

Journal Scientific and Applied Research, Vol. 30, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

INTELLIGENT MANAGEMENT OF LIMITED FUNCTIONALITY MODE UNDER SENSOR FAILURES IN AUTOMATED SECURITY SYSTEMS

Desislava N. Ivanova

Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: d.n.ivanova@shu.bg

Abstract: *Modern automated physical security systems rely on interconnected sensors to monitor conditions and changes in the physical environment. Reliable system operation depends on sensor availability, the trustworthiness of the acquired data, and the relevance of each information source to the function being performed. This paper presents a conceptual model for maintaining limited functionality under partial sensor failure by assessing the functional suitability of the available sensor configuration. The resulting assessment is used to determine the permissible level of automation, while an anomaly indicator is introduced to account for unusual combinations of events.*

Key words: *Intelligent security systems, Automation, Sensors, IoT, Context-aware management, Cyber resilience.*

1. Introduction

The development of the Internet of Things (IoT), intelligent sensors, automation, and machine-based information processing has enabled the design of security systems capable not only of detecting events but also of analyzing acquired information and initiating subsequent actions automatically. Such solutions are used in smart buildings, industrial facilities, access control systems, warehouses and logistics centers, transport facilities, and critical infrastructure. The integration of communication and technical resources is an essential aspect of the design and operation of modern security systems [5]. The broader evolution of intelligent technologies is also characterized by increasing complexity and adaptability, extending the capabilities of automated technical systems [11].

Sensor infrastructure plays a central role in the operation of such systems. It may comprise motion and presence detectors, magnetic contacts, cameras, radio-frequency identification (RFID) readers, biometric devices, temperature sensors, smoke and gas detectors, and other sensing devices. Information obtained from these sources provides the basis for determining the state of the monitored environment and for subsequent automated decision-making.

As the number of connected devices increases, so does the number of potential points of failure. Sensor information may be lost or degraded due to hardware faults, power interruptions, communication failures, energy depletion, incorrect configuration, environmental effects, or deliberate malicious interference.

The resilience of sensor networks to failures has been extensively addressed in the literature. Existing approaches include fault detection and diagnosis, redundancy, network reconfiguration, connectivity restoration, and the use of alternative information sources [1], [4]. Survey studies have also shown that sensor faults can significantly affect the reliability of smart environments [9].

Of particular interest is the assessment of system resilience in the presence of sensor failures. Probabilistic assessment methods reported in the literature consider sensor reliability and the effect of sensor failures on the correct determination of the system state [12].

For automated physical security systems, however, a further issue arises: whether the current combination of available and trustworthy sensor sources provides sufficient information to perform a particular function, and what level of automation can be permitted under the prevailing conditions.

This paper presents a conceptual approach for determining the permissible level of functionality and automation in the presence of partial sensor failure or reduced trustworthiness of sensor information. A set of indicators is introduced to characterize the condition and functional relevance of individual sensor sources, from which an integrated index of functional suitability is derived. The index is then used to determine an appropriate operating mode following a failure while accounting for the current operating context. The approach also considers the assessment of atypical deviations in sensor behavior.

2. Analysis of existing approaches

2.1. Resilience of sensor systems to failures

The reliable operation of automated systems depends to a considerable extent on the condition of the sensors they employ. In distributed sensor systems, individual components may become unavailable as a result of technical faults or communication disruptions [2].

Various methods are applied to mitigate the effects of such failures and to preserve or restore system operation, including approaches for restoring network connectivity following node failures [4], [14]. Existing approaches address fault detection and the subsequent adaptation of the system to its altered operating state [1].

In automated physical security systems, sensor-related problems may involve either loss of information or deviations in the acquired data. A particularly relevant case occurs when a sensor remains operational and accessible, while the information it provides is not sufficiently trustworthy for automated decision-making. Consequently, assessment of the sensor configuration should not be based solely on the operational status of individual devices.

2.2. Trustworthiness of sensor information

The operational status of a sensor does not necessarily guarantee the trustworthiness of the information it provides. A device may operate normally while its readings deviate from the actual state of the monitored object. The reliable use of IoT devices also requires consideration of cybersecurity capabilities that support the protection and trustworthy operation of connected devices [6].

Methods for sensor fault and anomaly detection are used to identify such conditions [9]. These methods allow information from an individual sensor to be evaluated against the expected behavior of the system or compared with data obtained from other information sources.

This distinction is particularly important in automated security systems, since formally valid but untrustworthy information may result in inappropriate automated actions. The ability to maintain a particular function should therefore also depend on the level of confidence assigned to the sensor information being used.

2.3. Preserving functionality under failure conditions

The resilience of an automated system implies the ability to maintain its essential functions under adverse conditions. In the context of cyber resilience, a system is expected to preserve the required functionality while adapting to changes in its operating conditions [8]. This approach is also consistent with cybersecurity risk management practices that emphasize the identification, protection, detection, response, and recovery functions of an organization [7].

A failure does not necessarily require a complete shutdown of system operation. When the available sensor information is insufficient, automated actions may be restricted while retaining only those functions supported by sufficiently trustworthy data.

In physical security systems, the impact of a failure depends on the function supported by the affected sensor. The system response should therefore reflect the role of that sensor and whether the required information can be obtained from alternative sources.

3. Concept of limited functionality mode

In this paper, limited functionality mode is defined as an operating state in which part of the sensor infrastructure is unavailable or provides information of insufficient trustworthiness, while the system retains enough reliable data to perform a defined subset of its functions safely.

The consequences of a sensor failure are not determined solely by the technical type of the affected device. For example, the failure of a corridor camera may have only a limited impact when the same area is covered by several other cameras. A failure of the same type of camera at the entrance to a critical area may have considerably greater consequences when it serves as the only source of visual verification. The impact of a failure therefore depends on the function supported by the sensor, the availability of alternative information sources, the trustworthiness of the remaining information, the protected area, the temporal context, and the current state of the system.

Fig. 1 presents the conceptual sequence of the proposed approach for system management under limited functionality. It covers sensor data processing and the selection of an appropriate operating mode, which subsequently determines the corresponding control action.

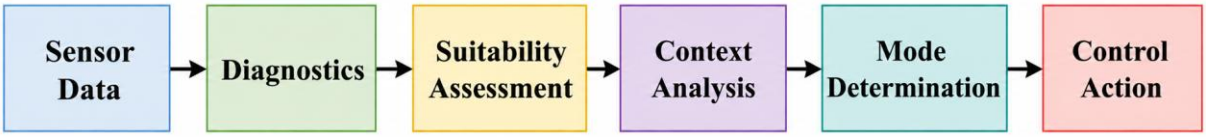


Fig. 1. Generalized scheme of the process for determining the operating mode

The assessment of a specific event and the selection of an appropriate response should be considered within the broader context of security management, where organizational and technical components contribute to maintaining the required level of protection [10].

4. Conceptual model for management under limited functionality

A. Sensor availability

For each sensor *Si*, an availability parameter *Ai* ∈ [0, 1] is introduced. For a completely unavailable sensor *Ai* = 0, whereas a fully available sensor is represented by *Ai* = 1.

B. Trustworthiness of information

The second parameter *Qi* ∈ [0, 1] characterizes the quality and trustworthiness of the information. A higher value of *Qi*, indicates greater confidence in the information provided by the corresponding sensor. At low values, the information is considered insufficiently trustworthy and its influence on automated decision-making is reduced.

The value of *Qi* may be estimated by examining the admissible range of sensor readings, their temporal sequence, historical data, and information obtained from other sensor sources. This distinction allows two different conditions to be identified:

- for *Ai* = 0 the sensor effectively provides no information;
- for *Ai* = 1 and *Qi* → 0 the sensor remains operational, but confidence in the information it provides is substantially reduced.

This distinction is particularly relevant to security systems because the second condition may be more difficult to detect.

C. Functional criticality

The third parameter *Ci* ∈ [0, 1represents the functional criticality of the sensor. It reflects the significance of a particular sensor for the function under consideration. It should be emphasized that *Ci* does not represent sensor reliability; rather, it indicates the importance of the information provided by that sensor for a specific decision.

5. Functional suitability index

To assess the current sensor configuration, a functional suitability index Fs is introduced. It is defined as

$$F_s = \frac{\sum_{i=1}^{n} C_i A_i Q_i}{\sum_{i=1}^{n} C_i}, \quad (1)$$

where n is the number of sensor sources.

Since *CiAiQ*i ∈ [0, 1] the resulting index satisfies $0 \leq Fs \leq 1$.

A high value of *Fs* indicates that the current sensor configuration provides sufficiently trustworthy information to perform the function under consideration. As the value of the index decreases, the ability to perform the function reliably is reduced, requiring corresponding restrictions on automated actions.

It is important that *Fs* not be interpreted as a conventional probability of failure-free operation. Instead, it represents a normalized conceptual indicator of the suitability of the current combination of sensor sources.

6. Context-dependent assessment of sensor significance

When *Ci* is defined statically, the significance of a given sensor is assumed to remain constant. In physical security systems, however, this assumption does not always hold.

For this reason, the following context-dependent formulation is proposed:

$$Ci = Ci\ (t, x, e), \quad (2)$$

where:

t – time of observation;

x – protected area;

e – current event or system state.

The functional suitability index can then be expressed as:

$$F_s(t,x,e) = \frac{\sum_{i=1}^{n} C_i(t,x,e) A_i Q_i}{\sum_{i=1}^{n} C_i(t,x,e)}, \quad (3)$$

his formulation allows the same technical failure to have a different impact on system behavior depending on the specific operating context.

7. Determination of operating modes

To determine the operating mode automatically, three threshold values T_1, T_2 and T_3, are introduced. These thresholds define the boundaries between the different levels of automation, with $T_1 > T_2 > T_3$.

Four operating modes are proposed, as presented in Table I:

Table 1. Operating modes

Mode	Condition	Description
M0 – Normal	$Fs > T_1$	Full automation
M1 – Limited Functionality	$T_2 \leq F_s \leq T_1$	Core automation is maintained with additional verification
M2 – Limited Automation	$T_3 \leq F_s \leq T_2$	Risk-sensitive automated actions are disabled and operator verification is required
M3 – Protective	$Fs < T_3$	Only predefined protective actions are permitted

The use of parameter-dependent control mechanisms is well established in automated technical processes. For example, compensation parameters such as k-Factor (Linear Advance/Pressure Advance) modify system behavior in response to changing process conditions, demonstrating the importance of appropriate parameter selection for maintaining the desired operational quality [3].

8. Anomaly assessment

Technical failures and deliberate interference may produce similar observable effects. For example, loss of communication with a sensor may result from a hardware fault, power interruption, or network problem, but it may also be caused by jamming, device compromise, or intentional disconnection. The model can therefore be extended by introducing an anomaly indicator $P_A \in [0, 1]$. The effect of incorrect sensor indications on system resilience is also relevant in this context, since false alarms may influence both state assessment and subsequent system response [13].

A low value of P_A indicates behavior consistent with common technical failures. As the value of the indicator increases, the observed combination of events is more likely to deviate from the system's typical behavior. For example, an isolated loss of communication with a single sensor may correspond to a low P_A, whereas the near-simultaneous loss of several independent sensors within the same protected area may result in a higher value. The operating mode selection can then be expressed as:

$$M = f(F_s P_A K), \quad (4)$$

where K represents the current operating conditions.

For the same level of functional suitability of the sensor configuration, the system may select different operating modes depending on the degree of detected anomaly. A higher degree of anomaly may result in a more restrictive level of automation due to indications of

atypical system behavior. In this paper, the P_A indicator is introduced at a conceptual level, while the development and experimental validation of a method for its determination are left for future research.

9. Architecture, advantages, and limitations of the proposed model

The proposed model can be represented by the following sequence:

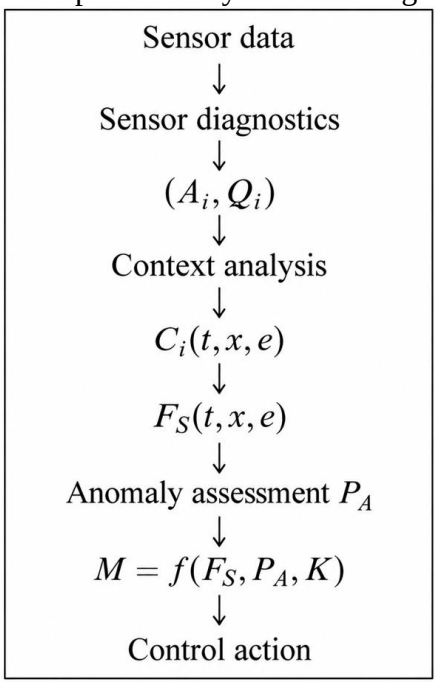


Fig. 2. Architecture of the proposed model

The architecture of the proposed model follows a sequential process for assessing the state of the sensor system and determining the permissible level of automation. First, the incoming sensor data are processed by assessing the operational status of individual sensors and the trustworthiness of the information they provide. The significance of each sensor is then determined with respect to the current operating conditions. The resulting assessments are combined through the *Fs*, index, which characterizes the functional suitability of the sensor configuration.

The degree of anomaly P_A is also taken into account. Based on these assessments, the system determines the appropriate operating mode and the corresponding permissible level of automation.

The proposed approach offers several potential advantages:

- it avoids a purely binary assessment of the state of the automated system. A single failure does not automatically imply that the entire system is unable to perform its functions;
- he distinction between *Ai* and *Qi* allows both completely unavailable devices and technically operational sensors providing information of low trustworthiness to be considered;
- through *Ci* the model accounts for the fact that sensors do not have equal significance for a given function;
- through *Ci = Ci (t, x, e)* the assessment becomes context-dependent. The same failure may have different significance in different protected areas or under different security operating conditions;
- the model allows a gradual reduction in the level of automation M0 → M1 → M2 → M3 rather than an immediate transition from normal operation to the complete suspension of automated actions.

This formulation is consistent with the general principles of cyber resilience, according to which a system should be capable of adapting and preserving its essential functions under adverse conditions [8].

The proposed model also has several limitations:

- he values of Ci must be determined for the specific application and cannot be considered universal;

- the estimation of Qi constitutes a separate and complex problem. In particular, identifying sensors that provide incorrect but formally admissible values remains challenging;

- the thresholds T_1, T_2 and T_3 should be determined experimentally and aligned with the acceptable level of risk;

- (1), used to calculate the functional suitability index, represents a weighted aggregate measure and may be insufficient when sensor sources are strongly dependent. If several sensors share a common communication channel or power supply, their failures cannot necessarily be treated as independent;

- the proposed P_A indicator does not constitute an implemented attack-detection algorithm. A high degree of anomaly does not necessarily indicate malicious interference, but rather the need for additional verification.

10. Conclusion

The Modern automated physical security systems depend on the reliable operation of multiple sensor sources. However, the failure of an individual sensor does not necessarily imply that the system has lost its ability to perform its essential functions. At the same time, maintaining full automation when the available information is insufficiently trustworthy may lead to inappropriate decisions and increased risk.

A conceptual model is proposed for determining the permissible level of automation in the presence of sensor failures or reduced trustworthiness of sensor information. The approach assesses the functional suitability of the current sensor configuration by considering the operational state of the sensors and their significance for the function being performed. This significance may vary according to the current operating conditions; consequently, the same failure may result in different system responses.

Based on the resulting assessment, an appropriate operating mode is determined, allowing automated actions to be progressively restricted. The model also provides for the consideration of atypical behaviour among sensor sources.

The proposed model is conceptual and does not constitute a complete algorithm for sensor fault diagnosis. Its primary purpose is to relate the state of the sensor system to the permissible level of automation, thereby avoiding a binary “operate-or-stop” approach. Further experimental validation is required to determine the threshold values and to assess the applicability of the model in real-world physical security systems.

Acknowledgment

The authors gratefully acknowledge the support provided by the project CoE UNITe BG16RFPR002-1.014-0004 funded by PRIDST, co-funded by the European Union.

References

[1] Adday, G. H., S. K. Subramaniam, Z. A. Zukarnain, and N. Samian. "Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions." Sensors, vol. 22, no. 16, Article 6041, 2022, DOI 10.3390/s22166041.

[2] Avižienis, A., J.-C. Laprie, B. Randell, and C. Landwehr. "Basic Concepts and Taxonomy of Dependable and Secure Computing." IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, 2004, pp. 11–33, DOI 10.1109/TDSC.2004.2.

[3] Bankov, B., Kuzmanov, Z., Tasinov, T., Todorov, T. T., Investigation of the Influence of the k-Factor Parameter on the Quality of Printed Parts Using Ingeo Biopolymer 4043D. Engineering Proceedings, Vol. 150, No. 1, Article 8, MDPI, 2026, DOI: 10.3390/engproc2026150008.

[4] Chouikhi, S., I. El Korbi, Y. Ghamri-Doudane, and L. A. Saidane. "A Survey on Fault Tolerance in Small and Large Scale Wireless Sensor Networks." Computer Communications, vol. 69, 2015, pp. 22–37, DOI 10.1016/j.comcom.2015.05.007.

[5] Dimanova, D., and Z. Kuzmanov. "Development of an Integrated Security and Communication System." International Scientific Refereed Online Journal, no. 63, November 2019, ISSN 2367-5721, pp. 83–91.

[6] Fagan, M., K. Megas, K. Scarfone, and M. Smith. IoT Device Cybersecurity Capability Core Baseline. NISTIR 8259A, National Institute of Standards and Technology, 2020, DOI 10.6028/NIST.IR.8259A.

[7] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, National Institute of Standards and Technology, 2024, DOI 10.6028/NIST.CSWP.29.

[8] Ross, R., V. Pillitteri, R. Graubart, D. Bodeau, and R. McQuaid. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160, vol. 2, rev. 1, National Institute of Standards and Technology, 2021, DOI 10.6028/NIST.SP.800-160v2r1.

[9] Sharma, S., K. Gupta, D. Gupta, S. Rani, and G. Dhiman. "An Insight Survey on Sensor Errors and Fault Detection Techniques in Smart Spaces." Computer Modeling in Engineering & Sciences, vol. 138, no. 3, 2024, pp. 2029–2059, DOI 10.32604/cmes.2023.029997.

[10] Simeonova, I., and Ts. Metodieva. "Model for Administrative Security Management in a Municipality." Journal of Security and Applied Research, no. 26, 2024, ISSN 1314-6289 print, ISSN 2815-4622 online, pp. 93–105.

[11] Tasinov, T. Y. “A Step Up – From 3D to 6D Printing. Possible and Future Applications of New Materials and Technologies in the Technology Education of Students.” In Innovative Models for Implementing Qualifications and Forming Competencies in the Educational System: Collection of Scientific Papers. University Publishing House “Episkop Konstantin Preslavski”, Shumen, Bulgaria, 2023, pp. 286-293. ISBN 978-619-201-732-3.

[12] Yoo, M., T. Kim, J. T. Yoon, Y. Kim, S. Kim, and B. D. Youn. "A Resilience Measure Formulation that Considers Sensor Faults." Reliability Engineering & System Safety, vol. 199, Article 106393, 2020, DOI 10.1016/j.ress.2019.02.025.

[13] Yoon, J. T., B. D. Youn, M. Yoo, and Y. Kim. "A Newly Formulated Resilience Measure that Considers False Alarms." Reliability Engineering & System Safety, vol. 167, 2017, pp. 417–427.

[14] Zeng, Y., L. Xu, and Z. Chen. "Fault-Tolerant Algorithms for Connectivity Restoration in Wireless Sensor Networks." Sensors, vol. 16, no. 1, Article 3, 2016, DOI 10.3390/s16010003.