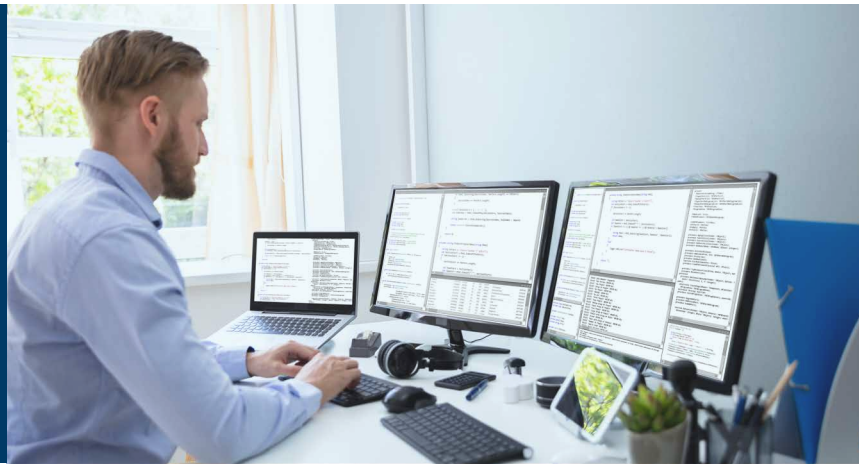
The Institution of Engineering and Technology

Agile in a safety-related environment

This flyer on Agile is one of two high-level IET guidance documents on the benefits and pitfalls / challenges of Agile development and DevSecOps (**Dev**elopment, **Sec**urity, **Op**erations)[1] practices for organisations undertaking safety-related projects, products, or services. Its aim is to spread awareness and to increase understanding and the use of good practice amongst engineering managers in this area.



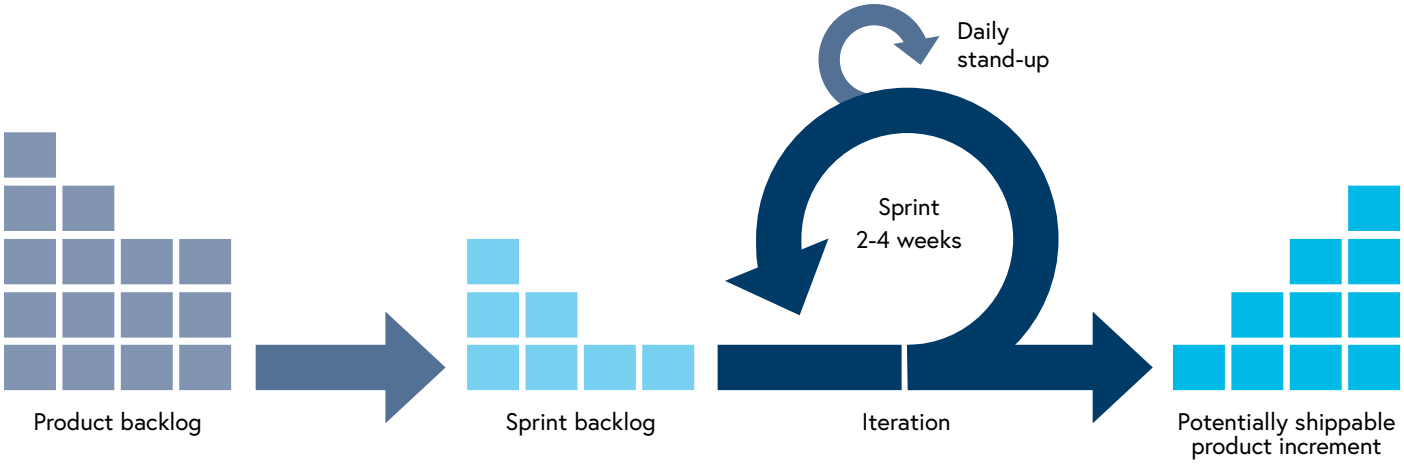
The Agile software development methodology emerged in the late 20th century and focuses on the iterative development of software to meet stakeholder needs in a rapid and responsive way. It emphasises building software incrementally, responding to customer feedback and continuously improving software development processes, tools, and techniques.

One milestone in the development of Agile methodologies was the publication of the Agile Manifesto in 2001, which detailed the following high-level principles:

1. **Individuals and interactions** over processes and tools
2. **Working software** over comprehensive documentation
3. **Customer collaboration** over contract negotiation
4. **Responding to change** over following a plan

These values were articulated by the authors of the manifesto in response to what they saw as misaligned priorities in software development. They felt that the focus should be on rapid, iterative development of software, with an emphasis on meeting customer needs as dynamically as possible. To this end, they believed that the bolded items (left) were worth more attention than the non-bolded items.

Figure 1: A typical Agile lifecycle.



[1] DevSecOps is an approach that uses high degrees of automation to improve the ability of teams to develop, deliver and manage the security of their software products. In doing so, it reduces costs, increases delivery rates and enhances a culture of transparency and assurance.

The Institution of Engineering and Technology

Since its publication, a significant number of criticisms of and reflections on the Agile manifesto have been authored; practitioners recognise the need for some degree of tailoring and balancing of these principles to enable Agile to work for organisations delivering complex systems. As an example, most organisations have expanded their definition of 'working software' to include a necessary level of documentation. The importance of sharp tools (i.e. tools that streamline development) has also been widely recognised.

One issue when considering the adoption of these development methodologies and practices is their applicability and suitability to safety-related or safety-critical system development. In such environments, ensuring the safety as well as the security of produced artefacts is crucial to any underlying assurance case of the system, product, or solution. The selected software development lifecycle must generate suitable and timely evidence to enable compliance with all specified safety and security standards; this does not necessarily preclude the use of Agile, however.

Organisations working in the safety-related field can assess whether adoption of Agile is appropriate for them by asking some simple questions:

1 Does the organisation have users or customers to whom they can deploy software for evaluation and receive rapid feedback?

If software cannot be rapidly demonstrated to users, reviewed by them and their feedback used to inform future software iterations, Agile may be of less benefit.

If on the other hand there are end users who can provide feedback on the software, Agile is worth serious consideration.

2 Does the organisation have a firm understanding of safety standards and what is required to achieve them?

If yes, it is entirely possible to develop an Agile lifecycle that meets both the business need (increased agility of development) and safety case obligations.

If no, Agile may create additional issues unless the organisation can communicate clearly how they will achieve and evidence their safety obligations.

3 Does the organisation have a regulator or other supervisory authority that has published standards and guidance for how software development should be undertaken within the domain?

If yes, it is critical to clear any proposed movement to Agile development with the regulator to be certain that such an approach is suitable and acceptable, as they may have mandated or recommended Agile methodologies.

If no, and the answers to the previous questions are yes, it is worth undertaking an investigation into which Agile technique is most suitable prior to migration.

Agile has many variants from simpler versions, such as Scrum, to those intended for doing Agile development at scale in complex system-of-systems environments such as Scaled Agile Framework (SAFe) and Large Scale Scrum (LeSS). The common factor is that they all support an incremental software development process. It is important that organisations considering moving to Agile research the available spectrum of techniques and select one that is likely to provide the most success, particularly in a safety related environment.

This is the second in a series of IET outputs on this topic. A more detailed document is currently being developed and will be published shortly.

All feedback on this paper is welcome. Please contact sep@theiet.org. This paper has been produced by the Engineering Safety Policy Panel. For more details on the Panel's work, visit theiet.org/engineering-safety.

The Institution of Engineering and Technology (IET) is working to engineer a better world. We inspire, inform and influence the global engineering community, supporting technology innovation to meet the needs of society. The Institution of Engineering and Technology is registered as a Charity in England and Wales (No. 211014) and Scotland (No. SC038698). Futures Place, Kings Way, Stevenage, Hertfordshire, SG1 2UA, United Kingdom.

E6D22001/Engineering Safety/0722