2015-03-01

Medical Device Software and Technology: the Past, Present and Future

Martin McHugh
Technological University Dublin, martin.mchugh@tudublin.ie

Recommended Citation

McHugh, M. (2015) Medical Device Software and Technology: the past, present and future, BEAI Spectrum, Biological and Clinical Engineers Association of Ireland, Spring 2015, pp. 28-32. doi:10.21427/D7F321

Medical Device Software and Technology:

The Past, Present and Future

Dr Martin Mc Hugh

Introduction

Early medical devices were crude and often dangerous. These devices had little complexity and only performed basic tasks. However, with advances in technology also came an increase in the complexity and functionality of medical devices. Medical devices became more and more relied upon in every day healthcare. As with technology in other industries, the medical device industry recognised the benefit of incorporating software into hardware devices. Software was first used in medical devices in in the 1980's. At this time, the software typically performed rudimentary functions such as turning a device on or off, or displaying limited information such as a patient's temperature. However, through advances in technology, the role of software has expanded well beyond its humble beginnings. A number of tasks traditionally performed manually by clinicians are now being performed by automated software driven devices. Medical device manufacturers have embraced the use of software in order to increase the level of functionality of their devices without the need for costly mechanical additions. Using software to replace mechanical components can also result in smaller, more portable medical devices. It is estimated that the amount of software in medical devices doubles approximately every 24 months (1).

As the amount of software used in medical devices is increasing, so too is the level of scrutiny which regulatory bodies are placing upon these devices. Traditional medical devices consisted of hardware components which could easily be examined to determine if a defect was present. However, with software driven medical devices it can be very difficult to identify defects. To overcome this challenge, regulatory bodies place restrictions on the processes that are followed when developing software for use in healthcare. Traditionally, these restrictions only applied to a device manufacturer, as a medical device was seen as a standalone entity however, this has now changed. Recent technological changes have resulted in the ability to connect medical devices to existing network infrastructure. This connectivity allows for the greater exchange of information and increases the availability of information produced from a medical device. However, this has created the possibility that devices sharing a network, which consists of a medical device, could have an impact on the safe and reliable performance of that medical device. While manufacturers and distributors are responsible for individual devices, Healthcare Delivery Organisations (HDO) are responsible for ensuring that medical devices connected to a network perform as intended. It has been shown that this responsibly typically falls upon clinical engineers and physicists within HDOs.

The use of mobile devices is also on the rise in healthcare. These mobile devices offer clinician access to a vast amount of information which can be used to help better diagnose

and treat patients. Nonetheless, a large amount of uncertainty remains with regards to the regulation of these mobile devices for use in a healthcare environment.

The Past

In the US, the Food and Drug Administration (FDA) regulates medical devices. The FDA in its current form originated in 1930. In 1938, the US Congress passed the Federal Food, Drug, and Cosmetic Act (FFDCA). This act gave authority to the FDA to oversee the safety of food drugs and cosmetics. In 1976, the FFDCA was amended to include medical devices. The key element of this amendment was that medical devices must be classified into one of three categories i.e. Class I low risk, Class II medium risk and Class III High risk. Any medical device that was marketed for use prior to this amendment became known as a pre-amendment device and as such, automatically received a Class III classification until reclassified by the FDA. As discussed, software was first used in healthcare during the 1980's. Consequently, in 1981 the FDA began to investigate the role of software in healthcare. In 1987 they published their Draft Software Policy, as they recognised that software used in healthcare could meet the definition of being a medical device. However, as the level of software based products grew beyond the FDA's expectations, they determined that it was impractical to adopt a single software policy. As a result, the Daft Software Policy was never officially published and was withdrawn in January 2005. Currently, the FDA does not specifically regulate any form of software used in healthcare and instead regulates *"any instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory" (2).*

In November 1997, the FDA signed into law the Modernisation act, known as the Food and Drug Administration Modernization Act (FDAMA). A key element of FDAMA is the advocating of the use of standards in the design review process. To support the FDAMA, the FDA published in the Federal Register, a list of standards to which medical device manufacturers could declare conformity. A key objective of the FDAMA was to reduce the burden on both the FDA and medical device manufacturers by reducing the regulatory obstacle to entry to international and domestic medical device markets. When the FDAMA was signed into law, the Centre for Devices and Radiological Health (CDRH) established Standards Technology Groups (STG), one of which had a specific focus on software. A STG is responsible for software categorised as follows:

- General process standards, which are technology independent;
- General process standards, which are technology dependent;
- Specific process implementations.

A number of standards are included on the federal register list of standards, of most significance with regards to medical device software development is IEC 62304:2006 Medical Device – Software Life Cycle Processes. Also of significance to medical device software and all types of medical device is ISO 14971 Application of Risk Management to Medical Devices. All medical devices marketed for use within the US, regardless of device safety classification, must provide evidence of adoption of a Quality Management System (QMS), such as in accordance with 21 CFR 820 Quality Systems Regulations (QSR) (3) and the FDA Design Control Guidance for Medical Device Manufacturers (4). Of note within the QSR

is Subpart C – Design Controls, which provides information as to which processes must be adhered to when developing regulatory compliant software. These include:

- Design & Development Planning (Specifications);
- Design Output (Coding);
- Design Review;
- Design Verification (Was the Product Built Right);
- Design Validation (Was the Right Product Built).

The primary objective of the QSR is to ensure the safe and reliable performance of a medical device. A device is deemed safe if it does not cause harm to a patient, clinician or third party and it is deemed reliable if it performs the desired function each and every time it is used.

In Europe, all medical devices marketed for use must conform to the regulations defined by the European Council. Medical devices intended for use within the European Union (EU) must have a CE conformance mark (5). To achieve this conformance mark, audits are performed on these devices to ensure their safety and reliability by notified bodies within each country. Within the Republic of Ireland, the National Standards Authority of Ireland (NSAI) is one authority responsible for ensuring conformity before awarding a CE mark. These devices typically needed to satisfy standards which include: EN ISO 13485:2003 (6) medical device quality management standard, EN ISO 14971:2009 (7) and the medical device product level standard IEC 60601-1 (8, 9). A key element of this process of achieving conformance differs to that in the US, as there is no single authority responsible for ensuring conformance. Once a medical device manufacturer has received the CE mark in one EU member state, then they are free to market their medical device in any EU member state.

The Present

In 2000, a report titled “To Err is Human”, identified that each year over 98,000 people die in hospitals due to preventable causes. An example of one such failure is the Therac-25. Therac-25 used software to control when a radiation beam spreader plate should move into place. A failure in this software resulted in the spreader plate not moving into place when required, resulting in 4 patients dying and 2 being left permanently disfigured. A subsequent report following these incidents identified that the software failed as a result of using legacy software and a single developer. In another case, a Panamanian Teletherapy device failed due to faulty software resulting in the death of 21 patients. It is reported that software was cited as being the most common cause for a medical device recalls (10) with 24% of all medical devices recalled by the FDA in 2011 being as a result of software failures (11).

Software as a Medical Device

In 2007, the European Council published the most recent amendment to the Medical Device Directive (MDD) known as 2007/47/EC (12). The original MDD, known as EC 93/42/EEC (13) was first published in 1993 and provided a definition as to what constitute a medical device for use in the European Union. A number of changes were included as part of this latest amendment, but perhaps the most significant change was the inclusion of software into the definition of being a medical device. While the use of software in healthcare was recognised

prior to this, it was seen as a constituent component of a hardware medical device. To provide further clarity as to what this change means, the amendment goes on to state that "*standalone software is considered to be an active medical device*". However, this wording only served to cause more confusion amongst medical device manufacturers. In 2012, the European Council published MEDDEV 2.1/6 (14) to provide clear guidelines as to what software could be considered as standalone software. This guidance document, as with the FDA approach to software, confirmed that the intended use of the software is the determining factor as to whether or not it was considered standalone software and consequently be subject to regulatory scrutiny.

There are four different types of software used in healthcare which are subject to regulatory scrutiny:

- Embedded software in a medical device e.g. software used as part of an infusion pump;
- Standalone software as a medical device e.g. software running on a personal computer which calculates chemotherapy dosages ;
- Hospital Information Technology e.g. electronic health records;
- Mobile Device Software e.g. smartphone and tablet apps.

FDA Medical Device Data Systems Rule

Prior to April 16th 2011, devices that now meet the current definition of being a Medical Device Data System (MDDS) were classified as either a Class III device (potentially high risk), or assumed the safety classification of the parent medical device to which they were connected. However, the FDA had been operating under their discretionary enforcement policy and therefore was not enforcing the Class III requirements on all MDDS. On April 16th 2011, a FDA rule became effective which classified a MDDS device as a Class I, 510 (k) exempt - medical device (15). This ruling came three years after the proposed ruling was issued on February 8th 2008. This final classification modifies FDA 21 C.F.R § 880.6310 (15) and describes a MDDS as being:

> *"software, electronic, or electrical hardware such as a physical communications medium (including wireless hardware), modems, interfaces and communications protocol"*

The FDA provided the following definition of what constitutes a MDDS:

> *"A device that is intended to provide one or more of the following uses, without controlling or altering the functions or parameters of any connected medical devices:*
> *(i) The electronic transfer of medical device data;*
> *(ii) The electronic storage of medical device data;*
> *(iii) The electronic conversion of medical device data from one format to another format in accordance with a pre-set specification; or*
> *(iv)The electronic display of medical device data."*

There is however, an exception to this rule. If software exclusively performs one or more of the functions outlined in the definition of a MDDS and is used for active patient monitoring, then it cannot be considered a MDDS and must be considered an accessory or medical device in its own right. This ruling created a level of ambiguity amongst medical device software development organisations. Electronic Health Record (EHR) and Computerised Physician Order Entry (CPOE) systems appear to meet the definition of being a MDDS, but are explicitly outside of the definition of being a MDDS. The reason cited for this, is that these systems possess the ability to order tests for patients automatically, thus generating clinical data which is beyond the scope of a MDDS.

The Future

Mobile Health

The term Mobile Health or mHealth refers to the use of mobile devices to support the practice of medicine. mHealth is most commonly seen in smartphones and tablets. Since the inception of these devices, there have been apps designed for use in healthcare. Most of these apps met the definitions of being medical devices and should have been subject to regulatory scrutiny. However, the developers of these apps were avoiding regulatory scrutiny by stating that the software they had developed was for lifestyle purposes and was not intended for use in direct patient care. In 2013, the FDA released its Mobile Medical Applications Guidance for Industry and Food and Drug Administration (15). This guidance document brought clarity to medical device application (app) developers. Initially, confusion arose as to whether platforms on which these apps operate would be subject to regulatory scrutiny, for example, would the latest version of Android need to be approved by regulatory bodies before a medical app which runs on Android could be approved for use. Fortunately, regulatory bodies have decided that once the app is fully validated in accordance with quality management regulations, such as ISO 13485 or the FDA Quality System Regulations (3). A recent survey in the UK identified the potential benefits to be gained by adopting mHealth (16). While this research is still in its early stages, it was revealed that if mHealth was used correctly there could be a 20% reduction in emergency admissions, 14% reduction in bed days and a decrease of 45% in mortality rates.

Clinical Decision Support Systems

The decision process in healthcare is essential. There are three decision processes which must be followed in connection with patient care(17):

- Diagnostic Process – determining which questions should be asked or tests to perform to establish a diagnosis;
- Diagnosis – determining the patients diagnosis based upon the diagnostic process;
- Management – determining the best course of treatment for the patient based upon the diagnosis.

As each of these processes is supported by the preceding one, a failure in one will result in an overall failure in the treatment process and could result in adverse effects being suffered

by the patient. As a result, medical device manufacturers have sought out a ways to support these processes through the use of software.

Decision Support Systems (DSS) is a software application which provides a solution to a decision maker by compiling useful information from a number of sources, such as raw data, documents and personal experiences. DSS have gained acceptance in other industries to assist in resolving structured and unstructured problems.

The healthcare industry has begun to embrace DSS, creating Clinical Decision Systems (CDSS). CDSS are of particular use in the healthcare industry as they take into account a number of variables and factors. These CDSS can provide clinicians with solutions based upon extensive records. Should a clinician wish to form the same solution without a CDSS, they would need to perform an exhaustive amount of research. This may be feasible in isolated cases, however for routine cases, the costs of implementing the CDSS would be exceeded by the ultimate benefits. An example of one such CDSS is an app developed by an Irish software organisation known as OncoAssist. This app, intended to run on mobile platforms, was developed in conjunction with oncologists to provide treatment dosages based upon a large volumes of historical data. This app is one of the first mobile apps of its kind to receive regulatory approval in Europe.

Medical IT Networks

Traditionally, when medical devices were connected to a network, the network would be an isolated network consisting of proprietary devices, installed and supported by the medical device vendor. This allowed the medical device vendor to have control over configuration, such as IP addressing, which made support and service of the network easier. With the medical device vendor providing the network, this relieved the hospital of the responsibility of supporting life critical applications themselves. However, use of proprietary networks in this way presented a number of disadvantages in that as medical devices increasingly were designed to be incorporated into a network, the result was a proliferation of these networks, resulting in the situation where large hospitals could have a large number of isolated networks. The maintenance of a large number of private networks is impractical and increasingly devices are being designed to be incorporated into a hospitals general IT network. General hospital IT networks are highly flexible and highly configurable. Incorporating a medical device into an IT network can introduce additional risks that are specific to the that device, which may not have been considered during the design and manufacture of the device (18).

In order to address these risks, IEC 80001-1: Application of risk management for IT-networks incorporating medical devices (19) was published in 2010 which outlines the roles, responsibilities and activities that are required for the risk management of a medical IT network. IEC 80001-1 advocates a life cycle approach to risk management. The standard looks at the medical IT network from the perspective of maintaining 3 key properties of the network – Safety, Effectiveness and (Data & System) Security. Safety deals with ensuring that the device does not cause harm to the patient, the user of the device or the environment. Effectiveness is concerned with ensuring that the device continues to provide

the intended result for the patient and the Responsible Organization. A Responsible Organisation is defined within the standard as an entity accountable for the use and maintenance of a medical IT network. Data & System Security ensures that information assets are reasonably protected from degradation of confidentiality, integrity and availability. A medical IT network is defined within IEC 80001-1 as “an IT network that incorporates at least one medical device”.

Conclusions

Medical technology has changed dramatically over the past 40 years. The level of software in medical devices has grown exponentially since its first inception. Software initially performed very limited tasks as part of a hardware device, however, this has now evolved to software potentially being considered a medical device in its own right. While the inclusion of software has increased the capabilities of medical devices, the number of failures of medical devices due to software faults has also increased and this has drawn extra attention from regulatory bodies.

A traditional medical device consisted primarily of hardware with the possibility of a software component. Due to advances in software technology, regulatory bodies have extended their definition of a medical device and now a medical device can be solely software with no hardware component. While this has created confusion amongst medical device manufacturers as to whether or not software is or is not a medical device, they simply need to refer to the intended use of the software and if this meets the definition provided by regulatory bodies, then the software is defined as being a medical device.

The use of mobile apps are growing at a fast pace within healthcare as these apps offer clinicians the ability to consult large amounts of historical data which assist them in making more informed clinical decisions, for example CDSS. These assist in the three stages of the diagnosis and treatment stage and will no doubt become common place in modern healthcare. It can be seen that advances in medical technology have grown at a furious pace of the past 40 years and through the further advancements including mobile technology, this growth is expected to continue.

References

1. Sarig I. Meet Embedded Software Quality Challenges in Medical Device Development. Medical Electronic Device Solutions [Internet]. 2012. Available from: http://medsmagazine.com/2012/02/meet-embedded-software-quality-challenges-in-medical-device-development/.
2. Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301, (2004).
3. FDA. Title 21--Food and Drugs Chapter I --Food and Drug Administration Department of Health and Human Services subchapter h--Medical Devices part 820 Quality System Regulation. Maryland: U.S. Department of Health and Human Services, 2007.
4. FDA. FDA Design Control Guidance for Medical Device Manufacturers. Maryland: Centre for Devices and Radiological Health, 1997.
5. British Standards Online (America), http://www.bsiamerica.com/en-us/Sectors-and-Services/Industry-sectors/Healthcare-and-medical-devices/CE-marking-for-medical-devices/.
6. EN ISO 13485:2003 Medical Device: Quality Management Systems. Requirements for the Regulatory Process, 24-July-2003.

7. EN ISO 14971:2009 Medical Devices. Application of Risk management to medical devices 31-July-2009.
8. EN 60601-1 Medical Electrical Equipment. General requirements for basic safety and essential performance. Collateral standard. Usability 31-May2010.
9. Emergo Group, http://www.bsiamerica.com/en-us/Sectors-and-Services/Industry-sectors/Healthcare-and-medical-devices/CE-marking-for-medical-devices
10. Eisenhart S. FDA Report: US Medical Device Recalls Up nearly 100% since 2003 2014. Available from: http://www.emergogroup.com/blog/2014/03/fda-report-us-medical-device-recalls-nearly-100-2003.
11. Selwood D. Software That Can Kill. Electronic Engineering Journal [Internet]. 2012. Available from: http://www.eejournal.com/archives/articles/20120711-swkills/.
12. European Council. Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007. EU Bookshop: European Council, 2007.
13. European Commission. Council Directive 93/42/EEC of 14 June 1993 concerning medical devices. 1993.
14. Medical Devices Guidance Document - Qualification and Classification of stand alone software MEDDEV 2.1/6, (2012).
15. FDA. 21 CFR Part 880 Medical Devices; Medical Device Data Systems Final Rule. Federal Register 2011;76(31):8637 - 49.
16. Department of Health. Whole System Demonstrator programme: Headline Findings: December 2011. 2011.
17. Musen MA, Middleton B, Greenes RA. Clinical decision-support systems. Biomedical informatics: Springer; 2014. p. 643-74.
18. Gee T. Medical Device Networks Trouble Industry: Medical Connectivity; 2008 [27/1/2012]. Available from: http://medicalconnectivity.com/2008/12/18/medical-device-networks-trouble-industry/.
19. IEC. IEC 80001-1 - Application of Risk Management for IT-Networks incorporating Medical Devices - Part 1: Roles, responsibilities and activities. Geneva, Switzerland: International Electrotechnical Commission; 2010.