Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P420-cd

An Analysis of Resilience and Risk Assessment in Digital Healthcare Systems

Georgia A. Tzitzili

Department of Financial and Management Engineering, School of Engineering, University of the Aegean, Chios, Greece.E-mail: fmer22005@fme.aegean.gr

Stergiani Spyrou

Lab of Medical Physics & Digital Innovation, Aristotle University of Thessaloniki, Thessaloniki, Greece
3rd Regional health Authority, Macedonia, Greece.E-mail:sspirou@auth.gr

Agapios N. Platis

Department of Financial and Management Engineering, School of Engineering, University of the Aegean, Chios, Greece.E-mail: platis@aegean.gr

Resilience assessment of a digital healthcare system is important to maintain continuity of critical operations, downtime of which may affect even patient's life. A resilient Hospital Information System (HIS) or subsystem should maintain its interoperability with other subsystems despite challenges such as technical failures, data breaches or natural disasters. This resilience is critical in ensuring that the HIS can continue providing accurate and timely information to healthcare providers and patients, even during times of crisis. The complexity of multiple Information Technology (IT) systems in hospitals and the interaction of subsystems with HIS, electronic patient records and national e-order systems for e-prescriptions or clinical orders highlight the importance of ensuring interoperability. The use of Markov models in reliability block diagrams is an approach that takes into account the weaknesses of IT equipment and infrastructure over time. With this approach, the reliability of the multidimensional functioning of the different subsystems in the health field can be assessed. The failure probability of a subsystem can be estimated, and the overall resilience of the systems can be highlighted. Limited literature in this area is notable. However, many additional steps need to be taken to improve resilience, since low resilience investments, problematic or incorrect employees' training on safety issues, lack of cybersecurity resilience strategies and risk management frameworks of healthcare organizations were identified as significant gaps in the digital healthcare system's resilience.

Keywords: critical infrastructure, dependability modeling, healthcare IT systems, healthcare services, information technology, resilience, reliability, risk.

1. Introduction

Digital healthcare systems consist of integral building blocks for the proper functioning of health service delivery systems. This causes their contribution to the establishment of resilient health systems, systems that can provide uninterrupted healthcare services (Biddle et al. 2020). The word "resilience" has multiple meanings due to the researchers' approaches in various fields over the years (Park et al. 2013) or distinct application areas, such as organizational, social, economic, and engineering (Hosseini et al. 2016). According to Haimes (2009), resilience is a system's ability to withstand a significant interruption within acceptable degradation parameters and to recover over an acceptable period of time, as well as within reasonable costs and risks. Resilience refers to the ability of an entity or a system to return to its normal state after the occurrence of an event that disrupts its state (Hosseini et al. 2016) or to adapt to varying conditions without, however, suffering any catastrophic loss of form or function and not exceeding an irrevocable tipping point (Park et al. 2013) and, generally, as Aven (2017) pointed out, to maintain or restore its functionality and performance after a change in the state of the system. Resilience in this paper highlights the meaning in two different aspects, (i) critical infrastructure resilience, which refers to the ability of a risk-exposed critical infrastructure system to resist, absorb, adapt to, and recover from the impacts of a risk in a timely and effective manner to maintain and restore essential services (Petersen et al. 2020) and (ii) cyber resilience, the ability of a system to anticipate, detect and withstand cyber threats and recover from an attack when it's achieved (Patriarca et al. 2022). Healthcare information technology infrastructures that, among other things, interact with other health institutions using web applications, according to the definition of Liu et al. (2021), are critical infrastructures whose operation can be affected by unforeseen and unavoidable events, such as malicious attacks.

Emerging technological developments as well as the complexity and criticality of healthcare services have a direct impact on the resilience of healthcare services (Biddle et al. 2020; Wiig and O'Hara 2021). The continuous demands of the delivery of health services, like the crisis of the recent pandemic covid-19, highlight the importance of the uninterrupted provision of health services along with the ability of the healthcare system to respond to a health crisis (Haldane et al. 2021). So far, information technologies in healthcare are crucial assets for storing, retrieving and distributing patient-related data and applications, such as management software, access to e-prescription or electronic health records, and supporting

healthcare professionals' decision-making. The current demands and developments that raised rapidly with the pandemic covid-19 and the actions towards digital transformation introduced to healthcare organizations technologies which offer access to new diagnostic and therapeutic decision-making methods, telemedicine, teleconsultation, robotics, Internet of Medical Things (IoMT) and other IT-related technologies (El-Sherif et al. 2022; Shen et al. 2021). mHealth applications, medical and public health practices delivered through mobile devices, were recorded mainly in pilot studies in 2017 (Wallis et al. 2017). However, the pandemic covid-19 prompted the rapid adoption of these telemedicine and teleconsultation practices to safely manage the increased number of infected patients and to continue routine follow-up treatment activities for patients, especially those with chronic diseases (Giansanti 2021; Farad Rafique et al. 2022; Asadzadeh and Kalankesh 2021). Moreover, the advanced personalized healthcare offered to patients has been further enhanced with the wide use of new technologies. Some of these technologies, like smart sensors, advanced Internet of Things (IoT), Artificial Intelligence (AI), and blockchain technologies, enhance healthcare management systems but,due to several security, privacy, interoperability and availability issues, offer new gates to threats (Junaid et al. 2022). Under these unprecedented requirements of healthcare delivery services, the digital transformation of the healthcare sector is an expected and essential development, but it has to be combined with the adoption of technologies and applications that should primarily be governed by cyber security and cyber resilience (Garcia-Perez et al. 2023). Computer disruptions can lead even to the unavailability of patient care delivery because, as Kramer et al. (2012) pointed out, there have been several infections that spread to medical devices, although it has not been confirmed that the malicious interventions targeted the medical devices' function. The risk of an attack depends on the severity of the diseases associated with the particular devices. The above highlight the importance of healthcare IT systems resilience.

As healthcare resilience is significantly related to the IT resilience of a healthcare organization, it is particularly important to focus on the resilience of both computers and networks and more specialized on cyber resilience, so that the effects of an attack are not reflected in the continuity of the provision of health services or even in the patient's life. After all, the main objective of resilience is to ensure continuity of services with the minimum impact. Assessing a healthcare information system's resilience, by continuously patching vulnerabilities, identifying and mitigating threats, training employees, and finding solutions for more immediate restoration and recovery, demonstrates a reliable process to ensure the system's functionality. The various security measures adapted for the security of digital healthcare systems in cyberspace are only one dimension of this approach. This paper aims to find all the variables related to resilience that may affect the rehabilitation, performance, and general operation of a digital healthcare system after a change in its status, to accomplish a feasible model for assessing the resilience of critical healthcare informatics infrastructures. The resilience analysis is expected to make a significant contribution to managing healthcare information technology systems' risks and improving overall healthcare resilience by providing digital services characterized by the best quality of service (QoS) with high reliability, availability, and performance. The systematic literature review applied can provide a comprehensive analysis of this topic in all its dimensions and provide the information for the quantified modeling of resilient digital healthcare systems.

2. Literature review

Healthcare IT system's resilience is based on the vulnerabilities and actions taken for redundancy and the secure technologies that exist in a healthcare organization. The systematic literature review carried out for this purpose highlighted the risks and various vulnerable or secure infrastructures as well as measures or approaches to improve them. Singh et al. (2013) highlighted 9 high-risk areas that include decision making support, computerized provider order entry (CPOE) and e-prescribing, test result reporting, transfer of sensitive data between systems within the organization and communication with other providers, functionality of electronic health record and its customization and configuration, patient identification and security issues of human behavior.

The nature of the incidents reported by European Union Agency for Cybersecurity (ENISA) to EU healthcare infrastructures between 2020-2022 were system failures 61%, human errors 14%, malicious actions 24% and natural phenomena 1%[a]. Table 1 gives more information about the causes and assets affected. The main vulnerabilities pointed out by the incidents and literature review, were software and hardware failures or bugs, human errors and access to IT infrastructure Data Management.

Table 1. IT Healthcare incidents per nature[a]

Nature of the incident	Technical causes	Technical assets affected
System failure	Hardware failure Software bug Faulty software changes/update Power cut Faulty hardware changes/update Overload Supply chain Other	Workstations Applications Server/domain controllers Switches and routers Other
Human errors	Faulty software changes/update Cable cut Policy/Procedure Flaw Faulty hardware changes/update	Workstations Applications Server/domain controllers Underground cables

[a] © European Union Agency for Cybersecurity (ENISA), 2021available at Incident reporting -CIRAS (europa.eu)

	Power cut	Other
	Phishing	
	Hardware failure	
	Other	
Malicious actions	Ransomware	Workstations
	Phishing	Server/domain controllers
	Malware and viruses	Mailbox
	DDoS attack	Website
	Vulnerability exploit	Other
	Identity theft	
	Faulty software changes update	
	Other	
Natural phenomena	Overload	Workstations
	Cable cut	Other
	Other	

Software failures include those arising from using computers with old versions and outdated operating systems (OS) or outdated software/applications. Outdated versions lead to software bugs commonly related to compatibility and interoperability issues. Hospitals' reliance on legacy software and medical devices of high cost and the fact that many people use the same computers explain why in practice is impossible to apply security and redundancy methods that other sectors may apply easier (Boddy et al. 2017). Increasing the cybersecurity budget and reallocating healthcare providers' resources can help improve healthcare IT resilience against threats (He et al. 2021). Investing in new IT infrastructure can improve resiliency so that there are redundancies and the continuity of operation of critical systems is maintained. However, creating a fully functional and resilient integrated system is a difficult and time-consuming process due to the need to ensure uninterrupted interoperability between multiple systems, while integration of critical subsystems might help adopting more resilient technologies, even small ones (Shrivastava et al. 2021). The most developing ones are digital twins, patients' virtual copies that use neural networks to train in resistance and deserve the terms of resilience, both to healthcare resilience and IT resilience (Zhang and Tai 2022; Zhang et al. 2020).

Moreover, the forefronts of the hardware failures are old hardware, workstations, and routers. Interconnection with Internet of Things (IoT) devices, such as wireless sensors that are widely used in the healthcare sector, as well as mobile phones or tablets used for mobile applications, can significantly highlight the risk of attacks, especially if no measures have been taken to configure them or if they have not been separated from the rest of the network or their access to the Internet has not been blocked (when their operation is possible without it). IoT technologies constitute a significant vulnerability for the healthcare system, like wireless sensors that arise during the pandemic covid-19. An attacker's access can easier be achieved through wireless sensor networks (WSNs) within a telecare medical information system (TMIS) or through comprehensive personalized healthcare services (CPHS) provided via WiFi and breach confidential and private health-related information. WSNs are applied to many areas of health services such as electrocardiograms (ECGs), voice over IP and audio/video conferencing, location awareness, and artificial intelligence (Bruce et al. 2013). For more resilient digital systems, have been proposed security models or protocols for WSNs that improve reliability, such as SensoTrust (Castillejo et al. 2015),BAKMP-IoMT, a blockchain-enabled authentication key reconciliation protocol for IoMT environment (Garg et al. 2020), a cloud-based authentication protocol (Mohit et al. 2017), an improved version that enables mutual authentication and privacy-maintaining prior to accessing TMIS (Li, Shih, and Wang 2018), a protocol based on received signal strength (RSS) measurement and public-key cryptography using Diffie-Hellman algorithm (Bruce et al. 2013) as well as proposals for establishing Healthcare 5.0 services (Taimoor and Rehman 2022).

Human errors are common challenges for healthcare IT security incidents because employees' training and support are not sufficient to limit them and the attacks they lead to (He et al. 2021). Healthcare employees' engagement is an opportunity for healthcare system to adopt a culture of HIT resilience and embrace changes made to this direction, such as Electronic Health Record (EHR) software updates (Barrett 2022). Other ways to limit human error related attacks are security awareness, policy enforcement, and the development of specific guidelines (He et al. 2021). The major causes of human errors, which unauthorized individuals can exploit, are due to lack of cybersecurity awareness and reduced adoption of specific guidelines given by cybersecurity experts. Healthcare employees skip important security steps, connect unauthorized hardware, fall victims to phishing, configure weak passwords in applications, mailbox or even their OS profiles, storing OS and application credentials in plain text, deny use of safer versions of software or delay software updates. As for natural phenomena, no searches where identified.

Last, but not least, a main group of vulnerabilities is the access to IT infrastructure Data Management. Healthcare sector contains multiple subsystems that all should be interoperable in updating the Electronic Medical Record (EMR) that is in the heart of the integrated information system of every healthcare organization. Several vulnerabilities of this category are lack of virtual private networks, irregular monitoring and coordination of database performance, problematic data security of Hospital Information System (HIS) applications, failure to implement software upgrades and security patches, lack of plan in backup, and lack of plan for database recovery. Singh et al. (2013) developed self-assessment guides for assessing high-risk elements of clinical systems, due to the criticality of interoperability between them and EHR. IT infrastructure Data Management issues, even in one subsystem may affect the overall operation of the hospital. For example, an attack to an active directory server might allow access to the core of the healthcare IT infrastructure, all user accounts passwords and security groups and even all EHR sensitive data, problem that may be reduced using machine learning algorithms trained in tracking network (Walsh and Borycki 2022).

There have been several CVEs (Common Vulnerabilities and Exposures) reported in CVE details website[b] for Hospital Information Systems (HIS) in the past. Here are a few examples:

- Vulnerability CVE-2020-25213 was found in a popular HIS's authentication process that allows obtainment of sensitive patient data.
- CVE-2019-19358 pertained to a weakness in the HIS's file-uploading functionality that an attacker may take advantage of to execute arbitrary code on the server.
- CVE-2016-2107 was related to HIS because many systems use the OpenSSL library for secure communication, since it was found in the library's encryption algorithm, and an attack may provide access to sensitive data.
- Vulnerability CVE-2022-36669 was found in SQL database, and provided a bypass, a flaw in database authentication, that can provide unauthorized access to sensitive data.

Strong measures are required to ensure continuity against threats that could affect the Healthcare IT infrastructure. Integrated management to build digital healthcare resilience can emerge by identifying and assessing risks and resilience that will lead to plans and policies to facilitate preparedness and response. Next part describes the methodology followed for this purpose.

3. Methodology

In this part, the proposed resilience assessment methodology of digital healthcare systems is described through a case study. The steps followed are described below:

- Identify Vulnerable/Secure IT infrastructure components: First step was to identify IT infrastructure components related to the hospital's information system, resilient ones and those with vulnerabilities. Different elements, subsystems and related vulnerable materials were identified by the literature review, healthcare IT vulnerabilities and the empirical mapping of interoperable healthcare subsystems.
- Assess system compatibility: Next step was to capture compatibility of HIS and the subsystems that interact with it. This included recording the correlations and related states that might be found in the event of an attack.
- Implementation and monitoring of an integration plan: Based on the assessment of vulnerable and secure infrastructures and the overall compatibility of the system, a resilience assessment model is developed for a case study and a comprehensive plan is given for the implementation of measures aimed at creating resilient critical healthcare IT infrastructures.

4. Healthcare main IT subsystems' role

Combining hospital IT infrastructure with Hospital Information System (HIS) and the subsystems that serve the overall delivery of healthcare is a complex and challenging task due to the multiple interactions between them. Figure 1 represents the interactions between the basic subsystems. The main system is HIS, which is an integrated information system that stores data for the best possible patients' support and treatment, as well as the overall management of administrative, financial and clinical data related to the patient's stay in the hospital (Mehdipour and Zerehkafi 2013). HIS includes the EMR system, which captures patient's healthcare information in the healthcare organization (Edmund, Ramaiah, and Gulla 2009). EMR data account for part of EHR, the digital overall patient's health information. Three subsystems related to the delivery of healthcare, the critical part of healthcare, are (Mehdipour and Zerehkafi 2013):

- Laboratory Information System (LIS), a healthcare software-based solution that manages laboratory data, patient information and test results.
- Picture Archiving and Communication System (PACS), a medical imaging technology that supports storage and provides access to images from imaging / radiological machines such as X-ray plain film (PF), computed tomography (CT) and magnetic resonance imaging (MRI). Digital Imaging and Communications in Medicine (DICOM) is the standard used by PACS to store and transmit images along with other non-image data, like scanned documents.
- Radiology Information System (RIS), a main system for electronic management of the data generated in radiology departments and diagnostic imaging centers. Its role is particularly important as it contributes to patient scheduling, examination performance tracking, reporting, results distribution, resource management, and procedure billing. The criticality of this subsystem lies in the fact that it mediates between HIS and PACS and its downtime prevents all radiological practices.

E-orders, the electronic orders that include clinical orders (referral for medical exams), e-prescription etc, are usually contained in HIS and in National Healthcare systems. That means that interoperability of a healthcare organization's system with this system is important in order to perform the tests.

[b] https://www.cvedetails.com/

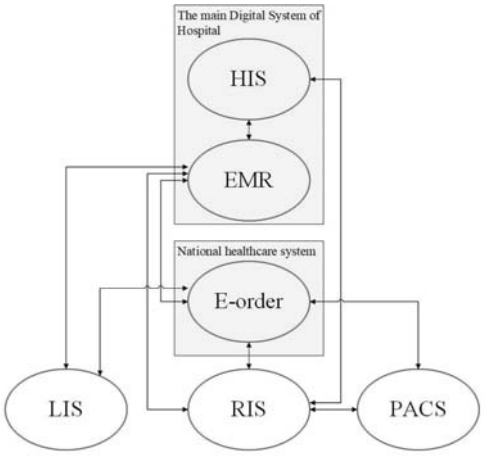

Fig. 1. Interactions between the main healthcare subsystems.

Data management of the subsystems of a HIS and the interoperability of those systems in a secure context can ensure the system's resilience. An application of a healthcare information subsystem can provide an entry point to larger healthcare networks, even the HIS and EMR data set. Table 2 gives the different states in which a system/or a subsystem may be according to the compatibility of other subsystems, even if the related to the subsystem software or database are not attacked.

Table 2. HIS's subsystem states and its interdependencies

System & Sub-systems	States
HIS	Fully operational: when all the subsystems are operational plus the interoperability between the subsystems. Partially operational: when any of PACS, RIS, EMR or LIS subsystem is either fully operational with problems in interoperability or partially operational or there is no interoperability with e-orders or any of them is offline. Offline: When the system is attacked or no interoperability is possible. Can function standalone but not for new patient entries.
LIS	Fully operational: when all the subsystems related are operational plus the interoperability with e-order system. Partially operational: when LIS is functioning but interoperability with HIS in terms of updating the EMR and ultimately HIS. Function is possible without EMR updates. Offline: When the system is attacked or no interoperability with e-order system is possible. Can operate standalone but with printed e-orders or printed results and only if the laboratory machines' functionality is not computer-based.
RIS	Fully operational: when PACS, EMR, interoperation with HIS are fully operational plus the interoperability with e-order system. Partially operational: when any of PACS, EMR or HIS is partially operational. Can operate standalone but without updating the related to the partially working system. Offline: When the system is attacked or no interoperability with e-order system is possible. Can work standalone but only with printed e-orders, only if the laboratory machines' functionality is not computer-based and without updating EMR and HIS.
PACS	Fully operational: when RIS is fully operational. Partially operational: When image production is possible but without combining image with RIS data. Offline: When the system is attacked or there is no interoperability with RIS.
Interoperability of any subsystem or HIS with EMR	Fully operational: When PACS, RIS and LIS subsystems are operational plus the interoperability between the subsystems. Partially operational: When either RIS or LIS is partially operational or offline but not at the same time. The function is partial for the new data related to the subsystem that is working fully. If examining only a subsystem or procedure, no partial operation may occur. Offline: When the system itself is attacked or RIS and LIS are offline at the same time. Can function standalone (if not attacked) but no update can occur.
Interoperability of any subsystem with e-orders	Fully operational: When RIS and LIS subsystems are operational. Partially operational: When either RIS or LIS is partially operational or offline but not at the same time. The function is partial for the new data that are related to the subsystem that is working fully. If examining only a subsystem or procedure, no partial operation may occur. Offline: When both RIS and LIS are offline at the same time. E-order system can function since it is a system out of the organization.

Since a system's availability is important in delivering the healthcare services, meaning that the subsystems of HIS are interoperable in order to achieve continuity and safety for clinical exams of a patient and deliver the needed treatment, it is critical situation when a system is offline. The three main states that describe a system's availability referred above are:

(i) Fully operational is a system when it is available and functions as expected.
(ii) Partially operational describes a system that is either limited available or has performance issues but at the same time is still able to provide some level of service.
(iii) Offline is referred for a completely unavailable or non-functional system.

The availability of the above systems has a significant impact on four dimensions. If LIS and RIS operation is not feasible, then no order can be placed. The operation of the hospital cannot proceed with rapid procedures, as is appropriate in cases of illness, and this can have a significant impact on the patient's health. If it is not possible to interact with EMR, then EMR is not updated immediately and this results in problematic patient management. If communication with the national electronic ordering system is not available, the test cannot be scheduled, and even when tests can be ordered from LIS and RIS, the expanded number of patients in these departments with hard copy orders can result in a chaotic

management situation and a delayed response, even if there is an emergency plan. This may happen as e-order interoperability downtime implies the simultaneous non-operation of the LIS and RIS subsystems of the first dimension. The most critical situation is that of a complete loss of access to the internal network and the internet, as it entails dealing simultaneously with all three previous effects. The above dimensions highlight the criticality of the uninterrupted operation of a hospital's information system/subsystems. A case study of inaccessibility to the internet/network is a doctor's order for radiological examinations of a patient with case (1) of flow diagram corresponding to the failure of RIS, case (2) corresponding to the interaction of RIS with the EMP, case (3) to the inability to communicate with the national ordering system and all first three cases simultaneously with the last dimension. Case (4) is related to PACS unavailability. The grey part of Figure 2 presents the possible redundancies. However, it is assumed that all radiology and diagnostic machines function regardless of access to network.

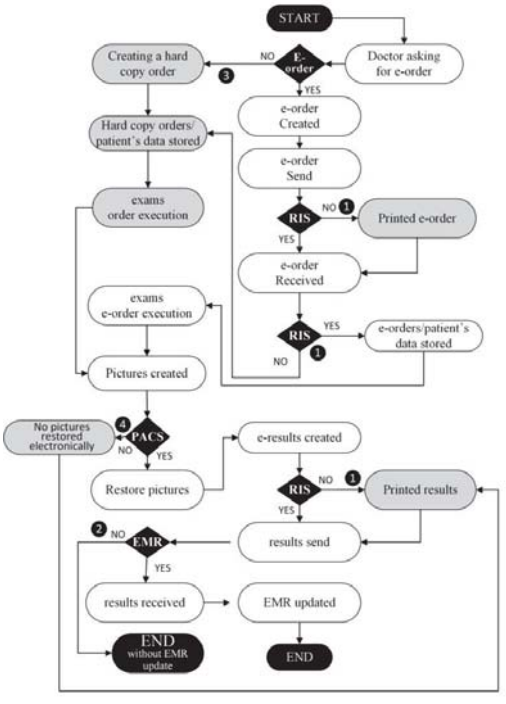

Fig. 2. Case study flow chart - Resilience in ordering radiological examinations.

The case study of Figure 2 highlights the particularities of healthcare information systems in relation to other systems/subsystems, like the main and critical interaction with the national electronic ordering system. It should be noted that is described only the performance of the examination, storage and distribution of the results in order to make the diagnosis. Critical additional points that are not mentioned are pharmacy information system (PIS) and treatment in general, medical information system (MIS), nursing information system (NIS) and clinical information system (CIS), patient management system (PMS) that includes patient's financial management and others.

5. Discussion

In order to improve IT healthcare resilience, hospitals can implement a comprehensive strategy that addresses various aspects of their operations. First step to this scope is conducting a risk assessment to identify potential vulnerabilities and weaknesses in the hospital's infrastructure, systems, and processes. Literature review nominated that problems come from infrastructure failures, malicious actions and human errors. After identifying them a continuing and disaster recovery plan must be made for maintaining critical operations, backup systems, and data recovery. This paper highlighted the importance of increasing investment in hospitals in order to replace old software and hardware and strengthen healthcare IT infrastructure Data Management actions. Adopting robust cybersecurity practices, including regular software updates, access controls to OS, software, systems, and network, scheduling employee training actions, and raising employee awareness can be powerful practices for responding to attacks. In case an attack is carried out, a good tool for optimal recovery from the incident is to draw up an incident response plan. Moreover, since a downtime or disruption may occur any time, healthcare employees should be trained on emergency preparedness in order to know and be able to apply on the response procedures and protocols. A similar plan should be communicated to patients, staff, and the community in the event of a disruption also, so that they understand that the procedures will be executed in a different way. Due to the rapid increase of IoT technologies during the covid-19 pandemic, it is really important for staff to get aware of the main security issues that arise using these technologies and a hospital's network. The interoperability, reliability, compatibility and availability of IT healthcare systems should be continuous and vital for healthcare professionals to face the daily crises of life and death. A solid understanding of the critical operation of any digital system in healthcare organizations and a tactic repeat of the above actions for resilience may lead to continuous effective healthcare units. Creating a comprehensive strategy can improve IT healthcare resilience.

Our future work will be based on the above description of the resilience of a HIS, which could be modeled using a Markov model. The main advantage of the Markov model is that it can model, in a relatively simple way, complex systems, such as the one described in the above analysis, accurately, flexibly and taking into account all relevant parameters. States in the model can include different levels of system's availability or performance according to resilience. Factors that play a decisive role in the transition probabilities between states are system failures, maintenance activities or changes in demand for system resources. The challenge of this approach is the existence of many different possible states, which can lead to a

difficult and time-consuming process. If the approach is to include all possible states, it may not be possible to accurately capture the behavior of all subsystems that develop complex correlations, particularly if there are many interacting variables and nonlinear relationships to be applied in the model. By designing a reliability block diagram (RBDs), using, for example, a Markov model, hospital administrators or IT staff can gain insights into the likely behavior of the system over time and identify potential areas of weakness or vulnerabilities that might be a part of an integration plan. This can contribute to a holistic approach of the systems involved and overcoming the difficulties of the complexity of healthcare systems.

Designing reliability block diagrams, assess of the reliability of complex systems is available. The advantage of using Markov models in RBDs is that they can account for the dynamic behavior of the system, taking into account the time-dependent nature of component failures and repairs. This model may be suitable for the complex interoperable environment of HIS.

Such a model could be used to identify the most critical elements of the system or to evaluate different strategies to improve its resilience, such as redundancy or backup systems or alternative pathways. Overall, Markov models can be a powerful tool for analyzing complex systems such as hospital information systems and can help stakeholders make informed decisions about system design, maintenance and operation. To achieve the Markov modeling, the first planned step is to record the fault tree of a subsystem's failure in order to capture the relationships of all subsystems and IT devices/equipment involved and also find out their failure possibilities that will be taken onto account in Markov modeling. This will be the basis to create the RBD that will be used for reliability and availability subsystem's analysis. The diagrammatic mapping will enable not only the IT resilience assessment but also the emergence of organization's capabilities to improve it.

6. Conclusion

Lack of an integrated strategy for IT healthcare cyber resilience was addressed through the systematic literature review. Although there have been proposed many reformative actions to create resilient digital healthcare systems, these were mainly limited to applications to improve new technologies such as WSNs. The improvement interventions were carried out with the help of technologies, such as blockchain and cloud applications. A particularly important dimension to achieve the continuity of healthcare delivery services is the interoperability of the different healthcare subsystems. The approximation of different systems' operation using Markov models in reliability block diagrams can be a drastic intervention to this end. Overall, the use of Markov models in reliability block diagrams can provide a more accurate and detailed assessment of system reliability, taking into account the dynamic behavior of the system over time. This approach can be particularly useful in assessing the reliability of complex systems with multiple interacting subsystems, where the failure behavior of individual components can have a significant impact on the overall system's reliability. Risk assessment and approaches to mitigate weaknesses and vulnerabilities, like empowering healthcare employees' awareness, creating emergency preparedness protocols, increasing the cybersecurity budget and reallocating healthcare providers' resources may improve the resilience of interoperable Health Information System (HIS) and subsystems maintaining their ability to continue functioning effectively and efficiently in the event of disruptions, failures or unexpected events. To this end, the Markov models in the reliability block diagrams proposed could be implemented in assessing a hospital's subsystem.

References

Asadzadeh, A., & Kalankesh, L. R. (2021). A scope of mobile health solutions in COVID-19 pandemics. *Informatics in Medicine Unlocked*, *23*. https://doi.org/10.1016/j.imu.2021.100558

Aven, T. (2017). How some types of risk assessments can support resilience analysis and management. *Reliability Engineering & System Safety*, *167*, 536–543. https://doi.org/10.1016/j.ress.2017.07.005

Barrett, A. K. (2022). 'Healthcare Workers' Communicative Constitution of Health Information Technology (HIT) Resilience'. *Information Technology & People*, *35* (2), 781–801. https://doi.org/10.1108/ITP-07-2019-0329

Biddle, L., Wahedi, K., & Bozorgmehr, K. (2020). Health system resilience: A literature review of empirical research. *Health Policy and Planning*, *35*(8), 1084–1109. https://doi.org/10.1093/heapol/czaa032

Boddy, A., Hurst, W., Mackay, M., & Rhalibi, A. E. (2017). A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, Liverpool, United Kingdom. https://doi.org/10.1145/3109761.3109793

Bruce, N., Gi-Hyun Hwang, & Hoon Jae Lee. (2013). A hybrid and fast authentication protocol for handoff support in e-healthcare systems among WSNs. *2013 International Conference on ICT Convergence (ICTC)*, Jeju Island, Korea (South). https://doi.org/10.1109/ICTC.2013.6675309

Castillejo, P., Martínez-Ortega, J.F., López, L., & Sánchez Alcón, J. A. (2015). 'SensoTrust: Trustworthy Domains in Wireless Sensor Networks'. *International Journal of Distributed Sensor Networks*, *11* (7).https://doi.org/10.1155/2015/484820.

Edmund, L. C. S., Ramaiah, C. K., & Gulla, S. P. (2009). Electronic Medical Records Management Systems: An Overview. *DESIDOC Journal of Library & Information Technology*, *29*, 3–12. https://doi.org/10.14429/djlit.29.273

El-Sherif, D. M., Abouzid, M., Elzarif, M. T., Ahmed, A. A., Albakri, A., & Alshehri, M. M. (2022). Telehealth and Artificial Intelligence Insights into Healthcare during the COVID-19 Pandemic. *Healthcare*, *10*, 385-400. https://doi.org/10.3390/healthcare10020385

Farad Rafique, J., Carlisle, G., & Glenford, M. (2022). A new privacy framework for the management of chronic diseases via mHealth in a post-Covid-19 world. *Journal of Public Health*, *30*, 37–47. https://doi.org/10.1007/s10389-021-01608-9

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, *121*. https://doi.org/10.1016/j.technovation.2022.102583

Garg, N., Wazid, M., Das, A. K., Singh, D. P,, Rodrigues, J. J. P. C. R, & Park, Y. (2020). BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment. *IEEE Access*, *8*, 95956–77. https://doi.org/10.1109/ACCESS.2020.2995917

Giansanti, D. (2021). The Role of the mHealth in the Fight against the Covid-19: Successes and Failures. *Healthcare*, *9*(1), 58-61. https://doi.org/10.3390/healthcare9010058

Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. *Risk Analysis*, *29*, 498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

Haldane, V., De Foo, C., Abdalla, S. M., Jung, A.-S., Tan, M., Wu, S., … Legido-Quigley, H. (2021). Health systems resilience in managing the COVID-19 pandemic: Lessons from 28 countries. *Nature Medicine*, *27*, 964–980. https://doi.org/10.1038/s41591-021-01381-y

He, Y., Aliyu A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Journal of Medical Internet Research*, *23* (4). https://doi.org/10.2196/21747.

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, *145*, 47–61. https://doi.org/10.1016/j.ress.2015.08.006

Junaid, S. B., Imam, A. A., Balogun, A. O., De Silva, L. C., Surakat, Y. A., Kumar, G., … Mahamad, S. (2022).: A Survey. *Healthcare*, *10*. https://doi.org/10.3390/healthcare10101940

Kramer, D. B., Baker, M., Ransford, B., Molina-Markham, A., Stewart, Q., Fu, K., & Reynolds, M. R. (2012). Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance. *PLoS ONE*, *7*. https://doi.org/10.1371/journal.pone.0040200

Li, C.-T., Shih, D.-H., & Wang, C.-C. (2018). Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. *Computer Methods and Programs in Biomedicine*, *157*, 191–203. https://doi.org/10.1016/j.cmpb.2018.02.002

Liu, X., Fang, Y.-P., & Zio, E. (2021). A Hierarchical Resilience Enhancement Framework for Interdependent Critical Infrastructures. *Reliability Engineering & System Safety*, *215*. https://doi.org/10.1016/j.ress.2021.107868

Mehdipour, Y., & Zerehkafi, H. (2013). Hospital Information System (HIS):At a Glance. *Asian Journal of Computer Science and Information Technology*, *1*, 2321–5658.

Mohit, P., Amin, R., Karati, A., Biswas, G. P., & Khan, M. K. (2017). A Standard Mutual Authentication Protocol for Cloud Computing Based Health Care System. *Journal of Medical Systems*, *41*, 50. https://doi.org/10.1007/s10916-017-0699-2

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., & Linkov, I. (2013). Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems: Perspective. *Risk Analysis*, *33*, 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x

Patriarca, R., Simone, F., & Di Gravio, G. (2022). Modelling cyber resilience in a water treatment and distribution system. *Reliability Engineering & System Safety*, *226*. https://doi.org/10.1016/j.ress.2022.108653

Petersen, L., Lundin, E., Fallou, L., Sjöström, J., Lange, D., Teixeira, R., & Bonavita, A. (2020).. *International Journal of Critical Infrastructure Protection*, *28*. https://doi.org/10.1016/j.ijcip.2020.100340

Shen, Y.-T., Chen, L., Yue, W.-W., & Xu, H.-X. (2021). Digital Technology-Based Telemedicine for the COVID-19 Pandemic. *Frontiers in Medicine*, *8*. https://doi.org/10.3389/fmed.2021.646506

Shrivastava, U., Hazarika, B., & Rea, A. (2021). Restoring clinical information system operations post data disaster: The role of IT investment, integration and interoperability. *Industrial Management & Data Systems*, *121*, 2672–2696. https://doi.org/10.1108/IMDS-03-2021-0128

Singh, H., Ash, J. S., & Sittig, D. F. (2013). Safety Assurance Factors for Electronic Health Record Resilience (SAFER): Study protocol. *BMC Medical Informatics and Decision Making*, *13*(1), 46. https://doi.org/10.1186/1472-6947-13-46

Taimoor, N., & Rehman, S. (2022). Reliable and Resilient AI and IoT-Based Personalised Healthcare Services: A Survey. *IEEE Access*, *10*, 535–63. https://doi.org/10.1109/ACCESS.2021.3137364

Wallis, L., Blessing, P., Dalwai, M., & Shin, S. D. (2017). Integrating mHealth at point of care in low- and middle-income settings: The system perspective. *Global Health Action*, *10*. https://doi.org/10.1080/16549716.2017.1327686

Walsh, J. M., & Borycki, E. M. (2022). A Resilience Model for Moderating Outcomes Related to Electronic Medical Record Downtime. In *Studies in Health Technology and Informatics*. IOS Press. https://doi.org/10.3233/SHTI210951

Wiig, S., & O'Hara, J. K. (2021). Resilient and responsive healthcare services and systems: Challenges and opportunities in a changing world. *BMC Health Services Research*, *21*. https://doi.org/10.1186/s12913-021-07087-8

Zhang, J., Li, L., Lin, G., Fang, D., Tai, Y., & Huang, J. (2020). Cyber Resilience in Healthcare Digital Twin on Lung Cancer. *IEEE Access*, *8*, 201900–201913. https://doi.org/10.1109/ACCESS.2020.3034324

Zhang, J., & Tai, Y. (2022). Secure medical digital twin via human-centric interaction and cyber vulnerability resilience. *Connection Science*, *34*(1), 895–910. https://doi.org/10.1080/09540091.2021.2013443