

Substantiation of a multi-sensor automated system for the protection of categorized facilities under conditions of mass riots

F.B.Achilov

A.A.Jalolov

Public Safety University of Republic of Uzbekistan

Abstract: *The article presents the scientific and technical foundations of a multi-sensor intelligent automated protection system designed to ensure the security of categorized facilities under conditions of mass riots. An algorithm is proposed for early threat detection, threat level assessment, automatic control of protective mechanisms and prompt notification of responsible personnel through the integration of acoustic, vibration, infrared and video surveillance means. The experimental studies substantiate that the automated system reduces response time compared with a conventional system and increases operational speed efficiency. In addition, the reliability, stability and economic efficiency of the system are evaluated, and the possibilities of its application for the intelligent technical protection of categorized facilities are substantiated.*

Keywords: *categorized facility, mass riots, public safety, intelligent technical protection, multi-sensor system, automated protection, integration, physical protection mechanisms, economic efficiency*

Introduction. Ensuring the security of categorized facilities is one of the multilayered tasks of the modern public safety system. At such facilities, protection is not limited to the physical presence of security personnel; it requires early threat detection, situation verification, control of physical barriers, and communication and notification to be combined within a single information environment. In Uzbekistan, the organizational and institutional foundations of public safety were further systematized by Presidential Decree No. PF-27 of 29 November 2021, which defines the directions for improving public safety processes and introducing modern technologies [1].

The relevance of the topic is explained by the growing complexity of threats to facilities. Mass gatherings, aggressive behavior, pressure on entry points, attempts to cause damage, and the simultaneous appearance of several risk indicators create a high cognitive load for the operator. Therefore, the automation of critical functions of a security system should be based not on removing the human from the system, but on the principle of augmenting human decision-making capability with technical means [4].

According to SIAT data of the National Statistics Committee of the Republic of Uzbekistan, the number of registered crimes in the country increased from 132,298 in 2024 to 155,002 in 2025, i.e. by 17.2%. This figure is not a direct indicator of the number of mass riots; however, it can be regarded as a contextual statistical indicator showing the general importance of rapid information processing and differentiated risk assessment for law enforcement systems [3].

From this standpoint, in ensuring the security of categorized facilities, it is becoming increasingly important to develop intelligent automated approaches that make it possible to receive, process and analyze information from various sources within a single system, rather than applying existing technical means separately. Under mass riot conditions in particular, threats are dynamic, multi-vector and rapidly changing, and detecting them reliably with only a single sensor or monitoring device may not be sufficiently effective. Under such conditions, a need arises to integrate the data

obtained from video surveillance, motion and approach detection, access control, physical barrier control, and audio and visual notification means.

To solve this problem, a hybrid architecture is proposed for protecting categorized facilities under mass riot conditions, which provides a comprehensive assessment of the situation around the facility through acoustic, vibration, infrared and video surveillance channels, dynamic determination of the threat level, safe control of actuators, and prompt notification of the responsible officer.

Main Body. Foreign literature shows that the main advantage of fusing data transmitted from different sensors is that the weaknesses of individual sensors are mutually compensated. Fusing data from different sensors in a multi-sensor perimeter is considered a promising approach for increasing detection robustness, reducing noise and uncertainty, and improving decision-making in complex environments [8].

One of the main problems in analyzing the movement of groups of people is that the boundary between “normal” and “abnormal” behavior depends on the specific situation and conditions. For example, running people may be regarded as normal in an area where a marathon is being held, whereas the same movement in front of a bank or a closed administrative facility may be regarded as a sign of potential danger. Therefore, when making decisions, an automated analysis system should rely not on a single external feature, but on a combination of several features, such as the time interval, the characteristics of the area, crowd density, direction of movement, speed of movement and the degree of approach to the facility. This approach makes it possible to assess movements in different situations based on context and to distinguish potential threats more accurately [6].

According to the core requirements of the NIST Artificial Intelligence Risk Management Framework, trustworthy artificial intelligence systems should possess such characteristics as validity and reliability, safety, resilience, accountability, transparency, explainability, privacy and fairness [7]. The Ethical Rules for the use of artificial intelligence-based solutions, registered in Uzbekistan in 2026, also establish the need to comply with safety and ethical requirements in the development, deployment and use of artificial intelligence systems [2]. Accordingly, the artificial intelligence component used to ensure the security of categorized facilities should be evaluated not only by its accuracy, but also by such criteria as the explainability of its decisions, the possibility of monitoring and auditing system operation, the traceability of the decision-making process, and human oversight.

The proposed multi-sensor automated system for ensuring the security of categorized facilities consists of five main functional units: 1) a sensor unit; 2) a control unit; 3) a data transmission unit; 4) a data display unit; 5) an actuator unit. Such an architecture integrates security means into a single interconnected cyber-physical system, enabling comprehensive processing of the data obtained from different sensors, threat level assessment and coordinated implementation of protective measures.

The first unit (sensor unit) consists of acoustic, vibration, infrared and video surveillance sensors. Their task is not the final assessment of an event, but the continuous collection of primary indicators.

The second unit (control unit) processes the data received from the sensor unit, activates the servo drive of the actuator unit, transmits the command to lower the armored shutter, and also sends a message about the external impact to the data transmission unit.

The third unit (data transmission unit) consists of a radio module and transmits the alarm signal generated as a result of an external impact to the data display unit via a radio channel.

The fourth unit (data display unit) displays to the operator the data received and processed by the microcontroller.

The fifth unit (actuator unit) is responsible for safely blocking entry points, activating mechanical protection elements, activating the emergency mode and switching the system to a backup power source.

An important feature of the system is the rejection of the “single-sensor decision”. For example, loud noise by itself may not indicate an attack. However, if an increase in vibration, the movement of a group of people toward the facility in the video frame, and an increase in movement density in the entry zone are recorded simultaneously with the noise, the hazard level of the event increases. The intelligent system works effectively precisely in such multi-indicator situations.

Three main scenarios are proposed for testing the operation of the system. Scenario A - escalation of tension around the facility; Scenario B - movement of a crowd toward the facility and an increase in risk indicators; Scenario C - detection of a direct aggressive impact on entry points or building structures.

In Scenario A, the main task of the system is preparation. The status of the sensors is checked, video analytics is activated, the monitoring frequency at critical entry points is increased, and personnel are informed of the change in the situation. If a dynamic increase in the risk index is detected at the Scenario B stage, access control is strengthened and physical protection means are brought to a state of readiness. At the Scenario C stage, the system gives priority to multi-source confirmation of the event, switching protective elements to a safe state, and notifying the responsible services.

Algorithmically, this can be expressed as follows: receiving data from sensors - time synchronization - noise filtering - assessment of sensor reliability - fusion of evidence from video and physical sensors - calculation of the risk index - scenario identification - providing the operator with a clear explanation - execution of an automatic action within the authorized scope - logging the event - returning to a safe state once the threat has subsided.

An experimental study was conducted to substantiate the effectiveness of using the system proposed by the authors.

During the experimental study, the response time and the time required to fully close the armored shutters were measured for the conventional manually controlled system (MCS) and the automated system (AS) (T_{MCS} and T_{AS}). Observations showed that, when a threat arose, the automated device promptly launched its assigned automatic cycle “Detection - Confirmation - Response - Blocking - Notification”.

The empirical data for the experimental study are presented in Table 1.

Table 1

Empirical data for the experimental study

Trial No.	Response time of the conventional manually controlled system T_{MCS} , s	Response time of the automated system T_{AS} , s	Difference (Δ), s
1	28.5	8.7	19.8
2	32.0	9.1	22.9
3	26.3	8.5	17.8
4	35.1	9.4	25.7
5	29.8	8.8	21.0
6	34.2	8.9	25.3

7	27.5	8.6	18.9
8	31.4	9.2	22.2
9	36.0	9.5	26.5
10	28.9	8.7	20.2
Mean	30.97	8.94	22.03

A comparative graph of the empirical data obtained in the experimental study is presented in Figure 1.

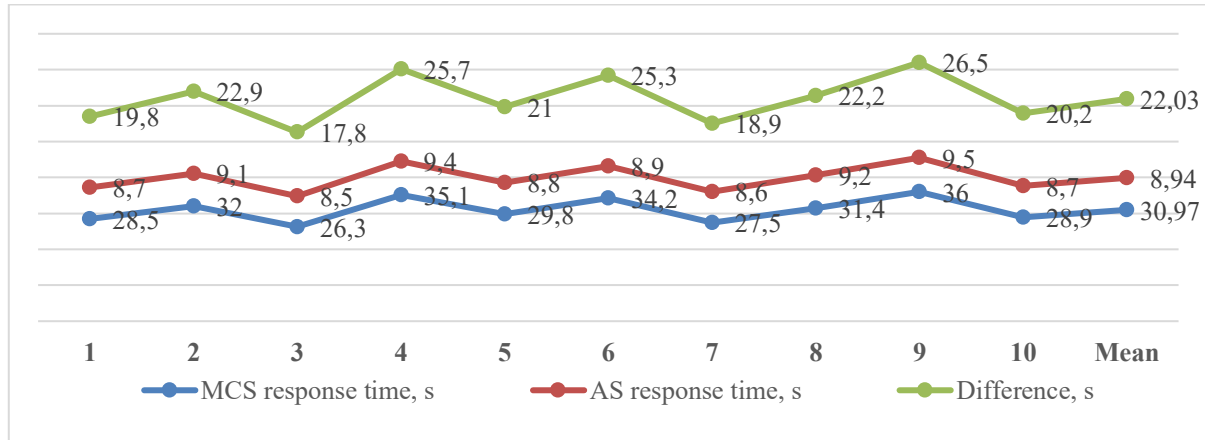


Figure 1. Comparative graph of the response times of the conventional manually controlled and automated systems

As can be seen from Figure 1, the time variability of the conventional manually controlled system (from 26.3 s to 36.0 s) shows a very high dispersion. This is directly explained by the psychophysiological factors inherent in the human factor. During mass riots, the guard's attention is distracted and, as stress increases, analytical thinking slows down and the overall response time increases. The automated system, by contrast, showed stable results (in the range of 8.5-9.5 s). In this case, most of the time was spent by the servo motors (the mechanical part) lowering the shutter. Methods of probability theory and mathematical statistics were used to ensure the reliability and objectivity of the empirical data obtained from the experimental studies. Based on the results of $n = 10$ trials measuring the response times of the two compared systems (conventional and automated), the following statistical indicators were calculated.

Calculation of the arithmetic mean. First, the average response time of each system was determined through the mathematical expectation (arithmetic mean). The following formula was used for this purpose (1):

$$\bar{T} = \frac{1}{n} \sum_{i=1}^n T_i \quad (1)$$

where $\bar{T}$ is the mean system response time; n is the number of trials ($n = 10$); T_i is the time recorded in each individual trial.

Average time taken by the conventional manually controlled system (based on Table 1):

$$T_{MCS} = \frac{28.5 + 32.0 + 26.3 + 35.1 + 29.8 + 34.2 + 27.5 + 31.4 + 36.0 + 28.9}{10} = 30.97 \text{ s}$$

Average time taken by the automated system (based on Table 1):

$$T_{AS} = \frac{8.7 + 9.1 + 8.5 + 9.4 + 8.8 + 8.9 + 8.6 + 9.2 + 9.5 + 8.7}{10} = 8.94 \text{ s}$$

Determination of the variance and standard deviation. To determine how reliable the obtained mean values are, as well as the degree of operational stability of the systems, the empirical variance (S^2)

and the standard deviation (S) were calculated. This indicator shows the extent to which the system deviates in a real situation.

The following formula was used to determine the empirical variance (2):

$$S^2 = \frac{1}{n-1} \sum_{i=1}^n (T_i - \bar{T})^2 \quad (2)$$

The following formula was used to determine the standard deviation (3):

$$S = \sqrt{S^2} \quad (3)$$

Calculations for the conventional manually controlled system:

For the conventional manually controlled system, the sum of squared deviations was $\sum(T_i - 30.97)^2 \approx 99.64$.

$$S_{MCS}^2 = \frac{99.64}{9} \approx 11.07$$

$$S_{MCS} = \sqrt{11.07} \approx 3.33 \text{ s}$$

Calculations for the automated system:

For the automated system, the sum of squared deviations was $\sum(T_i - 8.94)^2 \approx 1.064$.

$$S_{AS}^2 = \frac{1.064}{9} \approx 0.118$$

$$S_{AS} = \sqrt{0.118} \approx 0.34 \text{ s}$$

For the conventional manually controlled system, the standard deviation was 3.33 s. This proves that the response time varies considerably depending on the person's psychological state, attention and fatigue. For the automated system, this indicator was 0.34 s. That is, the automated system operates almost identically every time, with extremely high stability and accuracy.

Assessment of reliability using the coefficient of variation. The coefficient of variation (V) was used to evaluate and compare the relative variability of the systems (4):

$$V = \frac{S}{\bar{T}} \times 100\% \quad (4)$$

Calculations for the conventional manually controlled system:

$$V_{MCS} = \frac{3.33}{30.97} \times 100\% \approx 10.75\%$$

Calculations for the automated system:

$$V_{AS} = \frac{0.34}{8.94} \times 100\% \approx 3.80\%$$

According to the rules accepted in mathematical statistics [5], if the coefficient of variation is less than 10% ($V < 10\%$), the sample is considered highly reliable and the process highly stable. Hence, the operational stability of the proposed automated device (3.8%) is fully confirmed mathematically.

Calculation of the time efficiency coefficient. To determine the efficiency gained from introducing the new system, the difference between the response times was expressed as a relative percentage (5):

$$E = \frac{\bar{T}_{MCS} - \bar{T}_{AS}}{\bar{T}_{MCS}} \times 100\% \quad (5)$$

Using formula (5), we calculate the time efficiency coefficient:

$$E = \frac{30.97 - 8.94}{30.97} \times 100\% = \frac{22.03}{30.97} \times 100\% \approx 71.13\%$$

The mathematical and statistical calculations showed that, during mass riots, the proposed system responded faster than the conventional manually controlled system, with a 71.13% reduction in response time (on average 22 s earlier), and ensured reliable blocking of the protected facility. It should be noted that, in ensuring the security of a protected facility during mass riots, a 22-second advantage is a decisive amount of time for completely preventing rioters from entering the building. In terms of stability and reliability, the standard deviation of the developed automated device was 0.34 s, which scientifically substantiates that the device is free from the human factor and that environmental stress factors do not affect its operation. Furthermore, the rapid autonomous closing (within 8-9 s) of the armored shutters installed on the windows and doors of the building by the automated device not only ensures the security of the facility but also saves security personnel the time needed to neutralize the threat or to call in reserve forces.

Under modern conditions, the introduction of engineering, technical and security systems into practice is evaluated not only by their technical characteristics, but also by such fundamental criteria as economic profitability, the project payback period, and the return on security investment (ROSI). The economic efficiency of the proposed system is formed in direct (reduction of present costs) and indirect (prevention of potential losses) terms.

To calculate the production cost of the system, an estimate of material costs for its basic configuration was prepared based on current market conditions; it amounted to approximately UZS 660,000 per protection point.

To determine the direct economic efficiency of the system, the following formula was used (6):

$$E_{annual} = (L_{pot} + P_{sav}) - (K_{inv} + C_{op}) \quad (6)$$

where E_{annual} is the comparative economic efficiency after the introduction of the system (in UZS); L_{pot} is the equivalent of the potential physical damage that may be caused to the building during mass riots when a conventional security system is in place (state property that is difficult to restore); P_{sav} is the savings on wages paid to personnel engaged in visual monitoring to guard each door and window of the facility; K_{inv} is the initial capital expenditure for purchasing and assembling the system and integrating it with the shutters at the facility (~UZS 660,000); C_{op} is the cost of maintenance and electricity for one year of system operation. The study shows that the ATmega328P microcontroller used has minimal power consumption, while the LM2596 step-down voltage regulator is optimized to the maximum extent for energy saving. Consequently, the operating costs of the automated device are close to zero.

For example, if the ground floor of an administrative building has 15 vulnerable access points (windows and doors), fully automating this floor requires a one-time capital investment of $K_{inv} = 15 \times 660,000 = 9,900,000$ UZS. In the event of mass riots, the material damage to state property (L_{pot}) caused by stones thrown into a single room or by incendiary devices may amount to UZS 30-40 million. The fully autonomous and rapid (~8 s) response of the proposed system completely blocks this risk. In a single incident alone, the direct savings (efficiency) for the facility will be several times higher than the investment made.

The economic benefit of the proposed system is measured by the amount of potential losses prevented. To calculate it, the annualized loss expectancy (ALE) formula (7), widely used in international security risk assessment practice [9], was applied:

$$ALE = ARO \times SLE \quad (7)$$

where ARO (annual rate of occurrence) is the probability (frequency) of such threats occurring within one year; SLE (single loss expectancy) is the average financial loss that may be caused to the facility (state property) as a result of a single incident during mass riots.

Once the new system is introduced, it operates autonomously without the constant involvement of an operator and fully isolates the facility within ~8 s of sensor activation. As a result, the probability of loss (*ARO*) and the magnitude of loss (*SLE*) decrease sharply (in practice, approaching zero). On this basis, the return on security investment (ROSI) is determined using the following formula (8):

$$ROSI = \frac{ALE_{before} - ALE_{after} - K_{inv}}{K_{inv}} \times 100\% \quad (8)$$

where ALE_{before} is the expected annual loss with a conventional security system; ALE_{after} is the expected residual loss after the new system is installed; K_{inv} is the initial capital expenditure for purchasing and assembling the new system and integrating it with the shutters at the facility.

In a hypothetical example, the economic efficiency of the proposed system can be modeled mathematically as follows:

If $K_{inv} = 6,600,000$ UZS is spent to equip 10 points on the ground floor of a categorized facility with the automated device, and the potential financial loss (ALE_{before}) caused by stones and incendiary devices thrown at the building during mass riots is estimated at an average of UZS 50,000,000, then:

$$ROSI = \frac{50,000,000 - 0 - 6,600,000}{6,600,000} \times 100\% = \frac{43,400,000}{6,600,000} \times 100\% \approx 657.6\%$$

This means that each UZS invested in the proposed system makes it possible to preserve at least UZS 6.5 worth of state property and material assets during mass riots.

Conclusion. As a result of the research, the concept of a multi-sensor hybrid automated system for the intelligent technical protection of categorized facilities under mass riot conditions has been developed. The main scientific idea of the system is to fuse acoustic, vibration, infrared and video data within a single threat model rather than processing them separately.

The speed and stability efficiency of the proposed system has been confirmed experimentally. The results of the experiment conducted under conditions of a direct threat (an attack on the building and objects being thrown) showed that, with a conventional human-controlled security system, the average system response time was 30.97 s, whereas with the automated device this indicator was 8.94 s. As a result, time efficiency increased by 71.13%, and a decisive advantage of 22 s was achieved.

Consequently, errors associated with the human factor (dispersion) have been minimized. In the conventional human-controlled security system, the standard deviation was 3.33 s, and strong instability was recorded depending on the guard's stress and psychophysiological state. In the proposed system, the standard deviation was 0.34 s, ensuring extremely high precision and reliability (coefficient of variation of 3.8%).

The high economic profitability (ROSI) of the project has been substantiated. It has been shown that the capital cost estimate of the system, assembled from open-architecture electronic components, is approximately UZS 660,000 per protection point, with operating costs close to zero. According to the return on security investment (ROSI) calculations, the project pays for itself with a return of approximately 657.6%, i.e. every UZS 1 invested in the new system preserves at least UZS 6.5 worth of state property during mass riots.

References

1. Decree of the President of the Republic of Uzbekistan No. PF-27 of 29 November 2021 "On approval of the Concept of Public Safety of the Republic of Uzbekistan and measures for its

- implementation” // LexUZ. URL: <https://test.lex.uz/uz/doc-passport/-5749291> (accessed: 25.09.2026). (In Uzbek)
2. Ministry of Digital Technologies of the Republic of Uzbekistan. Ethical Rules for the Creation, Implementation and Use of Artificial Intelligence-Based Solutions. Registration No. 3787, 14.03.2026 // LexUZ. URL: <https://lex.uz/pdf/8083233> (accessed: 25.09.2026). (In Uzbek)
3. National Statistics Committee of the Republic of Uzbekistan. Number of registered crimes (by region) – SIAT // stat.uz. URL: <https://siat.stat.uz/data/800/?lang=uz> (accessed: 25.09.2026).
4. Achilov F.B., Jalolov A.A. Method of applying an automated device ensuring the security of categorized facilities during mass riots // INNOVATION TECHNOSYSTEMS. Scientific and Technical Journal. No. 2(22), 2026. P. 50–56. ISSN 2181-2152. Journal website: <https://mvahi.uz> (accessed: 25.09.2026). (In Uzbek)
5. Abdullayev Yo. Theory of Statistics: Textbook for students of higher educational institutions. Tashkent: O'qituvchi, 2002. P. 170–176. (In Uzbek)
6. Luque Sánchez F., Hupont I., Tabik S., Herrera F. Revisiting crowd behaviour analysis through deep learning: Taxonomy, anomaly detection, crowd emotions, datasets, opportunities and prospects // Information Fusion. 2020. Vol. 64. P. 318–335. DOI: <https://doi.org/10.1016/j.inffus.2020.07.008>.
7. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0) // National Institute of Standards and Technology. 2023. DOI: <https://doi.org/10.6028/NIST.AI.100-1>.
8. Shi T., Guo P., Wang R., Ma Z., Zhang Z., Li W., Fu H., Huijin F., Hao H. A Survey on multi-sensor fusion perimeter intrusion detection in high-speed railways // Sensors. 2024. Vol. 24, No. 17. Article 5463. DOI: <https://doi.org/10.3390/s24175463>.
9. ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management [Electronic resource]. URL: <https://exebit.wordpress.com/wp-content/uploads/2013/11/iso-27005-2011-ru-v1.pdf> (accessed: 28.03.2026). (In Russian)
10. Jumaniyozov T. S. O. G. L. OLIY HARBIY TA'LIM MUASSASALARIDA O'QUV JARAYONINI YANADA TAKOMILLASHTIRISHDA DARS JADVALINING O'RNI // Oriental renaissance: Innovative, educational, natural and social sciences. – 2022. – T. 2. – №. Special Issue 26. – C. 83-87.