Medicon Engineering Themes
Volume 9 Issue 2 August 2025
Article Type: Mini-Review
ISSN: 2834-7218

Assessment of Operational Risk for Medical Equipment

Calin Corciova*

Associate Professor, Department Medical Sciences, Medical Bioengineering Faculty, "Grigore T. Popa" University of Medicine and Pharmacy, Iasi, Romania

***Corresponding Author:** Calin Corciova, Associate Professor, Department Medical Sciences, Medical Bioengineering Faculty, "Grigore T. Popa" University of Medicine and Pharmacy, Iasi, Romania.

Received: August 31, 2025; **Published:** September 29, 2025

DOI: 10.55162/MCET.09.296

Abstract

Assessing operational risk for medical equipment is a cornerstone of providing safe and reliable medical services. This short article summarizes methods and practices reported in the literature between 2015 and 2024 and compares them with international standards (ISO 14971:2019; IEC 80001-1:2021). A structured search was conducted in PubMed, IEEE Xplore, and Scopus using keywords such as "operational risk", "medical device", "FMEA", "FTA", "Bayesian network", and "medical technology management". Inclusion criteria covered English-language peer-reviewed studies describing methods, comparisons, or case applications for operational risk of medical equipment; purely financial or market risk papers were excluded. The findings indicate that FMEA and FTA remain the most widely used tools, but they may underrepresent the dependencies between failure modes and face higher-order uncertainties. Hybrid and probabilistic approaches (e.g., Bayesian networks, Markov models, Monte Carlo simulation) address some of these gaps but require richer data sets and validation. Cyber security risks and interoperability challenges in IT networks that incorporate medical devices are inconsistently integrated into current practice. We conclude that combined methodologies, explicit treatment of uncertainty, and comparative empirical studies are needed to advance operational risk assessment and support patient safety and system resilience.

Keywords: operational risk; medical equipment; risk management; patient safety; standards; FMEA; FTA; Bayesian networks

Abbreviations

FMEA:	Failure Modes and Effects Analysis.
FTA:	Fault Tree Analysis.
MTBF:	Mean Time Between Failures.
MTTR:	Mean Time to Repair.
IT:	Information Technology.
IoT:	Internet of Things.
RPN:	Risk Priority Number.
QoS:	Quality of Service.
CMMS:	Computerized Maintenance Management System.

Introduction

Rapid advances in biomedical technology and widespread interconnection of medical devices have transformed diagnosis, monitoring, and therapy. At the same time, the provision of health care has become increasingly dependent on the availability, reliability, security, and interoperability of technical equipment. Operational risk - understood here as the possibility of events that affect availability, functionality, safety, or cyber security of equipment - stems from factors such as component ware, software or firmware defects, inadequate maintenance, human factors, environmental conditions, and vulnerabilities introduced by IT network integration. The consequences range from temporary delays to adverse events that affect patient safety. This review aims to provide a concise but critical review of the methods used to assess and control operational risk for medical equipment, highlighting strengths, limitations and gaps and outlining directions for future work [4].

In this context, operational risk assessment becomes an indispensable process in the management of medical equipment, with the role of identifying, analyzing and prioritizing risks, so that prevention and control measures can subsequently be implemented. Relevant international standards, such as ISO 14971:2019 and IEC 80001-1:2021, provide the methodological framework for the application of risk management principles in the medical field, integrating clinical, technical, and organizational aspects. At the same time, risk assessment should not be viewed only as a compliance requirement, but as a strategy for continuous improvement of the quality and safety of the medical act. By correlating the results obtained with performance indicators (uptime, maintenance costs, frequency of incidents), the assessment process becomes a management tool that contributes to the sustainability of the healthcare system [3-5].

Risk management for medical devices is anchored in ISO 14971:2019, which structures risk analysis, evaluation, control, and post-market surveillance. For IT-networks that incorporate medical devices, IEC 80001-1:2021 addresses responsibilities and risk management processes spanning safety, effectiveness, data, and system security. Complementary guidance is available in ISO/IEC 31010 regarding risk assessment techniques. Within this framework, operational risk reflects both safety and security considerations; therefore, integrated approaches are required.

Materials and Methods

Sources and search strategy

PubMed, IEEE Xplore, and Scopus literature published between January 2015, and August 2024 were searched. Search strings combined controlled terms and free text, for example, "(operational risk or reliability) and (medical device or medical equipment)", "FMEA", "FTA", "Bayesian network", "Markov", "Monte Carlo", "medical technology management" and "IEC 80001".

Inclusion and exclusion criteria

Articles in English presenting methods, comparisons, or case studies focused on the operational risk of medical equipment or IT networks incorporating medical devices were included in the analysis. The following were excluded: editorials, articles focused exclusively on market/financial risk, or those without methodological relevance.

Study selection process

Records were selected by title and abstract, and full texts were then assessed for eligibility. The data were plotted to capture the method class (e.g., FMEA, FTA, probabilistic), data needs, results, and limitations. Given the size and heterogeneity, no meta-analysis was attempted. rather, a narrative and comparative synthesis is the only approach.

Comparative analysis of risk assessment methods

Failure mode and effects analysis (FMEA/FMECA)

Advantages: widely understood, facilitates multidisciplinary discussions, provides structured prioritization through RPN (or variants).

Limitations: may overlook dependencies between failures; RPN combines scales; sensitive to subjective scoring; limited representation of uncertainty. Improvements include the use of separate prioritization metrics (S, O, D), fuzzy logic, or coupling with probabilistic models.

Fault tree analysis (FTA)

Advantages: top-down logic captures combinations of basic events that lead to an undesirable top event; supports qualitative and quantitative analysis.

Limitations: model complexity grows rapidly; requires credible probability data; static structure may not capture dynamic operational contexts.

Probabilistic and hybrid approaches

Markov models and Monte Carlo simulation support time-dependent reliability estimation (e.g., MTBF, MTTR) and maintenance strategy evaluation. Bayesian networks (including dynamic and hybrid forms) model conditional dependencies and update beliefs with new evidence, filling the gaps left by purely deterministic methods. However, these approaches require greater data maturity and specialized expertise, and their results must be communicated transparently to stakeholders [1].

Illustrative Cases

Case 1: Ventilator alarm failure and sensor drift

Context: Intermittent false negative alarm due to sensor drift and firmware threshold limitation. Assessment: Initial FMEA identified high severity but moderate incidence; subsequent Bayesian update - using maintenance logs - revealed higher conditional risk in certain humidity/temperature profiles. Control: Firmware correction, tighter environmental controls, and preventive replacement interval reduced risk to tolerable levels; monitoring dashboards added to track alarm performance.

Case 2: Infusion pump dosing error after software update

Context: Post-update incompatibility with drug library resulted in rare but critical bolus miscalculations. Assessment: FTA exposed a minimum cutoff set involving network latency and library synchronization failure; Monte Carlo simulation estimated the probability of the incident under different latency distributions. Control: Versioned updates with rollback, network QoS, automated library integrity checks, and user training; residual risk was reassessed as acceptable.

Implementation of Control Measures

Control strategies should combine preventive and predictive maintenance, standardized operating procedures, competency-based training, spare-parts logistics, and cybersecurity controls (asset inventory, hardening, patch management, network segmentation, anomaly detection). For high-criticality equipment, redundancy and fail-safe design reduce single points of failure. Digital monitoring (IoT/CMMS) supports early anomaly detection; alerts must be tuned to minimize alarm fatigue [2]. Risk management is iterative. Key indicators include uptime/availability, incident rates per 1,000 device-days, mean time between failures (MTBF), mean time to repair (MTTR), maintenance cost per operating hour, patch latency, and number of cybersecurity non-conformities. Periodic technical audits and post-incident reviews inform updates to the risk register and to control measures.

Discussion

Systematic implementation of operational risk assessment brings direct benefits such as patient safety (reduction of adverse events caused by defects or incorrect use), economic efficiency (reduced costs by preventing major breakdowns and optimizing the life cycle of equipment). Another aspect that needs to be considered is compliance and accreditation (support in complying with international regulations and obtaining quality certifications) and organizational culture oriented towards safety - the involvement of medical and technical staff in prevention processes.

Conclusion

Operational risk assessment for medical equipment benefits from a structured, standards-aligned, and data-informed approach. Classical methods provide accessible starting points but are insufficient alone in modern, networked contexts. Adopting hybrid methodologies, explicitly modeling uncertainty, integrating cybersecurity, and conducting empirical comparative studies can meaningfully reduce residual risk and enhance patient safety.

References

1. Dhillon BS. Medical Device Reliability and Associated Areas. CRC Press (2011).
2. Freyer S., et al. "Integrating cybersecurity into benefit-risk assessment for medical devices" (2024).
3. Hunte N., et al. "A hybrid Bayesian network for medical device risk assessment and management" (2022).
4. International Electrotechnical Commission. IEC 80001-1:2021. Application of risk management for IT-networks incorporating medical devices—Part 1: Safety, effectiveness and security in the implementation and use of connected medical devices or systems (2021).
5. International Organization for Standardization. ISO 14971:2019. Medical devices—Application of risk management to medical devices. International Organization for Standardization (2019).
6. International Organization for Standardization. ISO/IEC 31010:2019. Risk management—Risk assessment techniques. International Organization for Standardization (2019).
7. European Parliament and Council. Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices (MDR).
8. Khinvasara Tushar, Ness Stephanie and Tzenios Nikolaos. "Risk Management in Medical Device Industry". Journal of Engineering Research and Reports. 25. (2023): 130-140.
9. Smith J, Brown L and Y Zhang. "Risk management practices in healthcare technology management". J Clin Eng 46.3 (2021): 145-153.

Volume 9 Issue 2 August 2025