Arthur D Little

Risk Practice Viewpoint

Agile Safety

How to transform safety assurance - Introducing agile concepts in safety and risk-related areas

There are people who worry that agile approaches to developing systems and management processes will impair safety. However, proponents of an agile approach argue that the regular cycles of test and review will mean that the team will identify safety requirements that may have been missed under a traditional approach, improving the overall level of safety that is delivered, since when using agile the safety activities will be fully integrated with other activities (not just acting as a 'check' function), and the result will have better solutions built in. This paper seeks to start to explore the challenges of agile safety and build on a view that agile, when done well, could be safer than other (more conventional) approaches to safety management.

Traditionally many business processes are carried out in a linear, step-by-step manner where one step needs to be completed before the next is undertaken. This is especially true whenever safety is involved, because safety assurance processes tend to place a strong emphasis on documentation and sequential progress through stage gates. While such an approach is effective for providing assurance, sequential decision-making is often slow and inflexible. Moreover, such approaches can lead to a culture of overemphasis on following the process, and meeting requirements and targets to progress through each stage gate. Adhering to the process can become a goal in itself rather than a means to achieving the business aims, for example developing a robust, reliable and safe product, providing an efficient and effective customer service or managing the organization's risk exposure.

Therefore, organizations are increasingly looking to use new – agile – business processes to reduce time-to-market and improve the way they manage their business, develop products and serve customers. The agile process is a concept that first arose in software development, where it was used to allow development of systems based on rapid development cycles, and it is now being adopted in other areas where businesses seek to respond quickly to change. It involves principles such as flexibility, dynamic teamwork and networking.

The challenge

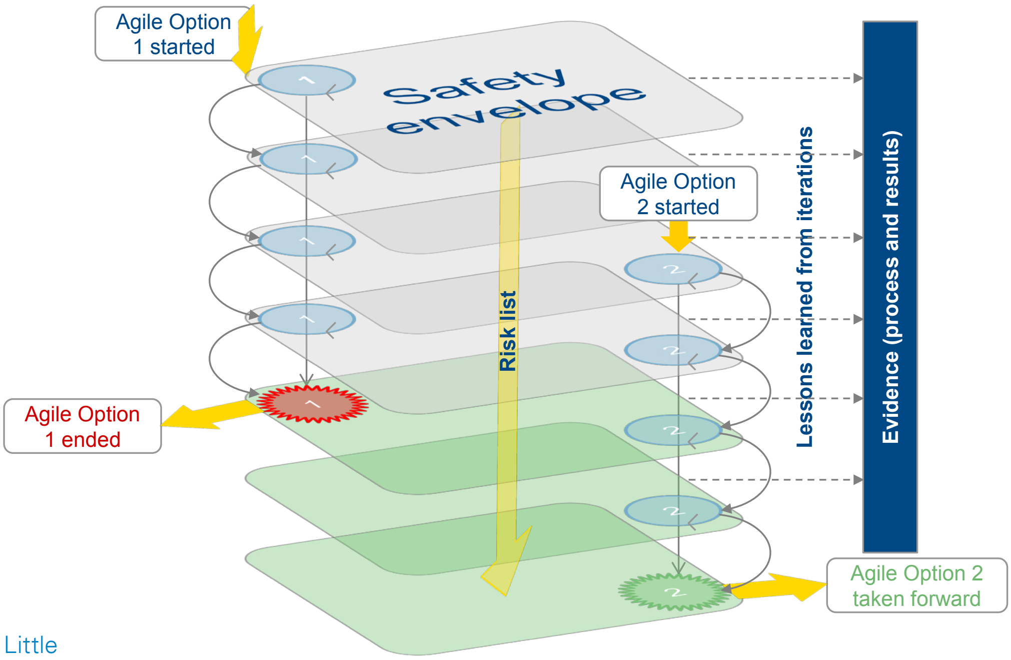
For organizations moving to agile processes for safety related activities there can be significant challenges to overcome. This arises as agile emphasizes delivering results and rapid change over processes, tools, documentation or plans. Existing regulations and standards in many industries make it difficult for the organization to adopt agile concepts, especially in the case of high-reliability systems, or where safety or security is affected. Indeed in most cases the use of a linear, gate-driven and highly documented process is explicitly prescribed. Despite these challenges, a number of organizations are exploring how to adopt agile concepts for these types of safety related situations.

To be successful and overcome the sometimes fierce resistance from proponents of the traditional approach, companies will need to be able to demonstrate that adopting agile processes delivers results that are at least as good as those achieved by applying the existing linear processes.

The way forward

One current concept that is showing some initial success is to define a clear safety envelope and focus on working within this envelope. The idea of the safety envelope is to define the boundary of what should be achieved, instead of creating a long list of all the things that must not be done. The safety envelope

Figure 1: The process in the safety envelope



Source: Arthur D. Little

says what to achieve, in a positive sense, to demonstrate safety at all times during change. For example, in a recent highways project that was using new innovative technology and operating regimes, a clear safety envelope was defined in terms of an agreed global safety level that allowed room for manoeuvre as options were explored, developed and tested. The project needed to show that it always stayed within the agreed safety envelope as the design and development work progressed. New concepts and trials could be implemented as long as the overall result could be shown to be within the envelope.

Another concept being explored is to develop and implement different options in parallel incremental steps (Figure 1).

As each agile iteration is carried out, multiple options may be implemented at the same time as long as the overall safety envelope is respected. Feedback is collected on the effects of the change and the lessons learned from each iteration are used to inform future development and iterations. Relevant evidence is collected from each cycle and fed back into future cycles to enable evidence-based decisions to be taken. Using this approach, organizations can agree and adjust the safety envelope with relevant stakeholders. They can then demonstrate, through evidence, that all changes stay within the defined and agreed envelope and that, hopefully, the overall result is actually improved as lessons are learned. This is shown in Figure 1 above, as multiple options are explored within the envelope, with lessons learned and evidence collected from each cycle. Activities such as hazard management are carried out and form part of the process of improving the overall result.

Not just theory

The use of agile approaches in safety applications is more than just theory. For example, a metro railway system is currently exploring how to manage change through the use of operational envelopes and model-based environments. The model-based environment would enable it to test changes to operations within the model, using agile principles. Multiple changes to operations could therefore be tested using agile development principles before the changes are tried on the railway.

An international manufacturing company recently adopted agile concepts when looking into ways of strengthening risk management processes for its product development projects. The standard procedures for updating the risk management guidelines and tools would have taken around 18 months. However, the company was keen to improve risk management on critical projects that were currently underway. The company first piloted some new ideas on a small number of existing projects, each at a different stage of the product development lifecycle. Further ideas that were thought to be useful were then rapidly implemented on around 20 projects. Not all ideas were rolled out to each of the 20 projects, but only those ideas that were relevant to each project. Based on the lessons learned and evidence of success, the company's project risk management guidelines and tools were updated and made available to all of the company's development projects. Not only were the new and improved guidelines and tools available nine months after the start of the first pilot project (i.e. in half the time of the standard updating process) but the changes included had also already been trialed and tested in real projects, making their wider adoption more likely and successful. Simultaneously a cadre of experienced enthusiasts was available to advocate the wider uptake of these approaches across the company.

Why might an agile approach be better?

There are a number of potential reasons why an agile approach to change may be safer, if done well. Anecdotal evidence suggests that many companies use, to some extent, agile principles and then pull together the formal plans, documents and process compliance at the end. Explicit recognition of this and the development of suitable agile processes will lead to greater efficiency and possibly safer products, as discussed below.

The theory behind much of what has been traditionally required to manage safety is that requirements can be set as part of the specification or plan, then they are delivered and checked or tested. One weakness with this approach is that at the planning stage the requirements may not actually all be known, especially if any innovation is involved. New requirements may, and in our experience often do, emerge as the work is undertaken because they were not known at the start. An agile approach works very well with such emerging safety requirements, as it aims to add new requirements as the development occurs and to test that the result delivers what is required by users.

Since the new system or procedures will emerge in increments it is possible for the end users to understand the safety implications of the new system or change earlier, as testing and use starts. This means that any significant potential safety concerns that had not been foreseen will be seen earlier in the change and can then be addressed, or, if it makes sense, the change can be abandoned before too much effort is invested. This same early testing process will also help new safety requirements emerge earlier in the change process so that they can be addressed as they emerge.

An agile approach can therefore lead to embedded safety, with identified safety requirements influencing design and leading to increased opportunities for innovation. In our experience this is especially important for sub-element integration; it is the behavior of interfaces between sub-elements of a process or system that are often least well understood. Early application of identified safety requirements to these interfaces can help eliminate unsafe system behaviors from interface functionality.

If the change is set up to deliver safety requirements in the early releases there will also be early delivery of the safety benefits, with greater evidence gathered of their delivery. At the same time there will be early detection of the failure of the change to deliver safety requirements.

The safety team will also be fully involved in the agile process and will not act as a checking function, which is often the case in the traditional approach. So the team will work together to deliver a safety result, not have safety 'bolted on'. The iterative approach also means that the assessment of the change can be done in smaller increments thus making sure that the requirements are well understood at all times. A further advantage of the close involvement of the safety team is the reduced project and commercial risks associated with safety approval. Early external review of the safety requirements will help build confidence and demonstrate that safety has been embedded at an early point within development of the process or system – this is often difficult to determine from document review alone so the early cycles of development and test will bring these to life. In our experience this approach tends to lead to fewer latent safety anomalies, which may under a traditional approach, only emerge at a later stage in release (either during development of a new version or after a period of use of the process or operation of the new system).

Conclusion

Organizations are increasingly moving to agile business processes as a means of improving efficiency, effectiveness and responsiveness to change. However, in certain safety or risk-related areas existing regulations and standards make this difficult. Some leading companies are exploring ways of adopting agile concepts for these areas and thinking through how this can be done. Promising approaches for further exploration include the use of safety envelopes and incremental/pilot implementation. To be successful in the long run, companies will need to demonstrate to stakeholders that the results achieved with agile processes are at least as good as those using traditional approaches, if not better. There is still some way to go before stakeholders can be convinced, but the early signs are promising.

The debate about agile approaches and safety will continue. It is clear that this subject cannot be ignored as calls are now being made to change standards so that agile safety can become an approved process for delivering safe systems and management processes. Will it be safer than the traditional approaches? On that we will have to wait a see, but there are reasons to believe that, if done well, it could be.

Contacts

James Catmur
catmur.james@adlittle.com

John Barker
barker.john@adlittle.com

Arthur D. Little

As the world's first consultancy, Arthur D. Little has been at the forefront of innovation for more than 125 years. We are acknowledged as a thought leader in linking strategy, technology and innovation. Our consultants consistently develop enduring next generation solutions to master our clients' business complexity and to deliver sustainable results suited to the economic reality of each of our clients.

Arthur D. Little has offices in the most important business cities around the world. We are proud to serve many of the Fortune 500 companies globally, in addition to other leading firms and public sector organisations.

For further information, please visit **www.adlittle.com**