Integrated Framework Deployment for Cybersecurity of Information and Communication Channels in On-Demand Printing

Tetyana Neroda[1]

[1] *Institute of Printing Art and Media Technologies in Lviv Polytechnic, Bandery St. 12, 79013 Lviv, Ukraine*

Abstract

Recent research in the security of computerized maintenance management systems reveals that conventional cybersecurity mechanisms remain primarily focused on external threats and fail to incorporate the operational specifics of telemetry streams and service log data. Addressing this gap, the present work substantiates the necessity of developing analytical approaches capable of detecting latent vulnerabilities in the information and communication channels of on-demand printing workflows. To this end, an analytical apparatus for real-time vulnerability assessment has been constructed within a multilayered service-oriented architecture. The apparatus integrates models of telemetry, maintenance logs, and risk evaluation into a closed mathematical cycle, thereby enabling a structured transition from heterogeneous big data flows to formalized representations suitable for quantitative analysis. The proposed framework provides metrics-driven insights into the impact of hidden vulnerabilities on production parameters such as throughput stability, workflow continuity, and confidentiality of client orders. Furthermore, it ensures that the outcomes of risk evaluation are directly transformed into executable protection actions, securing information and communication channels in dynamic printing environments.

Keywords

Computerized Maintenance Management Systems, Information System Vulnerabilities, Covert Data Leakage Channels, Predictive Maintenance, Telemetry Data Analytics.

Introduction

In the context of digitalization of operational printing, the role of Computerized Maintenance Management Systems (CMMS) is steadily increasing. These systems integrate data from equipment, sensor subsystems, and software modules to ensure continuity of the production process. Such complexes generate large volumes of information, encompassing maintenance logs, printing machine telemetry, workload data, and downtime records. Traditional approaches to cybersecurity deployment in industrial environments primarily focus on countering external attacks, protecting against malicious software, and controlling access.

At the same time, the issue of covert data leakage channels remains insufficiently studied, particularly those associated with temporal patterns, correlation links between parameters, and metadata accompanying technical information. In the operational printing sector, where the speed of order processing and the stability of printing processes are critical, such vulnerabilities may indirectly reveal confidential information about production organization, equipment utilization, or maintenance planning practices. This creates a rationale for more in-depth research on the risks associated with the security of big data generated by maintenance management systems.

Analysis of Recent Research

Recent scientific studies on the security of Computerized Maintenance Management Systems indicate

increasing risks associated with the processing of large volumes of data and their integration with other information systems. In particular, specialized research emphasizes insufficient attention to vulnerabilities arising from covert data leakage channels, such as temporal patterns, correlation links, and metadata accompanying technical data, which can be exploited for unauthorized access to confidential information about clients, production organization, and maintenance planning [1].

Another important aspect is the integration of CMMS with other enterprise information systems, which can create new vulnerabilities and complicate security management. In particular, research highlights the need to implement centralized patch management systems, utilize endpoint detection and response (EDR) tools, web application firewalls, and network protocol analyzers to ensure the security of such integrated systems [2]. The growing role of artificial intelligence technologies in big data analysis opens new opportunities for anomaly detection and predictive maintenance. However, this also introduces new security challenges, particularly in the context of protecting machine learning algorithms from manipulation and ensuring the transparency and explainability of AI-driven decisions [1, 3, 4]. Risks associated with data manipulation do not necessarily involve information theft, but rather covert alteration of data to gain advantage or influence processes. Such modifications can be subtle and difficult to detect, yet they may have serious consequences for the organization. Protection against these attacks requires the implementation of anomaly detection mechanisms, data integrity assurance, and regular system audits [5]. The use of cloud technologies for storing and processing CMMS data can also increase system flexibility and efficiency, but it introduces additional security challenges. Specifically, it is necessary to prevent data leakage, ensure compliance with regulatory requirements, and implement effective access control mechanisms. Given the growing adoption of cloud technologies, it is crucial to develop security strategies that take into account the specific characteristics of these environments [6].

The analysis of recent research has shown that the presented results are mostly limited to general approaches to the security of industrial systems, without considering the specifics of printing production. They primarily focus on standard aspects such as patch and software update management, without a detailed analysis of threats inherent to printing processes. Existing open-access publications pay insufficient attention to the detection of covert vulnerabilities that can be exploited for unauthorized access to confidential information, including temporal patterns, metadata, and correlation links in telemetry and maintenance logs. The implementation of interactions between various components of maintenance management complexes, including middleware, integrated sensor networks and data collection modules, is often overlooked, which complicates the prediction of potential attack paths and the assessment of risks for production processes. Furthermore, most studies do not take into account the specifics of order processing in operational printing, the speed of changes in production workflows, and their interconnection with order management systems, which creates additional opportunities for covert information leakage. Therefore, there is a pressing need to deploy an analytical framework for identifying hidden vulnerabilities within industrial infrastructure and to further assess their potential impact on production processes and information security. This opens opportunities for the development and implementation of real-time protection strategies for information and communication systems in operational printing environments.

Problem statement

Multilevel information and communication links between printing equipment in modern industrial lines, management servers, cloud services, and user interfaces pose the threat of emerging risks that go beyond traditional notions of security. Vulnerabilities may arise not only at the level of direct system access but also through indirect channels, including telemetry, maintenance logs, and machine workload data. Such leaks can indirectly reveal production cycles, equipment configurations, order characteristics, and organizational specifics of enterprise operations, complicating the development of a comprehensive framework for assessing potential threats and predicting their impact on the production infrastructure. In conditions of martial law and intensified competition in the printing services market, such leaks carry the risk of disclosing confidential information about clients, commercial terms of cooperation, and organizational features of production. Therefore, the objective of the present study is to develop an analytical framework for identifying such vulnerabilities, assessing their impact on the stability of production processes, and determining ways to prevent potential threats to the security of production data and the protection of client interests.

Service Architecture for Hidden Vulnerability Detection

The architecture of a service framework for detecting hidden vulnerabilities within CMMS environments involves the development of a multi-layered model for processing production telemetry and maintenance logs. Its purpose is not only to identify known anomalies but also to establish correlations that remain unnoticed in traditional monitoring systems. This approach is based on multichannel data collection from printing equipment, microclimate sensor modules, CMMS scheduling modules, and user interfaces.

The first level involves the normalization of telemetry streams, which enables the alignment of data in different formats and the elimination of temporal discrepancies in their acquisition. This provides a foundation for the subsequent integration of technical and organizational parameters. The second level focuses on the detection of latent dependencies in maintenance logs, where relationships between technical service events, such as the frequency of component replacements or the recurrence of equipment failures, are considered potential indicators of vulnerabilities in software or hardware.The third level is aimed at assessing information risks associated with side-channel data leakage. For instance, the analysis of the frequency of service module accesses or the duration of preventive operations can indirectly reflect production load schedules or specifics of cooperation with particular clients. This forms the basis for constructing a production activity profile, which, in the case of unauthorized access, could become a source of confidential information.

The final stage involves the integration of results into a unified assessment system, which combines detected technical anomalies with potential data security threats. The proposed architecture enables a quantitative evaluation of the impact of hidden vulnerabilities on the stability of production processes and the level of data protection, while also providing a foundation for the development of real-time preventive measures.

Analytical Framework for Real-Time Vulnerability Assessment

The analytical framework for detecting hidden vulnerabilities within CMMS environments in operational printing is proposed to be built on a defined multi-layered architecture, with each level having its own system of formalized dependencies. This approach provides not only a technical description of information flows but also the capability to quantitatively assess their impact on the stability of production processes and information security.

At the first level, the normalization of telemetry streams from printing equipment is considered. Telemetry is presented as a set of discretized temporal patterns t_i, within which a parameter v_i is recorded, allowing for the tracking of periodicity or anomalies in the data based on the recorded "time–value" pair within the studied interval (1):

$$\boldsymbol{T} = \{ (t_i, v_i) \}. \quad (1)$$

To eliminate gaps and synchronize time scales, a normalization operator $N : T \rightarrow T^*$ is applied, which transforms the original data into an aligned set T^*. This allows for the correct correlation of data from different sources.

The second level concerns maintenance logs, which are described as a set of events of type ℓ_j (for example, a fault code or operation description) with corresponding attributes a_j, indexed by the event number or entry in the maintenance log (2):

$$\boldsymbol{L} = \{(\ell_j, t_j, a_j)\}, \quad (2)$$

To identify latent dependencies between logs and telemetry, a correlation operator $C\ (T^*, L) \rightarrow D$ is introduced, which generates a set D of hidden dependencies that are not captured by standard monitoring tools.

The third level is focused on assessing the risks of side-channel data leakage. Here, for the time intervals Δt between events and weighting coefficients of different event types, a risk function is formulated (3):

$$\boldsymbol{R} = f(D, \Delta t, k) \quad (3)$$

The obtained value $\boldsymbol{R}$ provides a numerical assessment of risk or a vulnerability indicator, enabling the system to make real-time decisions (for example, initiating equipment checks, blocking suspicious communications, or generating alerts for the operator). Overall, this is interpreted as the probability that telemetry or logs indirectly reveal information about production loads or printing order data.

At the fourth level, the results are integrated into a unified assessment of the impact on production processes and information security. For this purpose, production process stability metrics $\boldsymbol{Q}$, which include average downtime, number of equipment failures, and duration of preventive maintenance, are processed through an integrated indicator reflecting the security status within the system via the assessed risk level and the quality or condition of control parameters (4):

$$\boldsymbol{S} = g\ (\boldsymbol{R}, \boldsymbol{Q}) \quad (4)$$

The value $\boldsymbol{S}$, aggregated through weighting coefficients, the "minimum" rule, a probabilistic model, or another analytical approach, allows for the quantitative determination of threat levels (such as acceptable, potentially hazardous, or critical) and supports decision-making regarding the necessity of protective actions in real time. As a result, model (4) enables the transition from abstract risk to a concrete assessment of the security state, which directly guides the actions of the protection system or operator interventions.

The proposed framework formalizes the architecture for analyzing telemetry and maintenance logs, transforming it into a system of mathematical operators and functions that ensures the detection

of hidden vulnerabilities and the prediction of their impact on production processes and information security in operational printing. The generalization of the integrated indicator $\boldsymbol{S}$ in the form of a threshold-based classification model provides a formalized delineation of security levels (OK, ALERT, CRITICAL) based on configurable thresholds θ_1 and θ_2, enabling the implementation of unified response criteria within the designed framework (5):

$$S = \begin{cases} \text{OK}, & S < \theta_1 \\ \text{ALERT}, & \theta_1 \le S < \theta_2 \\ \text{CRITICAL}, & S \ge \theta_2 \end{cases} \quad (5)$$

It should be noted that the classification model (5) is not self-sufficient without further interpretation of its results in the form of specific response procedures. Therefore, the next stage involves transitioning to an action function, which transforms the classification states into operational rules executed in real time, ensuring both the integrity of telemetry streams and the protection of information and communication channels from the further development of incidents (6):

$$act(S) = \begin{cases} \text{logging and monitoring}, & S < \theta_1 \\ \text{incident recording, access restriction}, & \theta_1 \le S < \theta_2 \\ \text{emergency procedure initiation}, & S \ge \theta_2 \end{cases} \quad (6)$$

Thus, by combining telemetry models, maintenance logs, and integrated risk assessment, the presented analytical framework (1)–(4), with the introduction of threshold values (5), culminates in an action function (6) that formalizes the selection of operations in real time based on the security level. This design enables the transition from abstract analysis to the automated execution of specific response procedures, creating a closed loop from data collection to practical application. Within the integrated framework, this approach not only allows for the detection of hidden vulnerabilities but also directly transforms assessment results into protective actions, ensuring the resilience of information and communication channels in operational printing against threats in a dynamic production environment.

Conclusions

The developed analytical apparatus integrates telemetry models, maintenance logs, risk assessment, and a composite security indicator, thereby forming a closed loop that transforms industrial big data into actionable decisions. This construction ensures systematic incident response, automation of protection procedures, and elastic integration of security analysis mechanisms into the production infrastructure without compromising its operational stability. The scientific novelty of the study lies in the formalized combination of telemetry and maintenance log analysis with a mathematical classification model of security states and the action function *act*(***S***), which defines real-time response rules. Such a configuration enables the transition from abstract risk evaluation to algorithmically implemented protective procedures and provides the capability to assess risks of indirect data leakage channels within production environments. The practical significance of the obtained results is determined by the adaptability of the integrated framework to diverse operational printing configurations, enhancing the level of cybersecurity without reducing order execution efficiency. Furthermore, the application of the analytical apparatus enables quantitative forecasting of the impact of hidden vulnerabilities on the stability of production processes and ensures the preservation of customer confidentiality, which is particularly significant in a

dynamic information and communication environment.

Declaration on Generative AI

The author have not employed any Generative AI tools.

References

1. Durnyak, B., & Romanyshyn., Y. (2023). Protection of a Printing Company with Elements of Artificial Intelligence and IIoT from Cyber Threats. *Advances in Artificial Systems for Logistics Engineering* III (pp.197-205). DOI:10.1007/978-3-031-36115-9_19
2. Aldea, M., & Gheorghică, D. (2020). Software vulnerabilities integrated management system. In 2020 13th International Conference on Communications (COMM) (pp. 111–116). DOI: 10.1109/COMM48946.2020.9141970
3. Shankar, L., Singh, C. D., & Singh, R. (2024). AI and CMMS: A powerful duo for enhanced maintenance in manufacturing. Educational Administration: *Theory and Practice*, 30(10), 1–10. DOI: 10.53555/kuey.v30i5.4434
4. Wieczorek, A. (2023). Assessment of usefulness of CMMS class system for Industry 4.0 enterprise. *Scientific Papers of Silesian University of Technology. Organization and Management Series*, 182, 1–12. DOI: 10.29119/1641-3466.2023.182.33
5. Lu, Y. J., Lee, W. C., & Wang, C. H. (2023). Using data mining technology to explore causes of inaccurate reliability data and suggestions for maintenance management. *Journal of Loss Prevention in the Process Industries,* 83, 105032. DOI: 10.1016/j.jlp.2023.105063
6. Arafat, M. (2018). Information security management system challenges within a cloud computing environment. In Proceedings of the International Conference on Future Networks and Distributed Systems (pp. 1–7). DOI: 10.1145/3231053.3231127
7. Mugarza, I., Flores, J. L., & Montero, J. L. (2020). Security issues and software updates management in the industrial internet of things (IIoT) era. *Sensors*, 20 (24), 7160. DOI: 10.3390/s20247160
8. Yadav, G., Paul, K., & Gauravaram, P. (2022). Vulnerability management in IIoT-based systems: What, why and how. *In Secure and Trusted Cyber Physical Systems* (pp. 1–27). Springer. DOI: 10.1007/978-3-031-08270-2_3
9. Kosmowski, K. T., Piesik, E., Piesik, J., & Śliwiński, M. (2022). Integrated functional safety and cybersecurity evaluation in a framework for business continuity management. *Energies*, 15(10), 3610. DOI: 10.3390/en15103610
10. Sappal, S., & Prowse, P. (2021). A cybersecurity vulnerability management system for medical devices. CMBES Proceedings, 44.