Making Healthcare Wireless Safer

By Prof Trish Williams, Ginger Mudd and Gihan Gunasekara,
Flinders Digital Health Research Centre, and
Dr Brendan Lovelock, Cisco Systems.

Sections

Introduction

The delivery of healthcare requires the often-precise orchestration of complex processes and resources to ensure safe, effective and accessible care. Information technology, in particular mobility (wireless) technologies, now plays a pivotal role in enabling this orchestration. Wireless technologies have undergone a rapid evolution and are now at the centre of critical care processes, replacing the traditional cabled communication, enabling the ubiquitous distribution of healthcare information. However, providing this expansive distribution of information comes with the cost of a far less deterministic delivery. Ensuring reliability in the information flow in wireless systems requires enhanced levels of systems design, deployment and maintenance to address this short coming, this includes understanding the wireless driven failure modes in the complete clinical system. Unfortunately, these activities are often significantly under resourced and not well understood. This can lead to an over estimation of the capabilities of wireless systems and an underestimation of the impact of systems failures, resulting in higher risk solutions being designed with the potential to fail at critical stages in the care process. This is not a failure of wireless technologies, as the limitations of these technologies are well known, but a failure to properly incorporate these limitations in the design of care delivery systems and the infrastructure to support these systems.

We are still at the beginning of the mobility (wireless) transformation of healthcare. Existing health IT infrastructure is going to continue to be stretched by the proliferation of mobile, medical, IOT and sensing devices, in addition to the advances in telemedicine. To accommodate this developing ecosystem, reliable and resilient digital infrastructure will be crucial. This infrastructure will include new technologies, such as Wi-Fi 6 and 5G, but more importantly it requires the safe deployment of existing technologies particularly Wi-Fi. Existing challenges span connectivity, resource management and infrastructure needs. Significantly, there is a lack of technical and context expertise when designing these networks, no real-time, proactive monitoring for issues and poor understanding of the failure modes that these technologies generate in the care systems they support. We have not yet solved the current problems in healthcare technology deployment and without doing so the adoption of new technology will not improve. The healthcare industry, as well as government and standards organisations, need to consider how to leverage the fast-evolving ICT ecosystem whilst maintaining safe and effective use of current technology.

This white paper explains why there is a need to pay close attention to this evolution and provides an approach to addressing the current issues in the deployment of wireless enabled healthcare systems together with a glimpse of what the future holds. The paper describes how healthcare delivery organisations can develop best practices in the safe deployment and use of wireless technologies now and into the future.

The delivery of healthcare requires the often-precise orchestration of complex processes and resources to ensure safe, effective and accessible care. Information technology, in particular mobility (wireless) technologies, now plays a pivotal role in enabling this orchestration.

What's the problem of contextualising Wireless to Healthcare?

Today, wireless networks are ubiquitous. In addition to the common use of mobile phones, no matter where you go, the availability of a local Wi-Fi connection is becoming a consumer expectation. The use and demand for wireless connectivity is ever increasing whether shopping at a mall, flying on a commercial plane or waiting for a loved one to emerge from surgery. The phenomenal growth of wireless networks is driven by the design evolution of personal devices enabled by the dramatic reduction in CPU size along with startling increases in processing power. Tiny sensor devices numbering in the millions are now transmitting data by the minute through wireless connections. Hospital networks must cater for the proliferation of these and other mobile technologies as they are the only practical solution to the complex information delivery and process management challenges facing care providers. Thus, wireless technologies, and in particular Wi-Fi, has become a mission critical capability in the array of hospital network tools.

This trend is also fueled by the Internet of Medical Things (IoMT) and smart wearable devices. These developments, together with the need for critical communications, security, privacy, data analytics and the common use of mobile devices, means that enterprise systems have a wide range of network needs. The result is a device and application dense operating environment with increasing demand for wireless bandwidth and reliable communications.

But healthcare is unlike other information environments, such as finance, manufacturing and education. Dealing with the combined avalanche of technology and demand requires a nuanced approach that is optimised to the needs of the healthcare environment. Health is differentiated in the complexity and highly federated nature of the information it shares, its urgency and particularly its impact on the individual. As a consequence, health information systems require designs that reflect those characteristics (BICSI, 2015).

Early use of wireless systems in hospitals was dependent on proprietary technology, but today's systems rely on off-the-shelf components and industry standards. This mix of technology, providers, devices and software, increases complexity and creates higher risks of failure. Ultimately, the specification, design, deployment and maintenance of a hospital wireless network requires a disciplined methodology. The implementation of effective, safe and secure wireless networks requires a collaboration of specialised skills involving infrastructure and IT experts, clinicians, administrators, and biomedical engineers. With a dramatic increase in demand that will be further fueled by imminent 5G and WiFi 6 rollouts, the safe approach to wireless deployment in hospitals needs to be founded on a safe systems approach. This is where the role of wireless networking, with its non-deterministic character, is analysed in terms of the needs of the service being delivered, the possibility of system failure and the redundancy strategies that mitigate harm when those failures occur. Further, there are obligations on healthcare providers for information accountability as well as the desire for increased efficiency, ubiquitous access, flexible data interoperability and portability, and crucially, reliable communications.

Why now? – Issues identified from research

While wireless technology offers dramatic efficiencies and can improve patient care, risk analysis and mitigation are paramount to patient safety. Analysis of real-world failures of wireless technologies in hospital environments reveals a series of common and unusual problems and failures. Some of the failures put patients at risk. This recent research highlights the factors and resulting issues impacting the safety of wireless technologies and wireless networks. The work emphasises the need for hospitals to seriously address how they design, deploy and support wireless-based care systems to ensure patient and staff safety.

Finding solutions

Healthcare Safe Wireless Framework

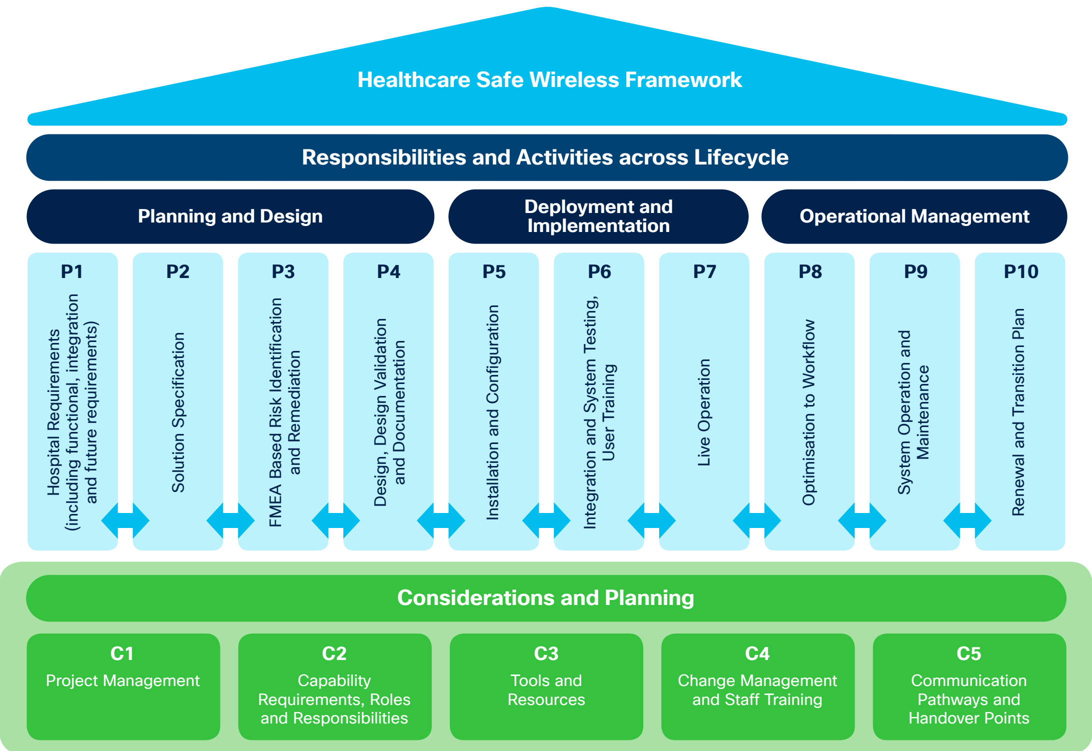
A wireless network must consider medical device technologies, including sensors, communications technologies, software technologies and the network infrastructure itself, but also it must consider how it supports the care processes of the applications that use it. Based on rigorous analysis and identification of significant and potential patient safety issues associated with wireless network design, implementation and use, and based on real-world incidents, a comprehensive Healthcare Safe Wireless Framework has been proposed for the safe implementation of wireless networks.

The framework is a practical, and systematic approach to the design and development of safe and secure wireless networks. The framework is aligned with the IEC/ISO 80001 International Standard for the *Application of risk management for IT-networks incorporating medical devices*. This new Healthcare Safe Wireless Framework provides a methodology for hospitals, designers and implementers to work together to employ informed, relevant and best industry practice and to minimize issues in wireless network deployment.

This approach to a protection framework for hospital wireless infrastructure is innovative because whilst other guideline documents on wireless networking in healthcare are available, they focus on maximising performance and benefits – which are important but do not address significant real-world issues in wireless deployments. This research has investigated real-world data. The resulting Healthcare Safe Wireless Framework addresses the common and unusual issues and incidents that occur in the use and deployment of critical Wireless technology and infrastructure. Using Wi-Fi systems it has identified the critical issues, analysed the root causes and devised mitigations to address the issues. Further, the research has mapped the issues and mitigations across a Wi-Fi deployment project lifecycle to enable integration with best practice in wireless deployment project management.

The framework specifically calls out the critical points of potential failure in the project process activities, as well as identifying the important information transition and communication points. Figure 1 provides the top-level structure to the Healthcare Safe Wireless Framework.

Figure 1: Healthcare Safe Wireless Framework



The Healthcare Safe Wireless Framework consists of three distinct stages (Planning and Design, Deployment and Implementation, and Operational Management) deconstructed into ten pillars of activity across a wireless deployment project lifecycle. The activities comprising each pillar and the specific issues the activity addresses are detailed in the framework. Further, the framework draws attention to crucial considerations that apply across all stages, pillars and activities in five capacities: Project Management; Capability Requirements, Roles and Responsibilities; Tools and Resources; Change Management and Staff Training; and Communication Pathways and Handover Points.

This framework is a methodology that will equip hospitals to build skilled teams, to accurately develop requirements specifications, understand the ramifications and impact of choices made in design, manage the project across its lifecycle, and ensure that technical, administrative and clinical outcomes are met. It identifies the important points in the process that specific expertise is required.

What issues does the Healthcare Safe Wireless Framework solve?

There are many preventable issues identified in each stage of a healthcare wireless network deployment. These range from a lack of design and testing process to a lack of basic ongoing IT and security processes. These include:

- **Poor communication**: a significant issue impacting many points across the project lifecycle, not least in the design phase where a lack of knowledge of the hospital environment, the processes, the devices, and appreciation for clinical workflow, cause significant consequent issues both in technology design and user expectations. Major projects, such as wireless deployment, have created a shift in focus from information governance and getting the basics right to conversations of customer experience. The organisational change that such projects create is important and is currently poorly managed.

- **Under-specification in design**: a consistent issue identified across the project lifecycle. Some decisions are based on cost without an understanding of the ramifications, and this together with a lack of future planning, are also evident. Longer term design and future use are poorly considered in the design phases, thus limiting the potential benefit of the proposed solutions.

- **Lack of expertise and skills sets**: these are a significant factor highlighted in the data analysis. This is across the spectrum of those involved in the project from designers, installers, operational management personnel and the clinical users of the wireless network.

Mission critical closed loop message-acknowledgement cycles: this is where failures in communication occur that have the highest risk to patient safety, and where secondary processes and technology coverage are not well considered.

On-going maintenance and incident management: particularly post deployment, suffer from a lack of defined process and established communication to resolution pathways.

This framework is a methodology that will equip hospitals to build skilled teams, to accurately develop requirements specifications, understand the ramifications and impact of choices made in design, manage the project across its lifecycle, and ensure that technical, administrative and clinical outcomes are met. It identifies the important points in the process that specific expertise is required.

The research into the issues focusing on WiFi systems revealed a wide scope with over forty separately definable Wi-Fi technology incident types, within sixteen specific identifiable issue categories (Table 1), the major problems relate to deployment architecture, software and license configuration, hardware failure and software errors. The Healthcare Safe Wireless Framework brings attention to and addresses these significant issues and failures.

Table 1: Categories of Wi-Fi Issues

Stage 1: Planning and Design	**Stage 2: Deployment and Configuration**	**Stage 3: Operational Management**
Project management	Deployment Architecture	Management
Planning	Deployment Verification and Testing	Monitoring
Design	Legacy Hardware	Performance
Technology Requirements	Configuration	Shadow IT
Budgeting	Software	Software
	People	Security
		Problem investigation and resolution

The Systems Implications of Wireless Technologies

Central to this framework is the need to analyse how the capabilities and limitations of wireless technologies impact upon clinical processes, and consequently, how these healthcare delivery systems need to be designed to accommodate these technology characteristics. While there are many frameworks that analyse systems risk, the Failure Mode and Effect Analysis has been broadly applied in healthcare information systems and forms the process used at the Pillar 3 Feasibility Analysis and Risk Identification stage of the Healthcare Safe Wi-Fi Framework. It is used to analyse risk, and to identify the risk mitigation processes that need to be designed into the system. This is one of many best practice tools used in the Healthcare Safe Wi-Fi Framework, and discussed in more detail here as an example of the integration capability of the framework.

Failure mode and effect analysis (FMEA)

The application of failure analysis and systems failure is commonly used for examining system issues in information systems failure in major incidents, for instance the Chernobyl disaster, the Apollo catastrophic incidents (Debons, 1987), and in car and other manufacturing industries (Anleitner, 2010; Braaksma, Klingenberg, & Veldman, 2012). Indeed, failure of systems as a result of design inadequacy (Bilinski, 1987) is a key concern where complex, integrated systems and different vendor hardware and software infrastructure, whilst interoperable, is deployed. For this reason whole of system testing is imperative (see Pillar 6 Integration and System Testing).

Failure mode and effect analysis (FMEA) adopts a systematic and proactive approach to investigating complex processes and designs, to identify where potential failures could occur in order to devise mitigation strategies (Chandonnet et al., 2013; Latino & Flood, 2004). As a prospective reliability analysis technique, FMEA is a team-based activity and used in healthcare to address patient safety where there are complex and high-risk processes. It should be noted that a FMEA is differs from root cause analysis (RCA), which only occurs after the occurrence of an event and seeks to identify underlying causes. Understanding the mechanics of failure is important and often poorly understood, so using a methodology such as FMEA assists in analysing the human thought process that is inherent in complex processes and design (Latino & Flood, 2004).

In approaching safe wireless network deployment, it is possible to use FMEA prior to, and after, implementing change as it is centred on process redesign to prevent incidents. Further, it combines detection of potential failure with the criticality of the process step. FMEA cannot eliminate risk, but it can identify the potential points of failure and failure modes that should be considered. This is of particular importance in the preventive maintenance of wireless networks (Braaksma et al., 2012) where it can provide reliability analysis for systems function, and in healthcare where people, process, environment and technology all impact outcomes (Prijatelj, Rajkovic, & Sustersic, 2013).

FMEA is undertaken using the following steps:

1. Define the problem to be assessed;
2. Assemble a multidisciplinary team of clinicians, IT personnel, health informaticians, wireless experts and those with specialised knowledge;
3. Describe the process under consideration using a structured analysis method – preferably graphically depicting the process-flow;
4. Analyse the potential vulnerabilities, errors, incidents and the critical area this may impact, and where possible the potential causes of these vulnerabilities. Use a scoring matrix to analyse the issues;
5. Identify actions and expected outcomes; and
6. Redesign process or initiate other mitigations using a systems development methodology (Prijatelj et al., 2013; Stalhandske, DeRosier, Wilson, & Murphy, 2009).

Further reading and detailed application of the technique in healthcare can be found at (Liu, 2019).

How will Wi-Fi 6 and 5G impact healthcare?

What is Wi-Fi 6?

Wi-Fi 6 (developed by the Institute of Electrical and Electronics Engineers (IEEE)), using the 802.11ax protocol, is the newest revision of the 802.11 wireless transmission standard. It is backwards-compatible with the previous wireless protocol version 802.11ac (now called Wi-Fi 5). The technologies behind Wi-Fi 6 result in surprising Wi-Fi speed, an extended range compared to Wi-Fi 5, and a more reliable connection. Wi-Fi 6 has faster speeds through higher data rates, increased capacity, and greater efficiency in device management.

Why is Wi-Fi 6 a leap forward?

In 2019, approximately 19 billion devices (7 billion of which are IoT devices) are connected to the Internet via wireless communications worldwide, many with the ability to share information between devices. By 2021 this is estimated to be 23 billion and by 2025 34 billion (IOT Analytics, 2019). So, our future Wi-Fi networks need to be capable of managing vast amounts of data traffic and Wi-Fi signals.

Wi-Fi 6 achieves this by

- Advanced speed with more bandwidth, realising speeds up to four times faster than previous Wi-Fi versions. The impact of this is a more consistent and reliable network communications providing a seamless experience for users, particularly those using IoT, voice, video and collaboration tools.
- Increased network capacity using improved features including better coverage, ability to handle more active clients per access point and using a new Target Wake Time capability. It does this by transmitting Wi-Fi signals more efficiently over the 2.4Gz band as well as using the 5Gz band. Wi-Fi 6 uses more efficient data encoding, resulting in higher throughput. Whilst the change in speeds over the 2.4Gz band may not be as noticeable in a small environment with few devices, such as at home, it will have a big impact in congested, busy and dense usage areas such as hospitals.
- Improved battery life and power consumption. With many low-power IOT devices connecting via Wi-Fi, Wi-Fi 6 has a new capability called Target Wake Time (TWT) that allows an access point to communicate with the connected device to schedule when the Wi-Fi radio needs to be awake or in sleep mode. This will improve battery life. As a result of this new capability any Wi-Fi enable device, including smartphones and laptops should have extended battery life as less polling of the Wi-Fi connection is required.

How does the Wi-Fi 6 leap impact healthcare?

Improving the Wi-Fi experience for patients and healthcare staff is a key benefit of Wi-Fi 6. Despite the move to use 5GHz Wi-Fi to increase the accessible spectrum and reduce band interference, in environments with solid objects and walls, the 2.4GHz spectrum can be more reliable.

In addition, the new capability for Target Wake Time has two significant benefits for healthcare. Firstly, the reduction in power consumption means that battery powered devices like sensors, patient monitors and the Internet of Medical Things (IoMT) devices will have extended battery life thus increasing the time between replacement or recharge. Secondly, by scheduling the connection times, device signals will avoid interfering with each other, and reduce network signal congestion. This creates more available bandwidth enabling activities that need more bandwidth such as video, VR immersive experiences (used for clinical training) and allows other bandwidth intensive connected devices to be better supported. Importantly, for Wi-Fi enabled medical devices, the resource allocation scheduling by the access point means less overlap and contention and thus less packet drop – i.e. a more reliable, less error prone connection and ultimately improved patient care.

Further, the saturation of devices with demands for continued connection means that Wi-Fi tends to function sub-optimally and much slower in crowded and device saturated environments. The technologies incorporated into Wi-Fi 6 improves by four-times the average speed for each user in areas with dense and high throughput such as emergency departments. Latency (delay in signal transmission) due to poor design and the need for actual 'real-time' data transfer and communication, as identified through the Cisco-Flinders University research, can be addressed by Wi-Fi 6 and its higher capacity, improved coverage and reduction in congestion capability. Also, the functionality to prioritise application traffic, such as using a mix of paging systems and IoT monitoring devices to ensure the most important data is transmitted first, will provide a more reliable application response.

5G Cellular Connection

What is 5G?

5G technology increases the performance of mobile technology by increasing throughput speed and capacity, reduced latency, ultrahigh reliability, higher connectivity density, and higher mobility (5G PPP, 2015). This is enabled by flexible and configurable network functions, provisioned using network slicing. Further, this will be the first cellular communication system specifically designed to integrate seamlessly machine to machine and human to machine type of communications and will be an enabler for the Internet of Things (IoT) (Psiha & Vlamos, 2017).

Why is 5G a leap forward?

5G uses extremely high frequency bands (30-300 GHz) and shorter wavelengths, therefore expanding the spectrum available for communication whilst using smaller physical antennas and support more devices (up to 100 per square metre) than the 4G network. It also has the capability to save power by understanding the data requested and switching to low power mode when a low rate is data sufficient or when not in use.

5G performance is measured by high availability and reduced latency including reduced jitter, reduced packet loss, increased packet survival time and delivery within time specifications. This means that the user experienced data rate (also referred to as mobility) is vastly improved as 5G has the ability to manage high traffic and connection density with better positioning accuracy.

In the future it is expected that a combination of 5G and Wi-Fi 6 will facilitate secure but fast network access. To the user this will be a seamless experience and overcome the issues of lack of reliable coverage in particular spaces and dead zones, particularly in high density areas such as hospitals. The combination of technologies will reduce the challenges and costs associated with more traditional network topologies.

How does the 5G leap impact healthcare?

The benefit in healthcare will be seen through expanded speed and bandwidth of the cellular network for communication Most importantly, where this technology is used for telemedicine, telepresence and 3-D tactile robotic tele-surgery (audio, video and haptic feedback enabled), an increased reliability and faster video can be realised; in effect, lowering the latency issues experienced in 3G and 4G communications. This also opens up the opportunity for virtual reality and augmented reality to be integrated into patient care and clinician training in real-time, where the quality of experience is important.

Further, the movement of healthcare to outside the hospital, with medical devices capability over Wi-Fi and cellular communication channels, provides new opportunities for healthcare delivery and monitoring. This ranges from wearable clinical-grade devices for patient monitoring to tele-presence and virtual reality for connected ambulances (Soldani et al., 2017), and patient tele-rehabilitation (Cisotto, Casarin, & Tomasin, 2019).

5G will facilitate new applications in smart asset tracking and management, intervention planning and follow-up, robotic and wireless tele-surgery and medical training, remote monitoring and real-time data analytics. These use cases are broader than the today's dominant care options, by instrumenting current environments and taking healthcare outside the confines of the hospital building. In clinical environments 5G will enable in real-time rapid data sharing, often of large files such as medical images, and fast simultaneous data collection from multiple points for analytics.

5G will decentralise the healthcare model and help meet healthcare consumer demand for convenience. It will also improve resource efficiency through teleconsultations, remote procedures and gradually transform healthcare to a home environment for preventive, routine and post-operative monitoring and care.

5G is not yet widely available but organisations should be planning to use this and the Wi-Fi 6 innovations.

Next Steps

The safe deployment of a Wireless network involves a resilient infrastructure with maximum availability supported and balanced with effective cybersecurity protection and ongoing monitoring. The research and futures described in this white paper have significance for hospitals, designers and implementers, and the international standards community. The Healthcare Safe Wireless Framework will enable designers and implementers of hospital wireless networks to employ informed, best and relevant industry practice. The Healthcare Safe Wi-Fi Framework provides a guide for hospitals, designers and implementers to work collaboratively to minimise issues in wireless network deployment.

Specifically, this will assist hospitals to build team capacity, develop sound processes and better manage wireless projects to meet business goals.

Consequently, this will provide hospital executives a level of governance over the process and assurance of safe wireless deployment, ultimately reducing patient safety issues due to the change process including installation faults and wireless issues.

Ultimately, the need for accurate and up-to-date information for patient care decision-making rests with the ability of a hospitals infrastructure to meet the clinical needs reliably and resiliently. As the clinical environment is increasingly inundated with wireless devices for communication, monitoring and treatment, coupled with the constant movement of staff and devices and the dynamic nature of healthcare, the necessity for reliable communication infrastructure becomes essential and more urgent. The future will include Wi-Fi 6 and 5G to take advantage of the added capabilities these technologies can provide (latency, speed, reliability, quality of service, and so on). Thus to protect current investments and provide a smooth transition to the future, it is vital to ensure that the existing and new infrastructure are as safe and reliable as they can be.

References

5G PPP. (2015). 5G Vision: The 5G Infrastructure Public Private Partnership: the next generation of communication networks and services. Retrieved from https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf

Anleitner, M. A. (2010). The power of deduction : failure modes and effects analysis for design: Milwaukee, Wisconsin : ASQ Quality Press.

BICSI. (2015). Guide to Medical Grade Wireless Utility (Supplemental Information 2), 1-15. Retrieved from https://www.bicsi.org/docs/default-source/publications/sup_002_mgwu.pdf?sfvrsn=63c51b2c_4

Bilinski, A. E. (1987, 1987//). System Failure Models as a Result of Design Inadequacy. Paper presented at the Information Systems: Failure Analysis, Berlin, Heidelberg.

Braaksma, A. J. J., Klingenberg, W., & Veldman, J. (2012). Failure mode and effect analysis in asset maintenance: a multiple case study in the process industry. International Journal of Production Research, 51(4), 1-17. doi:10.1080/00207543.2012.674648

Chandonnet, C. J., Kahlon, P. S., Rachh, P., Degrazia, M., Dewitt, E. C., Flaherty, K. A., . . . Agrawal, P. B. (2013). Health care failure mode and effect analysis to reduce NICU line-associated bloodstream infections. Pediatrics, 131(6), e1961. doi:10.1542/peds.2012-3293

Cisotto, G., Casarin, E., & Tomasin, S. (2019). Performance Requirements of Advanced Healthcare Services over Future Cellular Systems. arXiv e-prints. Retrieved from https://ui.adsabs.harvard.edu/abs/2019arXiv190601503C

Debons, A. (1987). System Issues in Information System Failure, Berlin, Heidelberg.

IOT Analytics. (2019). State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. Retrieved from https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Latino, R. J., & Flood, A. (2004). Optimizing FMEA and RCA efforts in health care. Journal of Healthcare Risk Management, 24(3), 21-28. doi:10.1002/jhrm.5600240305

Liu, H.-C. (2019). Improved FMEA methods for prospective healthcare risk analysis: Singapore : Springer.

Prijatelj, V., Rajkovic, V., & Sustersic, O. (2013). A Model for Risk Assessment in Health Care Using a Health Care Failure Method and Effect Analysis. Zdravstveno Varstvo, 52(4), 316-331. doi:10.2478/sjph-2013-0032

Psiha, M. M., & Vlamos, P. (2017). IoT Applications with 5G Connectivity in Medical Tourism Sector Management: Third-Party Service Scenarios (Vol. 989).

Soldani, D., Fadini, F., Rasanen, H., Duran, J., Niemela, T., Chandramouli, D., . . . Nanavaty, N. (2017, 4-7 June 2017). 5G Mobile Systems for Healthcare. Paper presented at the 2017 IEEE 85th Vehicular Technology Conference (VTC Spring).

Stalhandske, E., DeRosier, J., Wilson, R., & Murphy, J. (2009). Healthcare FMEA in the Veterans Health Administration. Patient Safety & Quality Healthcare, (September/October 2009), 30-33. Retrieved from https://www.psqh.com/analysis/healthcare-fmea-in-the-veterans-health-administration/