INTELLIGENT SYSTEM FOR EARLY INCIDENT DETECTION THROUGH AI VIDEO ANALYSIS AND IoDT SENSORS*

SILVIA H. NIKOLOVA

ABSTRACT: *Early detection of critical events is a fundamental requirement for modern monitoring, control and protection systems in industrial facilities, critical infrastructure, warehouse complexes and public spaces. Conventional solutions typically use standalone video cameras or specialized physical sensors, which limits reliability under adverse conditions, partial failures and complex emergency scenarios. This paper presents an architecture and algorithmic model of an intelligent system for early detection of fires, unauthorized intrusion and industrial accidents through the combined analysis of video streams and data from IoDT (Internet of Digital Things) sensors. The proposed system integrates AI video cameras, thermal imaging devices, and temperature, smoke, gas, vibration, motion and access-control sensors. Data are processed through computer vision, time-series analysis and multisensor fusion algorithms. The solution uses dynamic reliability assessment of individual channels, probabilistic incident estimation and multilevel alarm confirmation. Simulation results show that the combined AI + IoDT approach achieves an average accuracy of 98.1%, compared with 91.8% for video-only analysis. The integrated model reaches an AUC of 0.988, demonstrating that heterogeneous sensor fusion improves detection reliability and enables automated response to critical events.*

KEYWORDS: *artificial intelligence, video analytics, IoDT, sensor fusion, early detection, fire, intrusion, industrial accident, Edge AI*

DOI: https://doi.org/10.46687/MT26SHK

ИНТЕЛИГЕНТНА СИСТЕМА ЗА РАННО ОТКРИВАНЕ НА ИНЦИДЕНТИ ЧРЕЗ AI АНАЛИЗ НА ВИДЕО И IoDT СЕНЗОРИ

СИЛВИЯ Х. НИКОЛОВА

АБСТРАКТ: *Ранното откриване на критични събития е основно изискване към съвременните системи за наблюдение, контрол и защита на индустриални обекти, критична инфраструктура, складови комплекси и обществени пространства. Традиционните решения обикновено използват самостоятелни видеокамери или специализирани физически сензори, което ограничава надеждността им при неблагоприятни условия, частични откази и сложни аварийни сценарии. Настоящият доклад представя архитектура и алгоритмичен модел на интелигентна система за ранно откриване на пожари, нерегламентирано проникване и индустриални аварии чрез комбиниран анализ на видеопотоци и данни от IoDT (Internet of Digital Things) сензори. Предложената система включва AI видеокамери, термовизионни устройства, температурни, димни, газови, вибрационни и сензори за движение и контрол на достъпа. Данните се обработват чрез алгоритми за компютърно зрение, анализ на времеви редове и мултисензорно обединяване (Sensor Fusion). Решението използва динамична оценка на надеждността на отделните канали, вероятностна оценка на инцидента и многостепенен механизъм за потвърждаване на алармите. Основната цел е намаляване на времето за откриване, повишаване на точността и ограничаване на фалшивите аларми. Симулационната оценка на разработения модел показва, че комбинираният подход AI + IoDT достига средна точност 98,1%, докато моделът, използващ само видеоанализ, достига 91,8%. Площта под ROC кривата на интегрирания модел е 0,988. Резултатите показват, че обединяването на хетерогенни сензорни източници повишава надеждността на детекцията и създава предпоставки за автоматизирана реакция при критични събития.*

* Докладът е частично финансиран по проект № РД-08-113/05.02.2026 г. „Научна конференция с международно участие МАТТЕХ 2026 – ФТН“

1 Въведение

Развитието на изкуствения интелект, компютърното зрение, разпределените сензорни мрежи и Edge изчисленията създава предпоставки за преминаване от пасивно видеонаблюдение към интелигентни системи, които не само регистрират събития, но и извършват автоматична интерпретация на наблюдаваната среда. Особено важна е възможността за ранно разпознаване на опасни процеси, преди те да достигнат критична фаза.

Съвременните индустриални и инфраструктурни обекти се характеризират с висока степен на автоматизация, разпределени технологични процеси и значителен брой взаимосвързани устройства. Възникването на пожар, изтичане на опасни вещества, повреда на оборудване или нерегламентиран достъп може да доведе до човешки жертви, материални загуби, прекъсване на производствени процеси и отрицателно въздействие върху околната среда. Състоянието на критичната инфраструктура за район Шумен е анализирано в [1], а управлението на риска за обекти и съоръжения от критичната инфраструктура е разгледано в [29].

Ефективността на защитните системи зависи не само от способността им да разпознават вече настъпил инцидент, но и от възможността да откриват неговите ранни признаци. При пожар например началните индикатори могат да бъдат локално повишаване на температурата, наличие на дим, промяна в инфрачервения спектър или поява на характерни визуални структури. При индустриална авария ранните признаци могат да включват увеличени вибрации, необичайна температура, промяна в концентрацията на газове или отклонение в движението на механични компоненти.

Класическите системи за наблюдение често работят с един тип информация. Видеосистемите зависят от осветеността, атмосферните условия, положението на камерата и наличието на препятствия. Сензорните системи могат да регистрират физическа промяна, но често не осигуряват достатъчно информация за пространственото положение и причината за събитието. Това може да доведе до фалшиви аларми, пропуснати инциденти или забавена реакция.

Интегрирането на видеоанализ и IoDT сензори позволява формиране на по-пълна и устойчива оценка на наблюдаваната среда. В настоящото изследване IoDT се разглежда като разширена екосистема от интелигентни цифрови устройства, физически сензори, комуникационни модули и изчислителни възли, които обменят данни и участват в автоматизираното вземане на решения.

Основната цел е разработването на интелигентна архитектура за ранно откриване и класифициране на три основни категории инциденти: пожари и начални признаци на възпламеняване; нерегламентирано проникване; индустриални аварии и опасни технологични отклонения. Работната хипотеза е, че комбинирането на вероятностните оценки от видеоанализа и физическите сензори може да повиши точността на детекцията и да намали броя на фалшивите аларми.

2 Анализ на проблема и свързани изследвания

Съвременните методи за визуално откриване на пожар и дим използват конволюционни невронни мрежи, едноетапни детектори, трансформър архитектури и времеви модели [3, 4, 23]. При тях основно предимство е възможността за ранно визуално разпознаване на дим и пламък преди задействане на конвенционални точкови датчици.

Въпреки това точността остава зависима от контекста, осветлението и качеството на видеопотока.

При индустриалните приложения все по-широко се използват модели за анализ на многомерни времеви редове и графови невронни мрежи, които могат да моделират взаимозависимостите между температура, налягане, вибрации и други технологични параметри [5, 11–17]. Тези подходи са подходящи за откриване на ранни аномалии, тъй като оценяват не само абсолютните стойности, но и времевите и структурните зависимости между каналите.

В областта на системите за проникване и киберфизическата сигурност се използват хибридни модели, които съчетават CNN, LSTM, GRU и feature fusion [6–10]. Макар част от тези изследвания да са насочени към мрежови прониквания, принципът за обединяване на независими признаци е приложим и при физическа защита на периметър, където видео, движение и контрол на достъпа трябва да бъдат съпоставяни.

Съвременните разработки за ранно откриване на пожар все по-често комбинират интелигентни сензори, Edge обработка и IoT комуникация [19–22]. Тази тенденция показва, че надеждността на системата може да бъде увеличена, когато локалните AI алгоритми и сензорните данни се използват съвместно, а критичните решения не зависят изцяло от централен облачен ресурс.

2.1 Ограничения на системите, базирани само на видео

Алгоритмите за компютърно зрение могат да разпознават хора, превозни средства, дим, пламък, защитно оборудване и опасни действия. Тяхната ефективност обаче се влияе от редица фактори: недостатъчна или променлива осветеност; дим, мъгла и прах; частично закриване на обектите; отражения и сенки; ниска разделителна способност; вибрации на камерата; промени във фона; непознати обекти, които не са представени в обучаващата извадка. Откриването на обекти с военно предназначение в оптични изображения е разгледано в [34], а разпознаването на частично видими обекти и използването на трансфер на знания в MATLAB са теми на [2, 33].

2.2 Ограничения на системите, базирани само на сензори

Физическите сензори осигуряват надеждно измерване на температура, дим, газова концентрация, движение и вибрации, но обикновено предоставят локална информация. Един температурен сензор може да отчете повишение, без да е възможно автоматично да се установи дали причината е пожар, работещо оборудване или външен топлинен източник. Основните ограничения включват локален обхват на измерване; необходимост от подходящо разположение; дрейф на измервателните характеристики; прекъсване на комуникацията; повреда или замърсяване на сензора; невъзможност за визуална идентификация на причината.

2.3 Необходимост от мултисензорен подход

Мултисензорното обединяване позволява информацията от различни източници да се използва взаимно за потвърждаване или отхвърляне на предполагаемо събитие. Ако видеоалгоритъмът разпознае дим, а температурният и газовият сензор едновременно регистрират отклонение, вероятността за реален пожар е значително по-висока. При нерегламентирано проникване видеоразпознаването може да бъде комбинирано с инфрачервена бариера, сензор за движение и система за контрол на достъпа. При индустриална авария вибрационните и температурните данни могат да бъдат съпоставени с визуалното състояние на оборудването.

3 Архитектура на предложената система

Предложената архитектура е организирана в четири основни слоя: слой за събиране на данни; комуникационен слой; AI аналитичен слой; слой за управление, известяване и реакция. Между сензорния и аналитичния слой е предвидена Edge обработка, която намалява латентността и позволява локално функциониране при временна загуба на връзка с централния сървър.

3.1 Слой за събиране на данни

Първият слой включва всички устройства, които наблюдават физическата среда. Видеосистемата може да съдържа стационарни AI камери, PTZ камери, термовизионни и инфрачервени устройства, както и мобилни камери върху UAV или UGV платформи. Те осигуряват информация за форма, движение, позиция, поведение и визуални признаци на възникващи инциденти. Развитието и тенденциите при интелигентните камери за машинно зрение са разгледани в [18].

IoDT подсистемата използва температурни, димни, газови, вибрационни, акустични, инфрачервени, сензори за налягане и влажност, както и RFID устройства за контрол на достъпа. Всеки възел съдържа измервателен компонент, комуникационен модул, локална логика и уникален идентификатор. Като отделно направление при сензорните приложения е предложен модел на интерактивна система, базирана на ултрашироколентови сензори [24].

3.2 Комуникационен слой

Комуникационният слой осигурява обмен на данни между сензорите, камерите, Edge устройствата и централната платформа. В зависимост от приложението могат да се използват Ethernet, Wi-Fi, 4G/5G, LoRaWAN, MQTT и индустриални комуникационни протоколи. Видеопотоците се предават чрез подходящи протоколи за мултимедийни данни, а телеметрията от сензорите може да използва publish/subscribe механизъм.

За критични системи комуникационната инфраструктура трябва да осигурява автентикация, криптиране, контрол на достъпа, регистриране на събития, резервирани маршрути и синхронизация на времето. Времевата синхронизация е съществена, защото видео- и сензорните данни трябва да бъдат съпоставени за един и същ времеви интервал.

3.3 Edge обработка

Edge устройствата се разполагат близо до източниците на данни и изпълняват част от анализа локално. Това намалява латентността и комуникационното натоварване. На Edge ниво могат да се изпълняват филтриране на шум, компресиране, откриване на движение, базова AI класификация и локално съхраняване.

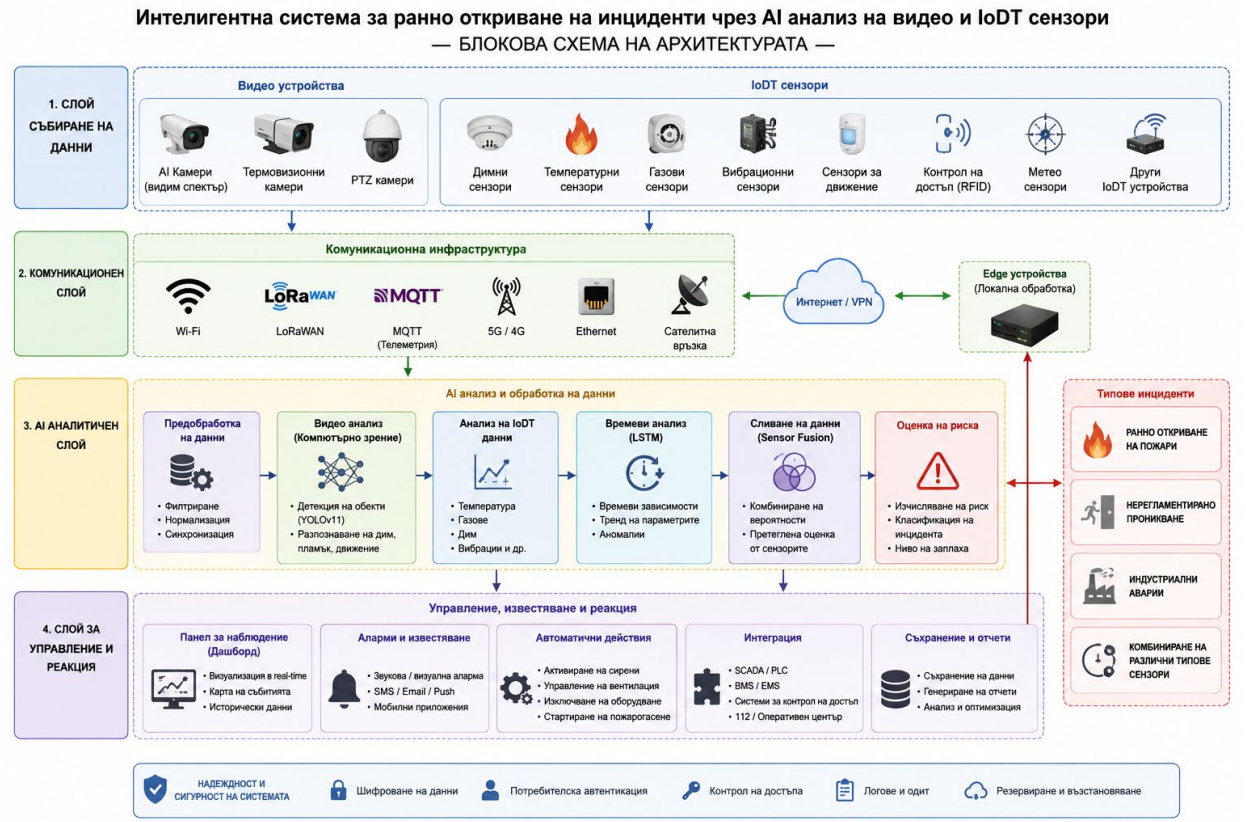
При критични приложения Edge обработката позволява системата да продължи да функционира дори при временно отпадане на интернет или облачната платформа. При достигане на предварително зададен критичен праг локалният възел може да генерира автономна аларма.

3.4 AI аналитичен слой

AI аналитичният слой обединява алгоритмите за видеообработка, анализ на IoDT данни, времеви анализ, Sensor Fusion и оценка на риска. Основните му функционални блокове са предварителна обработка, видео детекция, анализ на времеви редове, оценка на качеството на данните, динамично определяне на теглата, класификация на инцидента и оценка на риска.

3.5 Слой за управление и реакция

Последният слой включва операторски панел, визуализация на събитията, алармена система, мобилни известия, архивиране, автоматизирани защитни действия и интеграция със SCADA, PLC, BMS или други системи за управление. В зависимост от нивото на риск системата може да активира сирена, да управлява вентилацията, да изключи оборудване, да стартира пожарогасителна система или да блокира достъпа до опасна зона.



Фиг. 1. Блокова схема на архитектурата на интелигентната система за ранно откриване на инциденти

4 Предварителна обработка на данните

4.1 Предварителна обработка на видео

Видеопотоците преминават през последователност от операции: извличане на кадри, промяна на размерите, нормализация, корекция на яркостта и контраста, намаляване на шума, компенсиране на движението и отделяне на области на интерес. При термовизионните изображения се извършва температурна калибрация и определяне на области с необичайно висока температура.

4.2 Предварителна обработка на сензорни данни

За всеки сензор се извършват премахване на очевидно невалидни стойности, филтриране на импулсен шум, интерполация на липсващи стойности, нормализация, калибрационна корекция, изчисляване на плъзгаща средна и определяне на скоростта на изменение.

Нормализираната стойност на измервания параметър може да се изчисли чрез:

$$x_i^{norm} = (x_i - x_i^{min}) / (x_i^{max} - x_i^{min}) \quad (1)$$

където x_i е измерената стойност, а x_i^{min} и x_i^{max} са минималната и максималната допустима стойност за съответния параметър. За ранно откриване е важно не само абсолютното ниво на сигнала, но и неговата скорост на изменение:

$$\Delta x_i(t) = x_i(t) - x_i(t-1) \quad (2)$$

Бързото нарастване на температурата или концентрацията на газ може да бъде по-силен индикатор за опасност от единична висока стойност, поради което времевата производна се използва като допълнителен признак в аналитичния модел.

5 AI видеоанализ

5.1 Детекция и проследяване на обекти

За откриване на хора, превозни средства, машини и защитно оборудване може да се използва модел от семейството YOLO. За всеки открит обект се формират клас, координати на ограничителната рамка, вероятност на класификацията, времеви идентификатор, посока и скорост на движение. Наличието на човек в забранена зона се определя чрез пространствено пресичане между траекторията на обекта и предварително дефиниран полигон.

Проследяването във времето позволява разграничаване на краткотрайни шумови детекции от устойчиво присъствие и дава възможност за откриване на преминаване през виртуална линия, престой в защитена зона или движение в забранена посока.

5.2 Ранно откриване на пожар

Откриването на пожар включва анализ на цветови характеристики, форма, движение, текстура, промени между последователни кадри и термична информация. Визуалното разпознаване на дим и пламък е особено полезно в открити пространства, където класическите точкови датчици могат да реагират по-бавно.

За намаляване на фалшивите аларми визуалното разпознаване се комбинира с температура, дим и газови показатели. По този начин ярко отражение или заваръчна дейност не водят автоматично до критична аларма, ако липсва потвърждение от независими физически измервания.

5.3 Откриване на нерегламентирано проникване

Системата анализира преминаване през виртуална линия, престой в забранена зона, движение в необичайно време, нетипична траектория, движение в посока, противоположна на разрешената, и опит за манипулиране на оборудване. Видеоинформацията се съпоставя с RFID/идентификационни данни, инфрачервени бариери и сензори за движение.

Комбинирането на тези източници позволява разграничаване на разрешен служител от външно лице и намалява фалшивите аларми, причинени от животни, растителност или краткотрайни движения във фона.

5.4 Откриване на индустриални аварии

Видеоанализът може да идентифицира паднал човек, липса на защитна каска, разливане на течност, искрене, видима деформация, блокиране на производствена линия,

опасно приближаване до машина или необичайно движение на механичен компонент. Тези визуални признаци се използват съвместно със сензорни данни, тъй като част от най-ранните аварийни признаци не са видими в оптичния спектър.

6 Анализ на IoDT данни

Сензорните данни се обработват като многомерни времеви редове. За даден момент t входният вектор може да бъде дефиниран като:

$$x(t) = [T(t), S(t), G(t), V(t), M(t), H(t)] \quad (3)$$

където T(t) е температурата, S(t) е концентрацията на дим, G(t) е концентрацията на газ, V(t) е нивото на вибрации, M(t) е индикаторът за движение, а H(t) е влажността. За всеки параметър се определят нормално, предупредително и критично ниво.

Една възможна вероятностна оценка за отделен сензорен канал се получава чрез логистична функция:

$$P_i(t) = 1 / (1 + e\hat{}(-a_i(x_i(t) - \theta_i))) \quad (4)$$

където θ_i е прагът, а a_i определя чувствителността на прехода между нормално и опасно състояние. За откриване на времеви зависимости могат да се използват LSTM или GRU мрежи, които анализират последователност от измервания и могат да разпознават постепенно развиващи се отклонения.

7 Мултисензорно обединяване (Sensor Fusion)

7.1 Претеглено обединяване

За всеки източник се формира вероятност P_i за наличие на инцидент. Общата оценка се определя като претеглена комбинация:

$$P_incident = \Sigma_{i=1}^{n} w_i P_i \quad (5)$$

$$\Sigma_{i=1}^{n} w_i = 1 \quad (6)$$

Теглата отразяват базовата надеждност, точността и текущото качество на съответния сензорен канал. По-високо тегло се задава на източници, които са стабилни и релевантни за конкретния тип инцидент.

7.2 Динамично определяне на теглата

Статичните тегла не отчитат моментното състояние на устройствата. Поради това се предлага динамична корекция:

$$w_i(t) = r_i q_i(t) / \Sigma_{j=1}^{n} r_j q_j(t) \quad (7)$$

където r_i е базовата надеждност на i-тия източник, а $q_i(t)$ е показател за качеството на текущите данни. При замърсена камера или загуба на видеокадри теглото на оптичния

канал се намалява. При стабилна термовизионна информация и бързо повишаване на температурата относителното влияние на термичния канал се увеличава.

7.3 Правила за потвърждение на събития

Вероятностният модел се допълва с логически правила за потвърждение. За пожар могат да се използват комбинации от визуално открит пламък и висока температура; визуално открит дим и активен димен сензор; повишена температура, CO и термична аномалия. За проникване се използват човек в забранена зона и активиран сензор за движение; прекъсната инфрачервена бариера без валиден RFID достъп; движение в защитена зона извън разрешен интервал. За индустриална авария се комбинират високи вибрации и визуална деформация; повишена температура и необичайно движение на машина; газова концентрация над прага и визуални признаци за изтичане.

8 Оценка на риска и многостепенна реакция

Самата вероятност за инцидент не е достатъчна за определяне на приоритет. Необходимо е да се отчете и възможното въздействие. Оценката на риска се определя като:

$$R(t) = P_incident(t) \cdot C(t) \quad (8)$$

където C(t) е оценка на тежестта на последствията. Тя може да зависи от типа на обекта, наличието на хора, опасни вещества, критично оборудване и възможността за разпространение на инцидента. Анализът на причините и последствията като метод за управление на риска е разгледан в [26], а рискът от големи аварии с опасни вещества е обсъден в [28].

Ниво	Риск	Препоръчано действие
1	Много нисък	Архивиране и стандартно наблюдение
2	Нисък	Повишено наблюдение
3	Среден	Предупреждение към оператор
4	Висок	Автоматична аларма и локална реакция
5	Критичен	Незабавни защитни действия и уведомяване на аварийни екипи

9 Алгоритъм за функциониране на системата

Основният алгоритъм включва инициализация на камерите и IoDT устройствата, проверка на комуникационните канали, получаване на синхронизирани видеокадри и сензорни данни, предварителна обработка, AI анализ на видеото, анализ на сензорните времеви редове, оценка на качеството, динамично определяне на теглата, мултисензорно обединяване, класификация на инцидента, оценка на риска и задействане на подходяща реакция.

```
INPUT: video streams V, sensor streams S, thresholds Θ
INITIALIZE devices and AI models
WHILE system is active:
 acquire synchronized video and sensor data
 evaluate data quality
 preprocess video and sensor streams
 P_video ← video_AI_analysis()
 P_sensor ← temporal_sensor_analysis()
 weights ← calculate_dynamic_weights()
 P_incident ← sensor_fusion(P_video, P_sensor, weights)
 incident_class ← classify_incident(P_incident)
 risk ← P_incident × consequence
 IF risk ≥ critical threshold: activate emergency actions
 ELSE IF risk ≥ alarm threshold: notify operator
 ELSE IF risk ≥ warning threshold: increase monitoring
 store results
END WHILE
```

10 Експериментална постановка

За оценка на системата е дефиниран симулационен експериментален набор, съдържащ синхронизирани видеопоследователности и сензорни измервания. Изследвани са три основни категории: пожар, нерегламентирано проникване и индустриална авария. За всяка категория са моделирани както нормални, така и аварийни състояния.

10.1 Сценарии за пожар

Сценариите за пожар обхващат малък локален пламък; постепенно образуване на дим; прегряване без открит пламък; отражение, наподобяващо пламък; заваръчна дейност; дим от безопасен технологичен процес.

10.2 Сценарии за проникване

При проникване са моделирани следните ситуации: човек в забранена зона; преминаване през виртуална линия; движение на животно; разрешен служител с RFID идентификация; неразрешен достъп извън работно време; престой до защитено оборудване.

10.3 Сценарии за индустриални аварии

Сценариите за индустриални аварии включват повишени вибрации; прегряване на електродвигател; газово изтичане; разливане на течност; блокиране на механизъм; падане на работник; частична деформация на конструкция.

10.4 Сравнявани методи и метрики

Сравнени са три варианта: само AI видеоанализ, само IoDT сензори и комбиниран AI + IoDT модел. Оценката се извършва чрез Accuracy, Precision, Recall, F1-score, False Alarm Rate, Missed Detection Rate, ROC, AUC и матрица на объркване. Основните метрики се определят чрез:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (9)$$

$$Precision = TP / (TP + FP) \quad (10)$$

$$Recall = TP / (TP + FN) \quad (11)$$

$$F1 = 2 \cdot Precision \cdot Recall / (Precision + Recall) \quad (12)$$

11 Експериментални резултати

11.1 Обща точност

Метод	Точност
AI видеоанализ	91,8%
IoDT сензори	89,6%
AI + IoDT Sensor Fusion	98,1%

Комбинираният подход показва подобрение от 6,3 процентни пункта спрямо видеоанализа и 8,5 процентни пункта спрямо сензорния модел. Това потвърждава, че независимите информационни канали компенсират взаимно ограниченията си.

11.2 Резултати по вид инцидент

Вид инцидент	Само видео	AI + IoDT
Пожар	91,4%	98,1%
Проникване	93,2%	98,7%
Индустриална авария	88,6%	97,4%

Най-голямото подобрение се наблюдава при индустриалните аварии. Причината е, че ранни признаци като вибрации, газова концентрация и прегряване не могат да бъдат надеждно установени само чрез визуален анализ.

11.3 Матрица на объркване за видеоанализа

Реален клас	Предсказан инцидент	Предсказано нормално
Инцидент	458	42
Нормално състояние	39	461

При 1000 тестови наблюдения видеоаналитичният модел формира 458 истински положителни, 461 истински отрицателни, 39 фалшиво положителни и 42 фалшиво отрицателни решения. От тях се получават приблизително Accuracy = 91,9%, Precision = 92,2%, Recall = 91,6% и F1-score = 91,9%.

11.4 Матрица на объркване за AI + IoDT

Реален клас	Предсказан инцидент	Предсказано нормално
Инцидент	490	10
Нормално състояние	9	491

При интегрирания модел броят на пропуснатите инциденти е намален от 42 на 10, а фалшиво положителните решения – от 39 на 9. Получените показатели са Accuracy 98,1%, Precision 98,2%, Recall 98,0% и F1-score 98,1%.

11.5 ROC анализ

Метод	AUC
IoDT	0,913
AI видео	0,942
AI + IoDT	0,988

Стойността AUC = 0,988 показва много висока способност на комбинирания модел да разделя нормални и аварийни състояния. Разликата спрямо самостоятелните канали показва ефекта от мултисензорното потвърждение.

11.6 Фалшиви аларми и пропуснати детекции

Показател	Видео AI	AI + IoDT
False Alarm Rate	9,4%	6,2%
Missed Detection Rate	8,4%	2,0%

Относителното намаление на False Alarm Rate се оценява като:

$$\text{Reduction} = ((9{,}4 - 6{,}2) / 9{,}4) \cdot 100 \approx 34{,}0\% \quad (13)$$

Резултатът показва, че независимото потвърждение от няколко типа сензори ограничава неправилното активиране на алармите и едновременно с това намалява риска от пропускане на реално събитие.

12 Дискусия

Получените резултати показват, че мултисензорното обединяване има съществено значение за системите за ранно откриване. Видеоанализът предоставя пространствен контекст и идентифицира обекти и действия, докато IoDT сензорите измерват физическите характеристики на средата. Тези два типа информация са взаимно допълващи се.

При пожар термичните, димните и газовите сензори могат да потвърдят визуалното разпознаване на пламък. При неблагоприятна видимост термовизионните и температурните данни могат да компенсират намалената точност на оптичните камери. При проникване видеото позволява идентифициране и проследяване на обекта, а RFID системата и датчиците за движение дават допълнителна информация за разрешението и начина на достъп.

При индустриални аварии най-голямо значение имат времевите зависимости. Постепенното увеличаване на вибрациите или температурата може да бъде ранна индикация за неизправност, преди да се наблюдават видими повреди. Това обяснява по-голямото подобрение на комбинирания модел при този клас събития.

Основно предимство на системата е адаптивността. Динамичните тегла позволяват намаляване на влиянието на сензор, чиито данни са с ниско качество. Подходът повишава устойчивостта при частични откази, но изисква надеждна оценка на качеството на каналите и периодична калибрация.

Основните ограничения на представеното изследване са използването на симулационни данни, ограниченият брой класове инциденти, липсата на дългосрочна експлоатация в реален обект, необходимостта от обучение за конкретната среда и възможните комуникационни закъснения. Поради това числените стойности в раздел 11 следва да се разглеждат като резултати от моделна експериментална постановка, а не като универсални показатели за всички реални среди.

13 Надеждност и киберсигурност

Системата трябва да бъде проектирана така, че отказът на един компонент да не води до пълна загуба на наблюдение. Подходящи мерки са резервирани комуникационни връзки, Edge обработка, локално архивиране, самодиагностика, контрол на достоверността на сензорните данни, дублиране на критични сензори, периодична калибрация и автоматично превключване към резервен възел.

Киберсигурността включва криптиране на комуникацията, удостоверяване на устройствата, управление на сертификати, мрежова сегментация, регистриране и одит, защита срещу повторно изпращане на пакети, откриване на аномалии в трафика и контролирано актуализиране на софтуера. Особено важна е защитата срещу подмяна на сензорни данни, защото компрометиран IoDT възел може да предизвика фалшива аларма или да прикрие реален инцидент. Съвременните киберзаплахи са разгледани в [31], а сигурността на интелигентни структури в Интернет на нещата е анализирана в [32].

14 Практически приложения

Предложената система може да бъде използвана в производствени предприятия, складове за опасни вещества, енергийни обекти, транспортни терминали, пристанища, летища, логистични центрове, подземни съоръжения, минни и следминни територии, обществени сгради, интелигентни градове и други обекти от критичната инфраструктура. Архитектурата е мащабируема и позволява изграждане както на малки локални инсталации, така и на разпределени системи с множество камери и голям брой IoDT възли. При

планиране на последваща интеграция могат да се разгледат организацията на националната система за спешни повиквания [27] и геодезическите подходи и цифровите технологии за оценка и управление на риска от наводнения [30].

15 Заключение

В доклада е представена интелигентна система за ранно откриване на инциденти чрез интеграция на AI видеоанализ и IoDT сензори. Предложената архитектура комбинира пространствената и семантичната информация от видеото с физическите измервания на температура, дим, газове, вибрации и движение.

Основното предимство на подхода е възможността за взаимно потвърждаване на събитията от независими източници. Това повишава точността, намалява фалшивите аларми и съкращава времето за реакция. Симулационните резултати показват средна точност 98,1%, AUC 0,988 и значително намаляване на пропуснатите инциденти.

Бъдещата работа трябва да бъде насочена към изграждане на реален експериментален стенд, събиране на собствен набор от синхронизирани видео- и сензорни данни, оценка на латентността, проверка при частични откази и разработване на адаптивен модел за самообучение. Допълнително направление е интегрирането на FMEA [25], Fault Tree Analysis и Monte Carlo симулации за количествена оценка на надеждността и отказоустойчивостта на цялата система.

ЛИТЕРАТУРА:

[1] Диманова Д. В., Цанков Ц. С. Анализ състоянието на критичната инфраструктура за район Шумен. Годишник на Шуменския университет „Епископ К. Преславски“, Шумен, 2016, ISSN 1311-834X, с. 45–54.

[2] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения: Компютърен експеримент с трансфер на знания в MATLAB. DefTech 2025, 2025, с. 732–741. ISSN 2815-4282.

[3] Essahraui S., Dini P., Saponara S. Early fire and smoke detection using deep learning: A comprehensive review of models, datasets, and challenges. Applied Sciences, Vol. 15, No. 18, 2025, Art. No. 10255, DOI: 10.3390/app151810255.

[4] Khan R. A., Alam U. I., Raza B. R. H., Anwar M. W. Beyond boundaries: Advancements in fire and smoke detection for indoor and outdoor surveillance feeds. Engineering Applications of Artificial Intelligence, Vol. 142, 2025, Art. No. 109855.

[5] Fan Y., Fu T., Listopad N. I., Liu P., Garg S., Hassan M. M. Utilizing correlation in space and time: Anomaly detection for Industrial Internet of Things (IIoT) via spatiotemporal gated graph attention network. Alexandria Engineering Journal, Vol. 106, 2024, pp. 560–570, DOI: 10.1016/j.aej.2024.08.048.

[6] Ayantayo A., Kaur A., Kour A. et al. Network intrusion detection using feature fusion with deep learning. Journal of Big Data, Vol. 10, 2023, Art. No. 167, DOI: 10.1186/s40537-023-00834-0.

[7] Talukder M. A., Hasan K. F., Islam M. M. et al. A dependable hybrid machine learning model for network intrusion detection. Journal of Information Security and Applications, Vol. 72, 2023, Art. No. 103405.

[8] Henry A., Gautam S., Khanna S. et al. Composition of hybrid deep learning model and feature optimization for intrusion detection system. Sensors, Vol. 23, No. 2, 2023, Art. No. 890, DOI: 10.3390/s23020890.

[9] Lilhore U. K., Manoharan P., Simaiya S. et al. Hybrid intrusion detection model for Industry 4.0 networks using an optimized CNN–LSTM with transfer learning. Sensors, Vol. 23, No. 18, 2023, Art. No. 7856, DOI: 10.3390/s23187856.

[10] Imrana Y., Xiang Y., Ali L., Abdul-Rauf Z. CNN-GRU-FF: A double-layer feature fusion-based network intrusion detection system using a modified focal loss. Complex & Intelligent Systems, 2024, DOI: 10.1007/s40747-023-01313-y.

[11] Zhao M., Fink O. DyEdgeGAT: Dynamic edge via graph attention for early fault detection in IIoT systems. IEEE Internet of Things Journal, Vol. 11, No. 13, 2024, pp. 22950–22965, DOI: 10.1109/JIOT.2024.3381002.

[12] Zhao M., Peng H., Li L. Multivariate time-series anomaly detection based on dynamic graph neural networks and self-distillation in Industrial Internet of Things. IEEE Internet of Things Journal, 2024, DOI: 10.1109/JIOT.2024.3520362.

[13] Xie S., Li L., Zhu Y. Anomaly detection for multivariate time series in IoT using discrete wavelet decomposition and dual graph attention networks. Computers & Security, Vol. 146, 2024, Art. No. 104075, DOI: 10.1016/j.cose.2024.104075.

[14] Yang J., Yue Z. Learning hierarchical spatial–temporal graph representations for robust multivariate industrial anomaly detection. IEEE Transactions on Industrial Informatics, Vol. 19, No. 6, 2023, pp. 7624–7635, DOI: 10.1109/TII.2022.3216006.

[15] Zhang Z., Geng Z., Han Y. Graph structure change-based anomaly detection in multivariate time series of industrial processes. IEEE Transactions on Industrial Informatics, Vol. 20, No. 4, 2024, pp. 6457–6466.

[16] He S., Li G., Wang J., Xie K., Sharma P. K. Graph structure learning-based multivariate time-series anomaly detection in Internet of Things for human-centric consumer applications. IEEE Transactions on Consumer Electronics, Vol. 70, No. 3, 2024, pp. 5419–5431, DOI: 10.1109/TCE.2024.3409391.

[17] Wang J., Shao S., Bai Y., Deng J., Lin Y. Multiscale wavelet graph autoencoder for multivariate time-series anomaly detection. IEEE Transactions on Instrumentation and Measurement, Vol. 72, 2023, pp. 1–11, DOI: 10.1109/TIM.2022.3223142.

[18] Denev D., Tsankov Ts. Progress and trends in machine vision smart cameras. Scientific Conference with International Participation MATTEH 2020, Conference Proceedings, Vol. 2, Shumen, 2020, ISSN 1314-3921, pp. 116–124.

[19] Ali M. et al. A comprehensive review of advanced sensor technologies for early fire detection and IoT integration. Chemosensors, Vol. 13, No. 7, 2025, Art. No. 230, DOI: 10.3390/chemosensors13070230.

[20] AlQahtani A. A. S. et al. A comprehensive review and bibliometric analysis of IoT-based fire detection systems. Safety, Vol. 11, No. 2, 2025, Art. No. 41, DOI: 10.3390/safety11020041.

[21] Sharobiddinov D. et al. Edge-based autonomous fire and smoke detection using deep learning and IoT devices. Sensors, Vol. 25, No. 20, 2025, Art. No. 6419, DOI: 10.3390/s25206419.

[22] Yang Y. et al. Design and research of an intelligent detection method for video fire recognition and multi-sensor data fusion based on edge computing. Applied Sciences, Vol. 15, No. 19, 2025, Art. No. 10589, DOI: 10.3390/app151910589.

[23] Hussain M. et al. A comprehensive review on deep-learning-based data-driven methods for fire and smoke detection. IEEE Access, Vol. 12, 2024.

[24] Atanasov, V., Trifonov, T. A new model of ultra wideband sensors based interactive system. International Journal on Information Technologies and Security, Vol. 16, No. 1, 2024, pp. 39–48, ISSN 1313-8251. https://doi.org/10.59035/XYCG3094

[25] Arabadzhieva-Kalcheva N., Tsankov Ts. Failure Modes and Effects Analysis – FMEA. Scientific Conference with International Participation MATTEH 2022, Conference Proceedings, Vol. 2, Shumen, 2022, ISSN 1314-3921, pp. 58–62.

[26] Arabadzhieva-Kalcheva N., Tsankov Ts., Todorova M. Cause-Consequence Analysis as a Risk Management Method. Annual of Konstantin Preslavsky University of Shumen, Vol. XIV E, Faculty of Technical Sciences, 2024, ISSN 1314-8818, pp. 184–188. https://doi.org/10.46687/YT24NEL

[27] Диманова Д., Кузманов З. Национална система за спешни повиквания. Научна конференция MATTEX 2016, Шуменски университет „Епископ Константин Преславски“, 11–13 ноември 2016, с. 77–83, ISSN 1314-3921.

[28] Dimanova, D. Risk of major accidents with hazardous substances. SocioBrains, Issue 52, December 2018, pp. 49–53, ISSN 2367-5721.

[29] Dimanova, D. Risk management of critical infrastructure sites and facilities. SocioBrains, Issue 36, August 2017, pp. 67–73, ISSN 2367-5721.

[30] Stefanova, A. Flood risk assessment and management under directive 2007/60/EU: geodetic approaches and digital technologies for effective prevention. Environment. Technology. Resources, Proceedings of the 16th International Scientific and Practical Conference, Rezekne, Latvia, 19–20 June 2025, Vol. 4, pp. 393–397, ISSN 2256-070X. https://doi.org/10.17770/etr2025vol4.8402

[31] Nikolov, L., Slavyanov, K. On the Contemporary Cybersecurity Threats. Proceedings of the First International Scientific Conference CONFSEC 2017, Borovets, 11–14 December 2017, pp. 142–144, ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[32] Стоянова, В. Интернет на нещата – анализ на сигурността при интелигентни структури. II International Scientific Conference CONFSEC, Borovets, 2018, Year 2, Issue 2 (4). ISSN 2603-2945 (Print), ISSN 2603-2953 (Online).

[33] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване и разпознаване на частично видими обекти с военно предназначение в оптични изображения. DefTech 2025, 2025, с. 723–731. ISSN 2815-4282.

[34] Манов Л. Е. Съвременни технологии с изкуствен интелект за откриване на обекти с военно предназначение в оптични изображения. DefTech 2024, 2024, с. 675–682. ISSN 2815-4282.