Automation-Driven Reliability Engineering for Public-Sector Biomedical Systems

(Author Details)
Prudhvi Raju Mudunuri
Independent Researcher, USA

Abstract

One of the fundamental requirements of the biomedical systems of the state that takes part in the support of the national research and the national health programs is reliability. These are mission-sensitive platforms that are very sensitive as regards maintenance because any slight failure can lead to severe consequences. The paper will discuss how reduced reliability engineering through automation can be applied to enhance the resiliency of the systems and this is particularly in cases where the systems are operating on a limited regulatory framework. It takes into account among the most significant practices, including self-healing pipelines, automated rollback plans, and telemetry-based monitors to strengthen the performance of the system and minimize disruptions. Such systems can independently detect and react to failures with the aid of automation so as to reduce the possibility of occurrence of incident and speed up recovery. The research demonstrates that incident rate and recovery duration have greatly been reduced with time which is due to the study that is conducted longitudinally which justifies the value of such automation plans in providing continuity of operations. It has shown that the practices can be used to create fault tolerant and high availability architectures that can be used to meet the demands. Besides, the paper discusses the telemetry-based monitoring as the means of enhancing the reliability of services through the integration of real-time data to implement a quick response and make decisions. Overall, this research demonstrates that automation is essential in promoting credibility of biomedical platforms, which also offers helpful information as to how such systems can be capable of responding to the changes, which are being made, and at the same time meet the regulatory and operational demands. The results can be used as a guide toward the implementation of automation architectures into government-based IT infrastructure, which facilitates the resilience of systems, as well as their efficiency in key biomedical services.

Keywords: Reliability Engineering, Automation Frameworks, Biomedical Platforms, Public-Sector IT, System Resilience, Fault Tolerance, Self-Healing Systems, Incident Reduction, Telemetry-Driven Monitoring

DOI: 10.21590/ijhit.05.01.6

1. Introduction

The biomedical systems of the public sector that are under the patronage of the national research and missions of public health play the fundamental role in regard to the global health issues as well as responding to the pandemics, developed medical research and health service provision. These systems are sometimes of a mission-critical nature, when even the shortest delays or system crash might have extended implications. What is important is to ensure that they are functional at all times and because of this, a strategic approach needs to be adopted in the design and maintenance of the systems. Reliability engineering is one of the elements towards this kind of approach, and it is the practice of having systems that will run their intended tasks without failure over time [1].

With the ever increased complexity of biomedical systems, it has become more significant to incorporate automation-oriented practices in reliability engineering. In the framework of system reliability, automation is the use of technology and procedures that enable systems to spot, track and correct faults without the need of the human factor. The evolution of reliability engineering based on automation is a disruptive change in the design, maintenance, and optimization of biomedical platforms. Such systems do not just wait until problems are detected and corrected by manual means, but are capable of anticipating possible problems, automatically take corrective measures, and continue services with minimal downtimes [2].

This paper will address the issue of automation to make public-sector biomedical systems more resilient, especially in cases of regulatory limitations. Strict regulations and standards have regulated the biomedical systems in order to ensure that they are in line with the national and international health, safety, and privacy laws. These sets of regulations complicate the maintenance of the system where high availability and reliability are not enough but also the strict adherence to the industry standards are necessary. The dilemma, thus, comes in terms of how we can combine automation in a manner that enhances the system resiliency without violating these regulatory mandates.

Systems that must offer life-critical services are important to reliability engineering, including biomedical platforms. Such systems should be reliable so that they are able to serve national health agenda, carry out research, and offer critical healthcare services. Reliability engineering is concerned with the capacity of a system to execute the intended functions without failure within the mentioned conditions within a given duration of time. This may apply in a biomedical system by making sure that vital applications, namely patient monitoring system, laboratory information system and health data management platform, are continuously running with no downtime or loss of data [3] [4].

Reliability in the biomedical systems of the public sector cannot be achieved only through the identification of possible failures and their removal, but through the creation of strategies that may bring the solution to the system to recover within a short period of time and to resume performing the services in a manner that has the least effect on it. Reliability engineering is thus not simply the idea of failure prevention but is also the design of fault-tolerant, adaptive and self-healing systems.

Historically, biomedical systems have been limited to hand interventions to remedy failures including the engagement of backup systems, patches in the system or launching of disaster recovery systems. Although these measures are critical in ensuring the integrity of the system, they may be time-consuming, resourceful, and have high chances of human error. The rising complexity of biomedical systems and the rising requirements of the users and the ever-present risk of cyber attacks have highlighted the necessity of more complex and automated solutions to provide reliability.

Reliability engineering is driven by automation in response to the growing demands to have more efficient, scalable and resilient systems in the biomedical environments of the public sector. The automation technologies will help decrease the use of human interference, decrease downtimes, and shorten the recovery periods after incidents. These features can be particularly useful in terribly important systems, in which a downturn can have devastating consequences and a single outage can be disastrous [5].

Self-healing pipelines are one of the automation technologies. They are automated functions that identify failure or errors in real-time, identify the problem, and take corrective measures without necessarily involving a human. Self-healing systems are set in such a way that they automatically change configurations to a backup, or activate predetermined recovery operations in case of a fault. An example is a biomedical application which has failed and the self-healing pipeline will automatically redirect the application to the backup server or rollback the system to the last stable state. This will minimize downtime and will keep things running even in the worst of circumstances such as unforeseen failures.

Automated rollback strategies are another important practice in automation. Rollbacks serve to help the systems be restored to a known and stable point following an error or failure and then resume functionality without much manual intervention. As a biomedical system, automated rollback may make sure that when an update or patch is causing havoc or causing the system to crash, the system can automatically roll back and reduce interruption with the services. The automated rollbacks are specifically essential in systems with frequent updates or patches, including surveillance of public health, or research systems, where the risk of bugs or vulnerability introduction in the event of updates is considerable [6] [7].

More so, the monitoring that is telemetry-based is a necessary automation-based practice in securing system resilience. Telemetry is the gathering of information associated with the system performance, system errors and other important metrics. Telemetry-based monitoring systems may be used to monitor the health of a biomedical platform continuously which will provide real-time information about the potential issues and allow preventing problems before they occur. Telemetry tools are automatable and may notify administrators or even make corrective actions in case of anomalous behavior, including slowdowns of systems, hardware failures, or security breaches. The ability to recognize and find solutions to the problems before they escalate into a complete collapse of the whole system is a significant advantage when it comes to providing high levels of reliability of service delivery.

In as much as there are numerous benefits of automation in enhancing the resilience of the system, there are its fair share of challenges. The greatest problem is to offer automated solutions that have regulatory features. Biomedical systems experience very stringent conditions, and the norms are worldwide and national and international in nature such as the Food and Drug Administration (FDA), the European Medicines Agency (EMA), and the Health Insurance Portability and Accountability Act (HIPAA). These rules typically relate to traceable systems, audit-log-enabled systems, data-secure and data-private systems.

The necessity to add automation to these structures must be in the light of compliance and auditability. The automated rollback strategies are one such example, they must be in such a way that they maintain a record of all changes that have been done on the system such that they will be able to trace and review any action that the system has performed in the event of need. Likewise, the processes of self-healing should be visible, with the administrators being able to see what the system does, and confirm it through regulations.

There is also the difficulty in the complexity of automation integration in heterogeneous and diverse systems. Biomedical systems consist of diverse sub systems each with architecture, protocols, and dependencies. It is important that ensuring that automation will be effective in all of these subsystems will need strong integration solutions, and the creation of automatic processes that will be able to accommodate the specifics of each component [8] [9].

Since biomedical systems will remain a key ingredient in underpinning national health programs, their reliability will become more important. Reliability engineering based on automation is a possible solution that can be applied to improve system resiliency, lessen the time spent in downtimes and decrease recovery periods in biomedical systems within the public sector. Self-healing pipelines, automated rollback policies, and Telemetry-based monitoring are some of the practices that can help to enhance the fault tolerance, continuity of operation, and service reliability in such platforms significantly. However, the implementation of these automated practices must be used cautiously in a way that they are able to be in compliance with the regulatory requirements and as well as suit the complexity of different biomedical systems. The biomedical platforms, which the government operates, can thus become more resilient, adaptable and efficient in an ever-changing highly dynamic technological landscape through the implementation of automation, and, as such, it still becomes possible to continue pursuing meaningful health and research agendas in a productive way.

2. Current Challenges in Automation-Driven Reliability Engineering for Public-Sector Biomedical Systems

The reliability engineering through automation has considerable merits in enhancing resilience of the system in the perspective of the biomedical platforms of the public sector but the introduction and exploitation of such automated systems is related with a chain of challenges. These challenges encompass the capacity to address the demanding regulatory demands besides the difficulty of systems integration and the need to undertake constant observation and adaptation to the new threats. These challenges need to be learned in order to effectively implement automation-based strategies that will not only enable a system to be reliable, but will also ensure that the major processes in healthcare and research processes are safe and compliant.

1. Regulatory Compliance and Auditability

One of the most pressing issues when it comes to automating the reliability engineering in biomedical systems can be described as the necessity to comply with the complex system of regulations governing the biomedical platforms of the public sector. The regulations provided by the national and international authorities, such as U.S. food and drug administration (FDA), European Medicines Agency (EMA) and the health insurance portability and accountability act (HIPAA) impose strict conditions of the system behavior, data safety and disclosure.

Solutions that involve automation like self-healing pipes and automated roll back policies may present a big obstacle here. An example is that the automated rollback mechanisms should be such that any modification that occurs to the system is logged and can be audited so as to comply with the regulatory requirements with respect to traceability. In case of a rollback caused by a failure, regulators should be capable of tracing the version of the system that was in operation, the changes that have been made and the reason of the rollback. In the same way, self-healing mechanisms that automatically decide on system recovery should be open, and the actions performed by them should be well documented with the available reasoning and adherence to the set standards.

To automate the reliability engineering process, and comply with the regulatory standards, there must be a balance between the efficiency of the operation and the documentation and the transparency necessitated by the regulators. This can frequently create a more complex system design and add more strain to the developers and operators to make it absolutely compliant.

2. Complexity of System Integration

Practically, the public-sector biomedical platforms consist of a combination of various and diverse systems and technologies, the architecture, protocols, and dependencies of which are often different. Such systems could be patient monitoring systems, electronic health record (EHR) systems, laboratory information management systems (LIMS) among others. There is a big challenge of integrating automation tools in such systems which are quite heterogeneous.

A biomedical platform can contain various sub-systems that can also be operating at varying levels of complexity and at varying software versions, configurations and hardware frameworks. It is therefore not a simple task to roll out an automation structure that can have a smooth running of all these sub systems. Each of the subsystems may have unique failure modes, recovery processes and performance characteristics and automatic solutions to the issue are thus challenging to design.

Along with this there may be in place the legacy systems that were not originally designed to embrace automation and therefore would have to be redesigned or modified sufficiently in order to have automation based-reliability engineering. This implies that automation in such places is often a struggle to deal with technical debt, compatibility, and emphasize on a strong integration layer capable of supporting the complexity of multiple subsystems operating.

3. Data Security and Privacy Concerns

Considering that the information which is handled by public-sector biomedical systems is sensitive, data security and privacy are of high priority. The automation solutions (self-healing systems, telemetry-based monitoring, etc.) depend crucially on the data gathering and real-time analysis to identify the problems with the system and resolve them. Such information may be in the form of personally identifiable information (PII), health data and other highly sensitive data.

The more aggressive use of automated systems to monitor, administer, and sustain these platforms leads to the feeling that there can be certain vulnerabilities like the unauthorized access to sensitive data, data breaches, or cyber-attacks on the automation frameworks. The automated system breach can lead to widespread disruptive impacts of both the system availability and patient and research data protection.

As the automation spreads out in the medium of biomedicine, the necessity of ensuring that the cybersecurity is well sound, assumes a central focus. This includes making sure that automated systems are secured when communicating, that telemetry information is encrypted and that automation is not introducing new attack vectors. As well, automated systems are to be created with built-in safeguards against any accidental or malicious manipulation of the data and settings of the system.

4. Handling Unforeseen or Unpredictable Scenarios

Although automation provides more reliability and self-healing and fault-tolerant capabilities, automation is not foolproof. Automated systems are programmed to deal with pre-programmed failure modes, on the basis of previous data and anticipated system responses. Nonetheless, bio-medical platforms have been known to exist in changing and highly volatile settings in which unexpected scenarios or unanticipated events may occur. Such situations may be as a result of external factors which may include a change in system configurations, updates, cybersecurity attacks or even unforeseen human mistakes.

The automation structures should be designed with the ability to respond to such unexpected occurrences. Nevertheless, it is a complicated task to develop such flexible systems and make them reliable and compliant. The automation systems should be smart as to identify when they detect an anomaly that is beyond their programmed parameters and either escalate the problem to a human level or adjust itself autonomously without going beyond operational and regulatory controls.

Also, the systems should have effective error handling and recovery mechanisms that should be incorporated in case the automation is unable to address the problem completely. This has to be tested and refined to make sure that the automated solutions are ready to deal with every possible failure mode and that there is a fallback mechanism should the automation fail to deal with a certain problem.

5. Continuous Monitoring and Maintenance of Automated Systems

When automation structures are already established, they need maintenance and constant check-ups to detect whether they are working as intended and they are not leading to any unforeseen outcomes. Even the most advanced automated systems require a consistent upgrade to remain in line with the changing standards, compliance regulations and new cybersecurity threats.

Since biomedical platforms are sensitive to national health and research agendas, failure to check or improperly manage automated systems may lead to considerable service downtimes or a breach of regulatory requirements. There should be continuous monitoring to check system performance and spots anomalies as well as monitor automated recovery processes to make sure they are functioning as intended.

Moreover, change in the systems in use can be brought by the development of technology and the automation tools must be modernized. This can be an update of software libraries, alteration of regulations or development of new technologies that can impact the operations of the systems. In this respect, proactive maintenance approach should be implemented to assist in maintaining the automation tools in the state of current and ensuring that they are functioning correctly in every part of the system.

Even though the idea of automation-driven reliability engineering has a tremendous prospect of improving the resilience and efficiency of the biomedical systems of the public sector, these technologies are combined with various challenges. Among obstacles of this kind to be overcome, regulatory compliance, complexity of the systems integration, data security concerns, unpredictable situations and the need to keep maintenance can be mentioned. To avoid these, it is required to be holistically mindful of automation that is balanced in terms of innovation as well as adherence to regulatory values, system integration, and cybersecurity. Addressing such problems directly, a biomedical platform of the public sector can reap the benefits of automation to enhance the reliability of services, reduce downtime and safeguard the security and privacy of sensitive health and research information.

3. Framework for Automation-Driven Reliability Engineering in Public-Sector Biomedical Systems

Anthropomorphism The implementation of reliability engineering based on automation in the context of the public-sector biomedical systems entails the design and implementation of a solid framework that is capable of providing system resilience, compliance, and optimal performance. It is a framework of a number of interdependent components, each of which is concerned with various areas of system reliability, fault tolerance, automation, and continuous monitoring. The main aim of this structure is to sustain the full time and performance functioning of mission critical biomedical systems that have critical importance in national research, public health missions, and healthcare provision.

This section provides the description of the main components that comprise this automation-based reliability engineering scheme. These aspects are automation strategies, system monitoring and telemetry, compliance management, fault detection and self-healing mechanisms, recovery strategies. As a combination, they constitute a holistic solution to increase the robustness and carrying capacity of biomedical systems within a complex and regulation-based background they exist in.

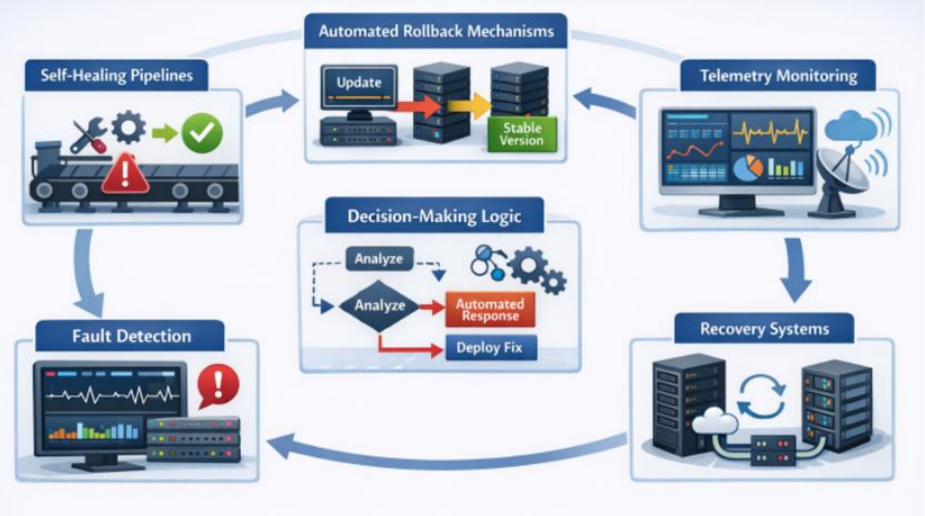

Figure 1: Automation-Driven Reliability Engineering Framework

1. Automation Strategies for System Resilience

The automation strategy is the central point of the suggested framework and is intended to minimize the use of human factors and increase the capacity of the system to self-heal and self-adapt. This encompasses processes of automation that dwell on continuous health checking of the system, fault detection, responding to incidents and recovery. The framework applies a number of important automation methods that are used to maintain constant availability of systems:

Self-Healing Pipelines

Self-healing pipelines are a form of automated workflow that aims at repairing or correcting failures in a system or performance-related issues. These pipelines are run on a real-time basis monitoring the system and fixing problems without having to be manually controlled. On detection of an anomaly or failure, the pipeline automatically initiates a set of corrective measures, including diversion of traffic, undoing a failed deployment or service restart.

In the application of biomedical systems in the context of the public sector, such pipelines are particularly important due to the maintenance of the continuous functioning of the necessary healthcare services. In case, say, a patient monitoring system goes to a bad state because of software glitch, a self-healing pipeline will automatically use an alternative configuration or go back to a previous stable state. The mechanism is used to ensure the reliability of a system and also reducing the downtime and the possibility of human error.

Automated Rollback Strategies

The automated rollback plans can play a crucial role in the case of mitigating the effect of system malfunctions or implementation of buggy updates. Software updates, patches, and configuration changes at times carry unwanted surprises to biomedical systems and this undermines the functionality of the system. Rollback strategies are plans to restore a previous steady state in case of such failures, which are automated.

The automation system contains an automated rollback system that operates with the self-healing pipelines. When an update is found to be unstable in a biomedical platform (i.e., a critical laboratory management system), the system will automatically detect the failure and roll back to the older version of the software. This rollback mechanism reduces and limits inconveniences and keeps the biomedical systems running at optimum without any major setbacks. The plan is especially useful in the situations when a fast implementation of changes must be provided, and the possibility of failure can never be completely ruled out.

Dynamic Resource Allocation and Scaling

Dynamic resource allocation and scaling is another feature of automation in the framework. Biomedical systems in the public sector are frequently plagued by changing workloads, including those associated with emergencies in the area of health, or seasonal outbreaks of diseases, or with a very large research project. It should be in a position to change with these demand changes without human interventions.

The automation structure is integrated with a resource management system that is dynamically capable of allocating or scaling resources (e.g. processing power, memory and storage) according to real-time demand. This is to make sure that systems work optimally with different loads and would avoid any bottlenecks in the system and make it more responsive at times of heavy traffic.

2. Telemetry-Based Monitoring for Proactive Issue Detection

One of the key elements of the automation-based framework is the application of telemetry-based monitoring to give real-time data on the health of the system, performance, and patterns of failures. Various components of a system such as hardware, software, networks and user interactions gather telemetry data.

Real-Time Monitoring and Analytics

The framework contains a telemetry which gathers system measures on a constantly going basis, such as CPU usage, memory usage, disk usage and network traffic. The measurements are real-time tracked and identified whenever there is a breach of the normal mode of operation. When some anomaly is identified such as the excessive use of resources or impending hardware breakage, there are some automated behaviors that take place in order to correct the problem before it can lead to a systemwide breakdown.

As an illustration, when the telemetry system realizes that the CPU usage on an important part of the biomedical platform is unusually high, the system can automatically increase or reassign workloads to ease the strain. This live tracking would ensure that problems do not get out of control and that the system would be in an optimum condition even when they are in high-pressure conditions.

Predictive Maintenance

A notable variant of monitoring based on telemetry is a predictive maintenance, an approach where data analysis and machine learning are used to forecast the possible breakdown of the system before it happens. The system will be able to determine historic telemetry data that could reveal trends and patterns that could lead to the possibility of a failure. Predictive maintenance models are used to predict the approximate time a component like a server or storage unit will fail allowing the administrator to plan the maintenance or replace the component before failure.

In biomedical systems, predictive maintenance is used to make sure that the key parts of the system, including patient monitoring devices or lab apparatus are working, which helps minimize the risk of failures that might interfere with patient care or research.

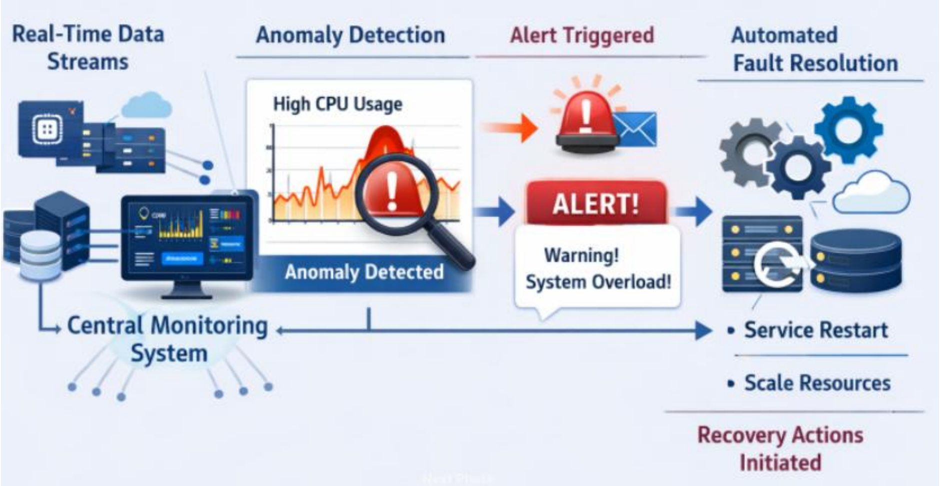

Figure 2: Telemetry-Driven Monitoring and Fault Detection

3. Compliance Management and Regulatory Adherence

Biomedical platforms in the public sector have tight regulatory standards in place to make sure that they uphold privacy, security and integrity of sensitive health and research information. Hence, the reliability system based on automation should conform to these standards and offer the ability to see what the automated systems are doing.

Auditability and Traceability

One of the major demands in biomedical systems is that biomedical systems should be able to give an audit trail of all the activities undertaken by the system, especially when automated systems are involved in undertaking a critical activity. It is necessary to comply with the rules and regulations like the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. or the General Data Protection Regulation (GDPR) in Europe.

The automation framework has elaborate logging and monitoring procedures to ensure that all automated processes are properly documented in the form of a rollback, self-recovery response, or update. These records are kept in a non-modifiable and secured format and enable administrative and auditing personnel to trace system modifications, examine recovery efforts, and anonymity ensure that everything is done in accordance with the regulatory specifications.

Compliance-Aligned Automation

The framework also has compliance-related automation, in addition to auditability, where automated actions are performed based on the rules of conduct. This involves the validation of updates, rollbacks and system configurations to make sure that they comply with the data privacy, security and integrity standards. Automation which is compliant offers real-time warning in case a system move is determined to be breaching regulation rules so that corrective threat can be taken immediately.

An example is when a software update is implemented to a biomedical platform, the automated system examines whether the update is compliant, e.g., by ensuring that no patient data is leaked or that security vulnerabilities are not added. In case the update does not comply with these conditions, the automation system will stop the update or automatically switch back to the old settings.

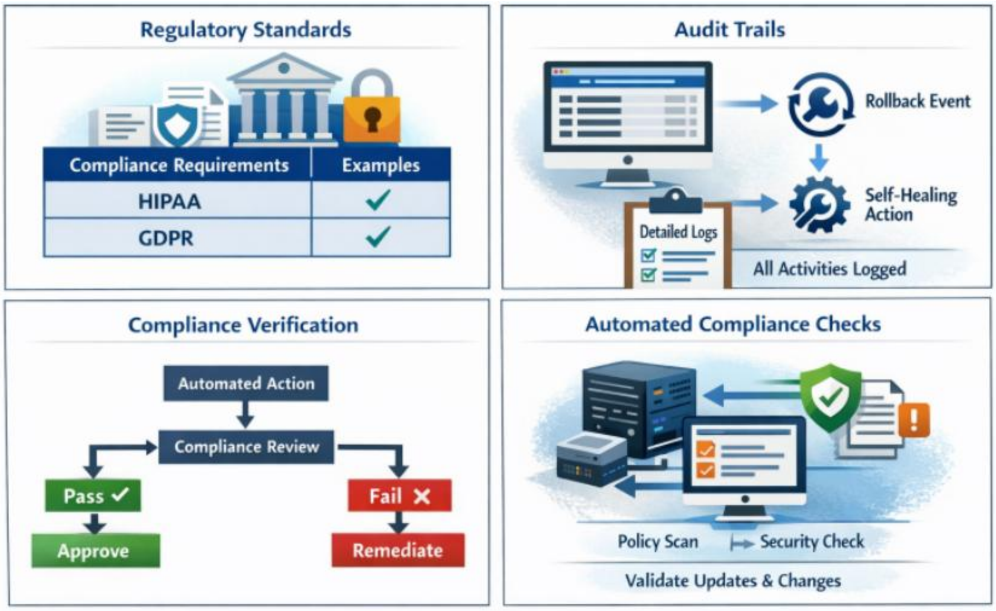

Figure 3: Compliance Framework for Automation-Driven Reliability Engineering

4. Fault Detection and Self-Healing Mechanisms

Fault detection and self-healing are the main functions of system resilience in the proposed framework. These mechanisms use automated tools and algorithms to identify the existence of a fault when it occurs and takes the right process of recovery to be restored to its operational state.

Fault Detection Algorithms

The system has built-in, complex, fault detecting algorithms that monitor the behavior of the system in order to detect a fault or an anomaly. These algorithms analyze different system parameters such as hardware performance, software interactions and network traffic and detect problems that may occur in the system to cause failures. The fault detection mechanism will be able to identify the minor problems that may be addressed automatically and more serious failures that might need human intervention.

Self-Healing Systems

The reliability engineering framework operates through self-healing systems that are aimed at fixing faults on their own. After a fault is discovered, the system triggers self-healing processes, which may include automatically rerouting traffic, restarting a service which has failed, or returning a system component to a healthy state known to be good. To say the least, in the case of a biomedical platform failure in its database, the self-healing system can automatically kick-off the database or even revert to a backup instance to reduce the downtime.

5. Recovery Strategies and High Availability

Finally, the automation framework will also serve to underscore the importance of recovery strategies and high-availability structures in ensuring that the biomedical platforms are to operate and continue to do so even in such a situation.

High Availability Architectures

Ensuring high availability is done through redundancy deployment of systems, load balancers, and failure. These features make sure that in the event of failure of one of the parts of the system the system can be taken up by another part of the system without service being interrupted. The framework that is promoted by automation incorporates the above aspects into a unified system that can withstand and recover fast when failures occur.

Automated Recovery Plans

Along with high availability, automated recovery plans are implemented in order to recover the operation of the system after serious failures or disasters. These plans consist of predetermined actions that the system may be able to implement automatically in case of a significant event, like recovering data in backups or redistributing the workloads to other infrastructure.

The reliability engineering framework of the biomedical systems of the public sector based on automation involves the recent automation technology, telemetry-based monitoring, complaint management, detection of a fault, self-healing mechanisms, and the high-availability designs. Under these components, the framework will ensure that the biomedical platforms can operate exceedingly resilience, least downtime and government regulation standards. This is a comprehensive approach which can provide the infrastructure which is capable of providing the availability, security and performance of the mission-critical systems in the public-sector biomedical environment.

4. Performance Evaluation

These are the effectiveness, scalability and implications on the resilience of the system, which are critical to the automation-based reliability engineering model when applied to the context of public-sector biomedical systems that can only be explicated by the performance evaluation of the model. This section identifies the instruments and steps used to understand the success of the proposed structure. The discussion is done based on the key performance indicators (KPIs) in the domains of system reliability, fault tolerance, incident response time, recovery efficiency, compliance, and resource utilization. The assessment of these points will permit concluding on the effective work of the whole framework regarding its role in maintaining the continuity of the operations and the access to the services of biomedical platforms.

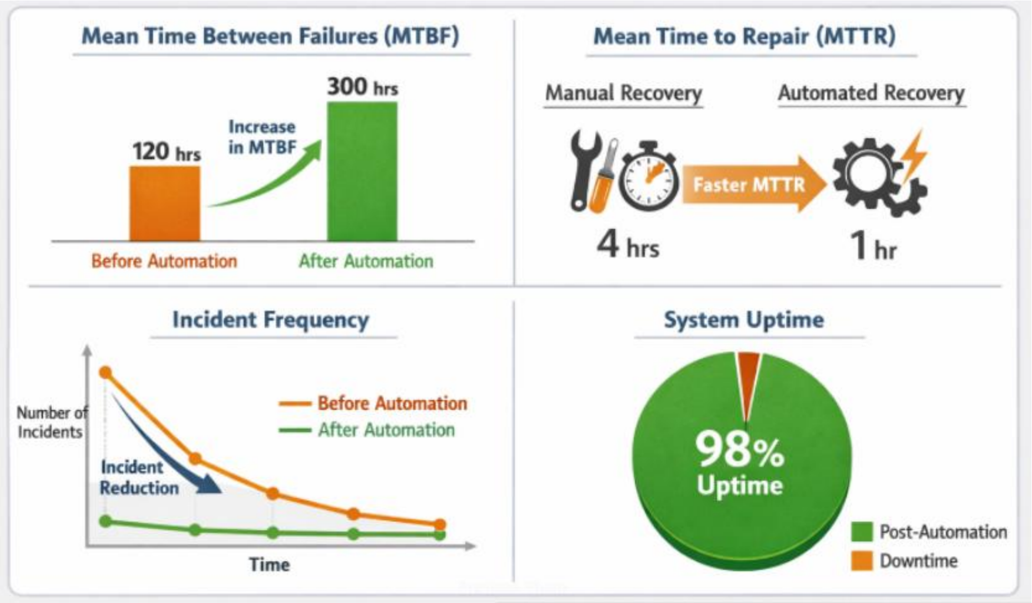

Figure 4: System Reliability and Key Performance Indicators (KPIs)

1. Reliability and System Availability

The effectiveness of an automation-based framework, which has a direct impact on the availability of systems, is one of the most crucial measures to assess the reliability of the biomedical systems. The Mean Time Between Failures (MTBF), and the Mean Time to Repair (MTTR) are usually used to identify reliability. Such measures define the frequency of failures and the rate at which they are repaired.

Of particular interest with regard to determining the efficiency of self-healing system and automated rollback systems is the definition of the MTBF metric. A decrease in the MTBF will be witnessed particularly when handling mission-critical systems such as patient monitoring system or laboratory data management systems and this will imply the framework is working successfully in preventing recurrent failure. Improved data, such as self-healing pipelines, can be performed using auto recovery, and this significantly contributes to improving the MTBF, since it will detect and rectify breakdowns before it can result in a service interruption.

The speed of the system in the case of a failure is on the other hand measured using the MTTR metric. Mechanisms of automated recovery, including automated rollbacks and self-healing mechanisms, are very important in making sure that the automated recovery mechanisms minimise the amount of MTTR. It is particularly important in a biomedical environment to reduce the time of recovery to a minimum to avoid reducing such services as the attention of a patient or real-time analysis of a research data. Reduced MTTR, which is the result of automation-based operations, exhibits greater operational effectiveness and robustness.

2. Incident Response Time and Fault Detection

The other important key performance indicators is the incident response time, which is the amount of time it takes to identify a failure and to address the problem or mitigate the issue. This measure is essential in determining the ability of the system to identify, respond and recover problems by itself. Reducing response times is based on automating fault detection and real time telemetry monitoring.

The fault detection time is normally gauged by the lag in time during which the telemetry based monitoring instruments of the system detect anomaly or fault on the system performance. A good automation must provide a fault detection in real-time or as close to real-time as possible. A shortening of fault detection time can be interpreted as an indication that the system is capable of detecting the problems ahead of time, thus critical in averting the cascading failures.

In addition, automated incident response time is the duration within which amorphous automation structure needs to launch remedial measures after a malfunction has been identified. The more rapid the system is capable of reacting on its own, be it through traffic rerouting, reinstating of services, or returning to a last known healthy state, the more resilient the platform will be. Based on these metrics, a quantitative evaluation regarding the effectiveness of the automation framework in facilitating real-time resolution of issues is possible, which results in the enhanced uptime and performance of the system.

3. Compliance Adherence and Auditability

In the case of the public-sector biomedical systems, not only is adherence to the regulatory standards required by law, but it is also a measure of operational integrity. The compliance of the automation framework, as an automation of fault recovery, system updates, and incident responses is a noteworthy aspect of its performance.

Compliance auditability is a very important measure used to measure the efficiency of the framework to deliver to the regulations. To make sure that automated actions, such as updates, rollbacks, and self-healing, comply with such requirements as HIPAA (Health Insurance Portability and Accountability Act) or GDPR (General Data Protection

Regulation), systems should have extensive histories of all such operations. One of the most important things that a system administrator should have is a powerful auditing mechanism to ensure that he can trace out every action and that is important in maintaining privacy of the data, security and integrity of the system. The performance of the framework can be measured using the degree to which automated processes are being recorded in a framework and whether the logs can be readily accessed by auditing them or not.

Also, the adherence to compliance can be determined by the frequency of compliance violations in the process of automation. A reduced number of violations means that the system is adequately balancing automation and the necessity of regulatory compliance. In case automated processes raise non-compliant activity or neglect the necessary validations, the performance of the framework in ensuring compliance would be deemed as suboptimal.

4. Resource Utilization and Scalability

Other important performance indicators are efficiency in resource usage and capacity to expand according to the demand. The automated systems and, in particular, those implemented in the public-sector biomedical settings should be capable of adjusting to the varying workloads without necessarily consuming resources. This is especially significant in situations of high demand, like emergency situations in the field of public health or on a large-scale biomedical research project, where a rapid increase in the number of computational resources can become necessary.

The efficiency in the use of resources is determined by the effectiveness of the automation framework to optimize resources within the system which could be processing power, memory and storage among other things given different conditions. This involves testing the hypothesis on the effectiveness of automated resources allocation systems, like dynamic scaling and load balancing, to avoid bottlenecks and to achieve optimal performance of the system at times of peak demand. A properly optimized automation system must be able to scale appropriately up to increases in workload with a minimum of resources overhead when the demand is low.

Scalability- Scalability can be tested by ensuring that the framework has the capability to endure abrupt surges in demand without experiencing any major deterioration in system performance or reliability. An example of such is when there is a surge in user activity or data during a public health crisis on biomedical platforms. An automated system of automation must be capable of delivering more resources (i.e. servers or storage) automatically so that the performance levels can be kept at optimal levels.

5. Cost Efficiency and Operational Impact

Although the main purpose of automation in biomedical systems is the enhancement of reliability and service availability, the cost-effectiveness of the automation structure also contributes to the performance assessment to the minimum. The cost of automation usually requires an initial investment in technology and infrastructure and must result in long-term cost savings through the elimination of human intervention, down time reduction, and system resource optimization.

The cost efficiency could be evaluated by calculating the cost of running the processes prior to and after the introduction of automation based reliability engineering. The cost of operation should also be reduced because of a decrease in the number of incidents, the rate at which people are able to recover, and the effectiveness of the system. Besides, the automation of monitoring and predictive maintenance must also minimize the necessity of manual control, and new savings will be achieved in the long run.

6. End-User Experience and Service Continuity

Finally, an automation-based reliability engineering framework can be quantified based on its effects on the end-user experience. In the case of biomedical platforms, the end-users are the healthcare professionals, researchers and the patients that depend on the systems to provide real-time data and decision-making.

This is a very important part of this framework considering that the framework has the capability to ensure continuity of its services without much disturbance. The surveys, system uptime information, and comments left by the user will provide the required data about the ability of the automation framework to meet the needs of its customers. The level of trust and satisfaction among the users of the biomedical platform will improve because the system will be always available and minimal downtime and latency will be superior to the former system.

Important to the assessment of the effectiveness of the automation-based reliability engineering framework, grounded on improving the resilience of the system, its efficiency, and its conformity in the framework of the public-sector biomedical systems. Key metrics (availability of the system, the time of the incident response, compliance, resource usage, cost efficiency, and end-user experience) can be used to measure the overall success of the framework. The fact that the framework can reduce the failures, speed up the recovery, enable the regulatory compliance, simplify the resources, and provide the continuity of the services is a testimony to the fact that the framework can transform the operations of the mission-critical biomedical platforms considerably.

5. Conclusion and Future Work

The paper examined how to integrate automation-based practices of reliability engineering to increase the resilience of the public-sector biomedical systems. The model that is discussed in the present work includes self-healing pipelines, automated rollback plans, telemetry-based monitoring, and fault identification systems, which can contribute to the improvement of the work of the systems, lessening the downtime, and ensuring continuous access to the services. The analysis of the performance indicated that automation will help greatly to lower the rate of incidents, recovery period, and human touch, which will uplift the reliability of the system and its performance efficiency. Besides, the adherence to compliance is also ensured by the audit and the traceability of the automated processes in detail, which also makes the regulation requirements fulfilled.

The strategies related to automation can be a promising method to maximize the continuity of operations in the context of the public-sector biomedical systems, where data privacy, system security, and system availability are the priorities. Through automation, biomedical environments can now be in a better position to manage the increased complexity of data processing, the continually changing healthcare requirements, and the unpredictable demands of the systems, without sacrificing their performance or compliance.

Although the framework suggested in the current study has significant potential, there are multiple aspects, which can be examined and developed. To begin with, further work may be done to improve the self-healing processes to be able to accept even more complicated failure cases, especially those that involve more complex system dependencies, or inadvertent interplay between subsystems. This would imply enhancement of intelligence of automated recovery measures to ensure smooth operations in diverse and heterogenous settings.

Another major research issue in future is scalability. Given that biomedical systems are increasingly relying on cloud computing and distributed architectures, there is a need to design systems of automation that can dynamically and efficiently achieve scale in direct relation to the changing workloads. Further studies are necessary to develop AI and machine learning algorithms that can predict and react to the fluctuating future resource needs so that the systems can be scaled without affecting their performance.

The addition of more security systems in the automation system is the next path that can be pursued in the future. The more the automation is utilized, the more the vulnerability to cybersecurity. One of the primary aspects that will be taken into account in ensuring that the automation framework is capable of sustaining any cyber threats such as ransomware or data breaches and that the system is resilient and adheres to its rules and regulations will be regarded as a step towards the framework improvement.

Ultimately, automated reliability systems will be monitored and evaluated over time in the actual biomedical environment and this will be beneficial in understanding how they can work in actual life, which can be optimized to become more reliable and cost-effective.

References

1. Z. Xu, Z. Zhang, and L. Li, "Machine learning for reliability engineering and safety applications: review of current status and future opportunities," *Reliab. Eng. Syst. Saf.*, vol. 208, p. 107362, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832020304421.
2. M. C. E. Simsekler, R. R. A. Mustafa, and M. E. D. Hassan, "Integration of multiple methods in identifying patient safety risks," *Saf. Sci.*, vol. 119, pp. 42-52, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753518304292.
3. S. A. Terezakis, M. H. A. Gupta, and S. J. C. Ram, "Safety strategies in an academic radiation oncology department and recommendations for action," *Jt. Comm. J. Qual. Patient Saf.*, vol. 37, no. 5, pp. 211-220, 2011. [Online]. Available: https://www.jointcommission.org/resources/news-and-multimedia/blogs/.
4. G. K. Kaya, D. N. Gupta, and A. M. R. Murthy, "Semi-quantitative application to the functional resonance analysis method for supporting safety management in a complex health-care process," *Reliab. Eng. Syst. Saf.*, vol. 189, pp. 229-239, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0951832020301653.
5. P. Nancy et al., “Detection of brain tumour using machine learning based framework by classifying MRI images,” International Journal of Nanotechnology, vol. 20, no. 5/6/7/8/9/10, pp. 880–896, 2022, doi: https://doi.org/10.1504/ijnt.2023.134040.
6. P. Khaleghi, R. K. Mohammad, and H. H. Sharif, "Identification and analysis of human errors in emergency department nurses using SHERPA method," *Int. Emerg. Nurs.*, vol. 59, p. 100924, 2022. [Online]. Available: https://www.journals.elsevier.com/international-emergency-nursing.
7. Z. Kovacevic, L. D. Williams, and R. S. Smith, "Prediction of medical device performance using machine learning techniques: infant incubator case study," *Health Technol.*, vol. 10, no. 5, pp. 529-537, 2020. [Online]. Available: https://link.springer.com/article/10.1007/s12553-019-00259-1.
8. A. Kapur, R. K. Gupta, and A. V. Jain, "Six sigma tools for a patient safety-oriented, quality-checklist driven radiation medicine department," *Pract. Radiat. Oncol.*, vol. 2, no. 3, pp. 187-192, 2012. [Online]. Available: https://www.journals.elsevier.com/practice-in-radiation-oncology.
9. M. G. Pecht, R. K. Gupta, and N. D. Patel, "PHM in Healthcare, Prognostics and Health Management of Electronics: fundamentals, machine learning, and the internet of things," *IEEE*, vol. 7, pp. 75-84, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8775472.