемостта, оперативната съвместимост и производителността на комуникационната инфраструктура. Това налага провеждането на сравнителен анализ, който да подпомогне избора на подходящ архитектурен модел в зависимост от специфичните изисквания на предприятията.

Целта на настоящото изследване е да бъде извършен сравнителен анализ на архитектурни модели за сигурна комуникация между ERP и SCADA системи в IoT-базирани предприятия. За постигането на тази цел са анализирани моделът на Пърдю, моделът с индустриална демилитаризирана зона и архитектурата „Нулево доверие“, като оценяването е извършено по критерии, свързани със сигурността, мащабируемостта, оперативната съвместимост и производителността на комуникационната инфраструктура.

2. Анализ на съвременните изследвания и архитектурни подходи

Развитието на индустриалния Интернет на нещата променя традиционния модел на взаимодействие между корпоративните и производствените информационни системи. Нарастващият брой свързани устройства, необходимостта от обмен на данни в реално време и интеграцията между ERP и SCADA системи създават предпоставки за повишаване на ефективността на производствените процеси, но едновременно с това увеличават рисковете, свързани с киберсигурността. В тази връзка редица изследвания са насочени към разработване на архитектурни решения, които да осигурят сигурен обмен на информация между корпоративните и индустриалните среди (Mosteiro-Sanchez et al., 2020; HaddadPajouh et al., 2021; Shtayat et al., 2023; Plattform Industrie 4.0, 2024).

В научната литература се отбелязва, че преминаването от традиционни изолирани SCADA системи към силно свързани IoT екосистеми води до разширяване на комуникационните връзки между производствените и корпоративните мрежи (Plattform Industrie 4.0, 2024). Интегрирането на облачни услуги, IoT устройства и индустриални комуникационни платформи създава възможности за централизирано управление и обработка на данни, но едновременно с това поставя по-високи изисквания към механизмите за защита на комуникацията и управлението на достъпа (HaddadPajouh et al., 2021). За организиране на комуникацията между различните нива на индустриалните системи традиционно се използват архитектури, базирани на Purdue Enterprise Reference Architecture (PERA). Моделът предлага йерархична структура за разделяне на корпоративните и производствените процеси, като по този начин улеснява управлението на информационните потоци и прилагането на политики за сигурност. Подобен подход е заложен и в редица индустриални стандарти, включително IEC 62443 и ISA/IEC 62443, които дефинират добри практики за сегментация и защита на индустриалните комуникационни мрежи (International Electrotechnical Commission, 2020; International

Society of Automation, 2024). С развитието на индустриалните мрежи и необходимостта от по-висока степен на изолация между отделните функционални области се утвърждават архитектурите с индустриална демилитаризирана зона (Industrial Demilitarized Zone - IDMZ). Този подход се основава на изграждането на междинна защитена зона между корпоративната и индустриалната инфраструктура, чрез която се осъществява контролираният обмен на данни. По този начин се ограничава директната комуникация между отделните мрежови сегменти и се намалява рискът от разпространение на инциденти към критични производствени системи (Mosteiro-Sanchez et al., 2020; International Electrotechnical Commission, 2020; Stouffer et al., 2023).

Паралелно с развитието на традиционните модели все по-широко приложение намират архитектурите от тип „Нулево доверие“ (Zero Trust Architecture - ZTA). Архитектурата „Нулево доверие“ е систематизирана в NIST SP 800-207 от Роуз, Борчърт, Мичъл и Конъли (Rose et al., 2020) и се основава на принципа, че нито един потребител, устройство или услуга не следва да се считат за надеждни по подразбиране. Последващи изследвания разглеждат възможностите за прилагане на този подход в индустриални среди чрез използване на механизми за непрекъсната автентикация, динамично управление на достъпа и микросегментация на мрежата (Liu et al., 2024; Mirani et al., 2022; Paul & Rao, 2023; Plattform Industrie 4.0, 2024). Особено внимание се отделя на приложението на Zero Trust архитектурите в IoT среди, характеризиращи се с голям брой взаимосвързани устройства и динамично променящи се комуникационни взаимоотношения (Mirani et al., 2022; Plattform Industrie 4.0, 2024). В тази насока Цао и съавтори (Cao et al., 2024) разглеждат възможностите за автоматизация и оркестрация на архитектурата „Нулево доверие“, включително механизмите за удостоверяване и контрол на достъпа при нейното внедряване в реални мрежови среди. Допълнително Лиу и съавтори (Liu et al., 2024) подчертават значението на архитектурите от тип Zero Trust за изграждане на сигурни корпоративни IoT екосистеми, като акцентират върху необходимостта от непрекъсната верификация на потребителите, устройствата и комуникационните връзки. Подобни изследвания са представени и от Сантос и съавтори (Santos Jr. et al., 2024), които разглеждат прилагането на принципите на архитектурата „Нулево доверие“ за защита на комуникацията между програмируеми логически контролери (PLC) и SCADA приложение. Авторите изследват защитата на информационния обмен при допускане, че индустриалната мрежа може да бъде компрометирана, като използват криптографски механизми и проверка на комуникацията между участващите мрежови компоненти.

Разгледаните източници показват наличието на различни подходи за осигуряване на сигурна комуникация между корпоративните и индустриалните системи. Съществуващите изследвания са насочени както към усъвършенстване на традиционните архитектури, базирани на йерархична сегментация, така и към внедряване на нови модели, основани на

принципите на Zero Trust. Независимо от това по-голямата част от източниците разглеждат отделни архитектурни решения или конкретни аспекти на сигурността, без да предлагат единна рамка за сравнителна оценка на архитектурите PERA, IDMZ и ZTA по отношение на сигурността, мащабируемостта, оперативната съвместимост и производителността на комуникационната инфраструктура.

3. Методика на сравнителния анализ

Сравнителният анализ на архитектурните модели за сигурна комуникация между ERP и SCADA системи има за цел да осигури обективна оценка на тяхната приложимост в IoT-базирани предприятия. За тази цел е разработена методика, основана на набор от критерии, които отразяват основните изисквания към комуникационната инфраструктура в съвременните индустриални среди. Изборът на критериите е съобразен с особеностите на интеграцията между корпоративните и производствените системи, както и с изискванията, формулирани в стандартите IEC 62443 и ISA/IEC 62443 за защита на индустриалните комуникационни мрежи (International Electrotechnical Commission, 2013; International Electrotechnical Commission, 2020; International Society of Automation, 2024). Изборът на критериите е основан и на най-често използваните показатели за оценка на индустриални комуникационни архитектури, идентифицирани в разгледаните литературни източници (Mosteiro-Sanchez et al., 2020; Mirani et al., 2022; Sain et al., 2026; Rose et al., 2020; Schachinger et al., 2026). Анализът обхваща трите архитектурни модела, разгледани в предходния раздел – Purdue Enterprise Reference Architecture (PERA), Industrial Demilitarized Zone (IDMZ) и Zero Trust Architecture (ZTA).

За оценяване на архитектурните модели са избрани четири критерия, които характеризират основните изисквания към сигурната комуникация между ERP и SCADA системи в IoT-базирани предприятия. Критерият „Сигурност“ характеризира способността на архитектурния модел да ограничава неоторизирания достъп до информационните ресурси, да осигурява сегментация на комуникационната инфраструктура и да намалява риска от разпространение на киберинциденти между корпоративната и индустриалната мрежа. Критерият „Мащабируемост“ оценява възможността за разширяване на комуникационната инфраструктура чрез добавяне на нови устройства, услуги и комуникационни връзки без необходимост от съществени промени в архитектурния модел. Критерият „Оперативна съвместимост“ отразява способността на архитектурния модел да осигурява взаимодействие между различни хардуерни и софтуерни платформи, както и интеграция между ERP и SCADA системи. Критерият „Производителност“ оценява влиянието на архитектурния модел върху обмена на данни в реално време и способността му да поддържа необходимото ниво на комуникационна ефективност при нарастване на натоварването. За осигуряване на сравнимост между резултатите е използвана петстепенна оценъчна скала, представена в Таблица 1.

Таблица 1

Интерпретация на оценъчната скала

Оценка	Интерпретация	Характеристика
1	Много ниско ниво	Архитектурата осигурява ограничено покриване на съответния критерий
2	Ниско ниво	Налични са базови механизми, но със съществени ограничения
3	Средно ниво	Критерият е удовлетворен в приемлива степен, но съществуват ограничения
4	Високо ниво	Архитектурата осигурява добро покриване на критерия при незначителни ограничения
5	Много високо ниво	Архитектурата осигурява пълно или почти пълно покриване на критерия

Оценките се определят въз основа на характеристиките на архитектурните модели, описани в научната литература и приложимите индустриални стандарти (Paul & Rao, 2023; Plattform Industrie 4.0, 2024; Rose et al., 2020; Santos Jr. et al., 2024; Schachinger et al., 2026). Оценяването се извършва чрез качествен анализ на характеристиките на разглежданите архитектури, като всяка оценка отразява степента на съответствие на архитектурния модел с дефинираните критерии. Използването на единна оценъчна скала позволява извършването на съпоставим анализ между различните архитектурни подходи. Прилагането на оценъчната скала цели да намали субективността при сравнението на архитектурните модели чрез използване на единни критерии и предварително дефинирани нива на оценяване. По този начин се осигурява възможност за последващо количествено сравнение на разглежданите архитектури и формиране на комплексна оценка за тяхната приложимост в IoT-базирани предприятия.

3.1 Комплексна оценка на архитектурните модели

Всички критерии се разглеждат като равнозначни и участват с еднаква тежест при формирането на комплексната оценка. Това допускане е направено с цел осигуряване на съпоставимост между резултатите и избягване на допълнителна субективност при определяне на тегловни коефициенти. За обобщаване на резултатите от сравнителния анализ е използван комплексен показател К, който се определя като средноаритметична стойност на оценките по отделните критерии:

$$K = \frac{(S + M + O + P)}{4}, \quad (1)$$

където:

- S е оценка по критерий: Сигурност;
- M е оценка по критерий: Мащабируемост;
- O е оценка по критерий: Оперативна съвместимост;
- P е оценка по критерий: Производителност.

Получената стойност на показателя K позволява количествено сравнение между разглежданите архитектурни модели и определяне на тяхната обща приложимост за изграждане на сигурна комуникационна инфраструктура между ERP и SCADA системи в IoT-базирани предприятия. Разработената методика създава единна основа за оценяване на архитектурите PERA, IDMZ и ZTA и позволява последващото извършване на сравнителен анализ по предварително дефинирани критерии.

4. Сравнителен анализ на архитектурните модели

Архитектурните модели PERA, IDMZ и ZTA са сред най-разпространените подходи за осигуряване на сигурна комуникация между корпоративните и индустриалните информационни системи. Независимо че всички модели са насочени към защита на обмена на данни между ERP и SCADA системи, те използват различни принципи за сегментация на мрежата, управление на достъпа и контрол на комуникационните потоци.

Референтният модел Purdue Enterprise Reference Architecture (PERA) се основава на йерархична организация на комуникационната инфраструктура, при която корпоративните и производствените системи са разделени в отделни функционални нива (International Electrotechnical Commission, 2020; Stouffer et al., 2023; Schachinger et al., 2026). Основно предимство на този подход е ясното структуриране на информационните потоци и възможността за централизирано управление на комуникацията между отделните слоеве. В същото време архитектурата е разработена в условията на ограничена свързаност между информационните системи и не отчита в пълна степен динамичния характер на съвременните IoT среди. Това води до ограничени възможности за детайлен контрол на достъпа и управление на комуникацията на ниво устройство или услуга.

Архитектурата с индустриална демилитаризирана зона (IDMZ) представлява развитие на класическите принципи за мрежова сегментация чрез въвеждане на междинна защитена зона между корпоративната и производствената инфраструктура (International Electrotechnical Commission, 2020; Stouffer et al., 2023). Този подход намалява риска от директно проникване към критични производствени ресурси и позволява по-добър контрол върху обмена на данни между различните функционални области. Независимо от това внедряването на IDMZ е свързано с допълнителни комуникационни компоненти и по-

висока административна сложност, което може да затрудни разширяването и управлението на инфраструктурата при голям брой свързани устройства.

За разлика от традиционните модели за организация на индустриалните комуникации, архитектурата „Нулево доверие“ (ZTA) се основава на принципа, че нито един потребител, устройство или комуникационна връзка не следва да бъдат считани за надеждни по подразбиране (Rose et al., 2020). Използването на механизми за непрекъсната автентикация, микросегментация и управление на достъпа на базата на идентичност позволява ограничаване на възможностите за неоторизиран достъп и разпространение на заплахи между отделните сегменти на мрежата (Liu et al., 2024; Paul & Rao, 2023; Plattform Industrie 4.0, 2024). Тези характеристики правят архитектурата особено подходяща за среди с голям брой IoT устройства и динамично променящи се комуникационни взаимоотношения. Основно ограничение на подхода е по-високата сложност при внедряване и необходимостта от допълнителни механизми за управление на идентичности и политики за достъп.

Въз основа на разгледаните характеристики е извършена сравнителна оценка на архитектурните модели по критериите, дефинирани в раздел 3. Оценките в Таблица 2 са определени чрез сравнителен качествен анализ на конкретни технически характеристики на разглежданите архитектурни модели. За всеки критерий са отчетени механизмите за мрежова сегментация, контрол на достъпа, изолиране на комуникационните зони, управление на идентичности, възможности за разширяване на инфраструктурата, взаимодействие между разнородни системи и влиянието на допълнителните защитни механизми върху комуникационните процеси. Оценяването се основава на характеристиките, описани в приложимите стандарти IEC 62443, NIST SP 800-82 и NIST SP 800-207, както и в разгледаните научни публикации. Стойностите по петстепенната скала представляват сравнителна качествена оценка, а не резултати от експериментално измерване.

Таблица 2

Сравнителна оценка на архитектурните модели

Критерий	PERA	IDMZ	ZTA
Сигурност	3	4	5
Мащабируемост	3	3	4
Оперативна съвместимост	4	4	4
Производителност	5	4	4

По критерий „Сигурност“ PERA получава оценка 3, тъй като йерархичното разделяне на корпоративните и производствените нива създава основа за мрежова сегментация, но самият модел не дефинира детайлни механизми за удостоверяване,

динамично управление на достъпа и непрекъсната проверка на комуникационните участници. IDMZ получава оценка 4, тъй като въвеждането на междинна защитена зона между корпоративната и производствената инфраструктура ограничава директния обмен на данни и позволява прилагане на защитни стени, контролирани комуникационни канали и междинни услуги, в съответствие с принципите за сегментация на индустриалните мрежи, разглеждани в IEC 62443 и NIST SP 800-82. ZTA получава оценка 5 поради използването на принципа за липса на подразбиращо се доверие, проверка на идентичността, минимални права за достъп, микросегментация и динамично управление на политиките за достъп (International Electrotechnical Commission, 2020; Stouffer et al., 2023; Rose et al., 2020; Paul & Rao, 2023).

По критерий „Мащабируемост“ PERA получава оценка 3, тъй като йерархичната структура позволява структурирано разширяване, но създава ограничения при динамично променящи се комуникационни връзки и голям брой IIoT компоненти. IDMZ също получава оценка 3, тъй като добавянето на нови системи и услуги може да изисква промяна на правилата за филтриране, допълнителни комуникационни връзки и управление на междинните защитни компоненти. ZTA получава оценка 4, тъй като идентичностно ориентираното управление на достъпа позволява по-гъвкаво включване на нови потребители, устройства и услуги. Не е присъдена максимална оценка поради повишените изисквания към управлението на идентичности, политики и голям брой разнородни IoT устройства (Mirani et al., 2022; Liu et al., 2024; Cao et al., 2024).

По критерий „Оперативна съвместимост“ трите архитектури получават оценка 4. Нито един от разглежданите модели не е ограничен до конкретен приложен комуникационен протокол и те могат да бъдат използвани при интеграция на различни ERP, SCADA и IIoT компоненти. Реалната оперативна съвместимост обаче зависи и от използваните комуникационни протоколи, интерфейси, шлюзове и софтуерни реализации, поради което на архитектурните модели не е присъдена максимална оценка (Mirani et al., 2022; Sain et al., 2026).

По критерий „Производителност“ PERA получава оценка 5 поради сравнително пряката и ясно структурирана организация на комуникационните потоци и липсата на задължителни допълнителни проверки при всяка комуникационна заявка. IDMZ получава оценка 4, тъй като преминаването на трафика през защитни стени, прокси услуги и други междинни компоненти може да въведе допълнително комуникационно закъснение. ZTA също получава оценка 4, тъй като удостоверяването, проверката на политиките и прилагането на контрол върху отделните комуникационни сесии създават допълнително изчислително и комуникационно натоварване (Stouffer et al., 2023; Liu et al., 2024; Sain et al., 2026).

Направените оценки показват, че отделните архитектурни модели имат различни силни страни и ограничения. Следователно стойностите в Таблица 2 следва да се

разглеждат като сравнителни качествени оценки, получени въз основа на конкретните технически характеристики на архитектурите и литературните източници, а не като абсолютни или експериментално измерени показатели.

За обобщаване на резултатите е изчислена комплексната оценка К съгласно формула (1). Получените стойности са представени в Таблица 3.

Таблица 3

Комплексна оценка на архитектурните модели

Архитектура	К
PERA	3,75
IDMZ	3,75
ZTA	4,25

Комплексната оценка, представена в Таблица 3, показва различия в степента на съответствие на разглежданите архитектурни модели спрямо предварително дефинираните критерии за оценка. Най-висока стойност на показателя К е получена за архитектурата ZTA (К = 4,25), което се дължи на високите оценки по критериите „Сигурност“ и „Мащабируемост“. Този резултат отразява способността на архитектурата да осигурява детайлен контрол на достъпа, микросегментация на комуникационната инфраструктура и ефективно управление на голям брой взаимосвързани устройства, характерни за съвременните IoT-базирани предприятия. Архитектурите PERA и IDMZ получават еднаква комплексна оценка (К = 3,75), но постигат този резултат чрез различни комбинации от характеристики. При PERA по-високата оценка по критерия „Производителност“ компенсира по-ниските оценки по критериите „Сигурност“ и „Мащабируемост“. От своя страна архитектурата IDMZ демонстрира по-добри характеристики по отношение на сигурността благодарение на допълнителната изолация между корпоративната и производствената среда, но за сметка на по-висока инфраструктурна сложност и ограничена гъвкавост при разширяване на системата. Получените резултати показват, че изборът на архитектурен модел не следва да се основава единствено на стойността на комплексния показател, а трябва да отчита и спецификата на конкретната индустриална среда. В среди с високи изисквания за киберсигурност и голям брой свързани устройства архитектурите, базирани на принципите на Zero Trust, предлагат по-добри възможности за адаптация и защита. В същото време архитектурите PERA и IDMZ остават приложими при инфраструктури с ясно дефинирани комуникационни потоци, по-ниска динамика на мрежовата среда и необходимост от поддържане на висока производителност на комуникационните процеси.

5. Заключение

Извършеният сравнителен анализ на архитектурните модели PERA, IDMZ и ZTA показва, че те притежават различни предимства и ограничения при осигуряването на сигурна комуникация между ERP и SCADA системи в IoT-базирани предприятия. PERA осигурява ясно функционално и йерархично разделяне на корпоративните и производствените системи, IDMZ въвежда контролирана защитена зона между корпоративната и индустриалната инфраструктура, а ZTA допълва тези механизми чрез идентичностно ориентиран контрол на достъпа, минимални права, микросегментация и непрекъсната проверка на комуникационните участници.

Получените резултати показват по-висока комплексна оценка за ZTA поради по-доброто покриване на критериите, свързани със сигурността и адаптивността към динамични IoT среди. Това обаче не означава, че разглежданите архитектури следва да бъдат прилагани като взаимно изключващи се решения. Техните принципи и механизми могат да бъдат използвани съвместно, като PERA служи за функционално структуриране на корпоративната и производствената инфраструктура, IDMZ осигурява защитен комуникационен слой между тях, а принципите на Zero Trust позволяват детайлен контрол на достъпа до отделните системи, услуги и устройства.

По този начин съвместното им прилагане позволява да бъдат съчетани предимствата на йерархичната сегментация, защитата на границата между IT и OT средите и динамичния контрол на достъпа. Следователно при реални индустриални среди е възможно изграждането на комбинирана архитектура, която използва елементи на PERA, IDMZ и ZTA в зависимост от конкретните технологични, комуникационни и организационни изисквания. Бъдещо развитие на изследването може да бъде насочено към разработване и експериментално валидиране на подобен комбиниран архитектурен модел.

Използвана литература:

1. Liu, C., R. Tan, Y. Wu, Y. Feng, Z. Jin, F. Zhang, Y. Liu, Q. Liu. Dissecting Zero Trust: Research Landscape and Its Implementation in IoT. Cybersecurity, Vol. 7, 2024, Article 20. DOI: 10.1186/s42400-024-00212-0.
2. Mosteiro-Sanchez, A., M. Barcelo, J. Astorga, A. Urbieta. Securing IIoT Using Defence-in-Depth: Towards an End-to-End Secure Industry 4.0. Journal of Manufacturing Systems, Vol. 57, 2020, pp. 367–378. DOI: 10.1016/j.jmsy.2020.10.011.
3. Mirani, A. A., G. Velasco-Hernandez, A. Awasthi, J. Walsh. Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. Sensors, Vol. 22, No. 15, 2022, 5836. DOI: 10.3390/s22155836.

4. Mičieta, B., V. Biňasová, M. Gašo, D. Hanzlovič. MES Utilisation Within Intelligent Manufacturing Systems: A Hierarchical Integration Framework and KPI-Based Verification. Sustainability, Vol. 18, No. 13, 2026, 6887. DOI: 10.3390/su18136887.
5. HaddadPajouh, H., A. Dehghantanha, R. M. Parizi, M. Aledhari, H. Karimipour. A Survey on Internet of Things Security: Requirements, Challenges, and Solutions. Internet of Things, Vol. 14, 2021, 100129. DOI: 10.1016/j.iot.2019.100129.
6. International Electrotechnical Commission. IEC 62443-3-3:2013. Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels. Geneva, Switzerland, 2013.
7. International Society of Automation. ANSI/ISA-62443-2-1-2024. Security for Industrial Automation and Control Systems – Part 2-1: Security Program Requirements for IACS Asset Owners. Research Triangle Park, NC, USA, 2024.
8. Shtayat, M. M., M. K. Hasan, R. Sulaiman, S. Islam, A. U. R. Khan. An Explainable Ensemble Deep Learning Approach for Intrusion Detection in Industrial Internet of Things. IEEE Access, Vol. 11, 2023, pp. 115047–115061. DOI: 10.1109/ACCESS.2023.3323573.
9. Sain, D., T. Rosenstatter, O. Saßnick, C. Schäfer, S. Huber. Secure Data Bridging in Industry 4.0: An OPC UA Aggregation Approach for Including Insecure Legacy Systems. IEEE Access, Vol. 14, 2026, pp. 72414–72433. DOI: 10.1109/ACCESS.2026.3691926.
10. Paul, B., M. Rao. Zero-Trust Model for Smart Manufacturing Industry. Applied Sciences, Vol. 13, No. 1, 2023, 221. DOI: 10.3390/app13010221.
11. Plattform Industrie 4.0. Zero Trust and Industrie 4.0: Perspectives from the Use of ML. Berlin: Federal Ministry for Economic Affairs and Climate Action, 2024.
12. Cao, Y., S. R. Pokhrel, Y. Zhu, R. Doss, G. Li. Automation and Orchestration of Zero Trust Architecture: Potential Solutions and Challenges. Machine Intelligence Research, Vol. 21, 2024, pp. 294–317. DOI: 10.1007/s11633-023-1456-2.
13. Rose, S., O. Borchert, S. Mitchell, S. Connelly. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020. DOI: 10.6028/NIST.SP.800-207.
14. Santos Jr., R., F. G. Cabral, P. M. M. Lima. Zero-Trust Security Implementation for Industrial Networks. Congresso Brasileiro de Automática – CBA 2024, Vol. 4, No. 1, 2024. DOI: 10.20906/CBA2024/4237.
15. Schachinger, F.-K., T. Rosenstatter, U. Pache. PURITY – An Industry-Standard-Based Security Framework for IT-OT Convergence. IEEE Access, Vol. 14, 2026, pp. 57014–57032. DOI: 10.1109/ACCESS.2026.3682366.
16. Stouffer, K., M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule, M. Thompson. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-82r3.
17. International Electrotechnical Commission. IEC 62443-3-2:2020. Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design. Geneva, Switzerland, 2020.