Collaborative Discussion 1: Information System Failure

My colleague Anrich brought forward a heartbreaking example of a systems failure that led to six documented cases of patients being given overdoses of radiation during therapy.

Anrich noted how only a single developer had worked on the projects code. To this I added:

Hi Anrich,

This is a very interesting case. On medical projects I have worked on, developers were not allowed to review their own code as they may miss things a fresh pair of eyes would not. For projects like this where the config should change the output, we would create test steps in a verification matrix that would test changing between different configs. It may be hard to measure radiation safety of course so I imagine that would be left disconnected and instead perhaps voltages could be read to test the output as "black box".

My colleague Jonathan looked into the standards involved in this process and wanted to know if anyone knew which standards applied to medical devices specifically, to this I responded:

Hi Jonothan,

Organizations that want to produce medical devices will often follow the ISO 13485 directive for their QMS. ISO 13485 has requirements for things like change control and document control.

For CE marking in the EU, for a long time the Medical Device Regulation has been the main standard, this is however, being superseded by the Medical Device Directive this year. The new MDD has a greater emphasis on the life cycle of a medical product with increased requirements on post-market surveillance. MDD also requires all new products to be registered in the EUDAMED database with a unique identifier (UID).

To show compliance with the MDD organizations can apply the standard of IEC 62304 (medical device software) which covers safe software design and maintenance. Every medical device software will need to be given a safety classification of either A, B or C. The classification of the device software affects the level of documentation and testing required. IEC 62304 describes tasks that need to be completed during the software development process such as requirement analysis, detailed design and integration and integration testing. The standard does allow a large area of freedom on how some of these stages are carried out, for example, integration testing can be either very in-depth or simply check the project complies (bad), the organization must justify their approach.

References

Bellairs, R. (2019) What Is IEC 62304? Compliance Tips For Medical Device Software Developers. Available from: https://www.perforce.com/blog/qac/what-iec-62304 [Accessed 10 February 2021].

David brought forward an interesting case where a system delivered by IBM was defective. This conversation raised a discussion of different implementation approaches such as "direct change over" and "phased implementation".

Hi David,

Thank you for sharing this very interesting example. I have read a more recent article and found out a little more about each side take on the failure.

There seem to be multiple problems here, firstly the project ended up $30M over budget and 5 months late, secondly - as you said - the system went live in a defective state. It seems to me that the project blowing its budget could cause a snowball effect that could lead to bad business decisions such as deploying early.

Reading that this new system disrupted profits for months, I wonder whether it would have been possible to run both the new and old system in parallel during a testing phase.

If the systems could be run in parallel (which may induce an overhead) then it could give the means to confirm the correct operation of the new system by comparing it to that of the pre-existing system.

We have learned about iterative development; I think it's interesting to note that this can enable flexible project costing if each phase of iteration is costed separately. I wonder if an iterative development approach could have helped with costing and testing on this project.

Belden, J. (201) BRIDGESTONE VS. IBM: PARTIES AGREE TO REACH AGREEMENT Available from: https://upperedge.com/ibm/bridgestone-vs-ibm-parties-agree-to-reach-agreement/ [Accessed 09 Feb 2021].*