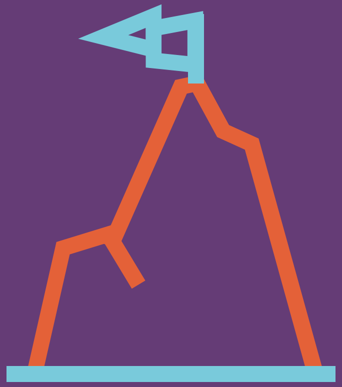
Bluefruit®
Software

Why is psychological safety critical to managing software risk?

By Emily King

Contents: Why is psychological safety critical to managing software risk?



Introduction

Is traditional risk management enough?

What does it *really* take to prevent hazards and harms from embedded devices and systems?

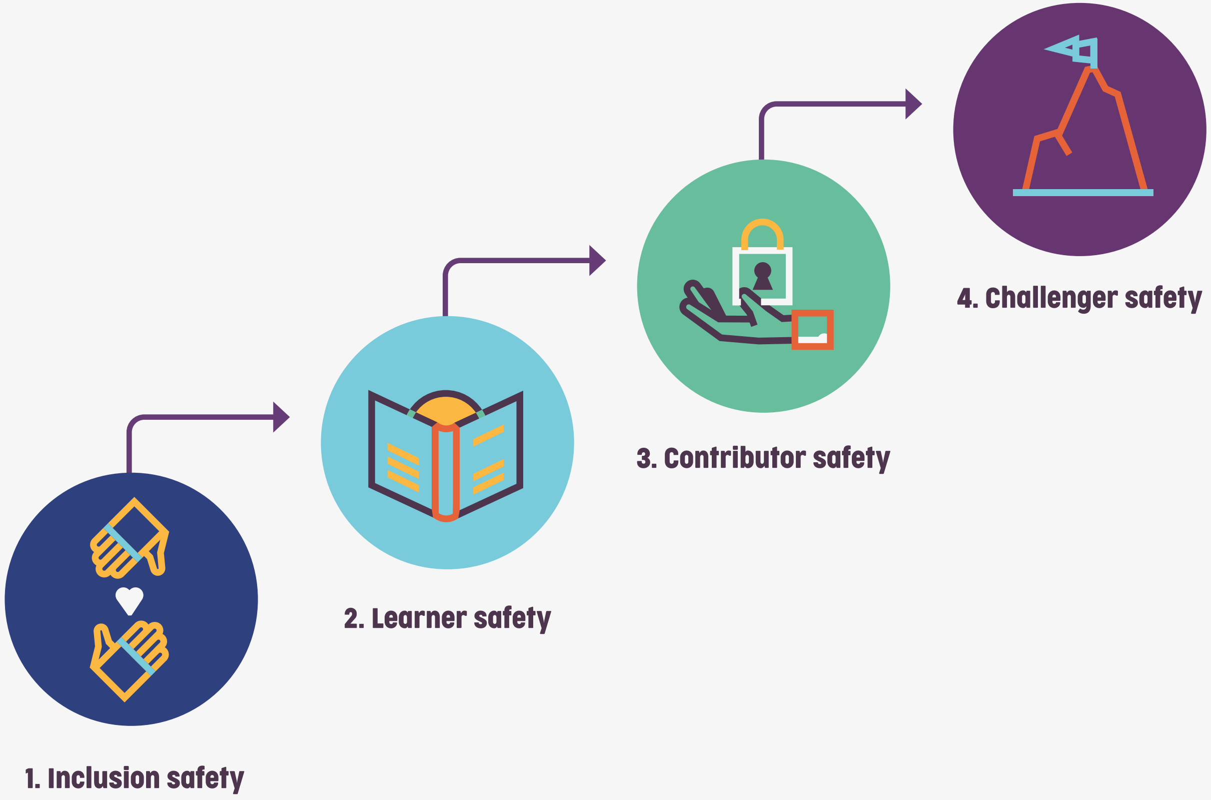
Is the use of traditional risk management, from risk management matrices to Failure Modes and Effects Analysis (FMEA) and similar, enough to prevent harmful outcomes?

Will your Quality Management System (QMS) have your project's back when something unpredicted happens?

In the coming pages, you'll find out that traditional risk management isn't enough. And that there's one tool missing from many software development and product teams' toolboxes:

Psychological safety.

Source: Based on The 4 Stages of Psychological Safety by Timothy R. Clark [1, p. xiii].



Risk isn't just for compliance-heavy sectors

It's understandable that the medtech, aerospace, and automotive sectors face a wall of standards when it comes to getting their products in front of customers. The stakes are far higher: from loss of life to the cost of wasted R&D investment because a product just isn't safe enough to remain on the market or even get there in the first place.

And yet the problem with many traditional ways of handling risk, from risk registers or FMEA, to QMS or following an ISO relevant to your product, are that:

- They're tick box orientated.
- They don't easily allow for uncertainty or handling unknown unknowns (the things you don't know, you don't know at project kick-off or after a product is in front of customers).
- They don't encourage people to speak up when it's needed, like when they discover an unknown unknown.

You could have a great suite of tools from process to QMS, project management, and documentation to help you handle risk. It'll mean nothing if people can't stand up and speak when something doesn't seem right.

Later, we'll be looking at case studies involving:

- The startup that failed: Theranos, and
- Aerospace titan, Boeing

As examples of where going beyond tick boxes, and where using psychological safety would have helped manage risk and potentially prevent some big hazards and harms.

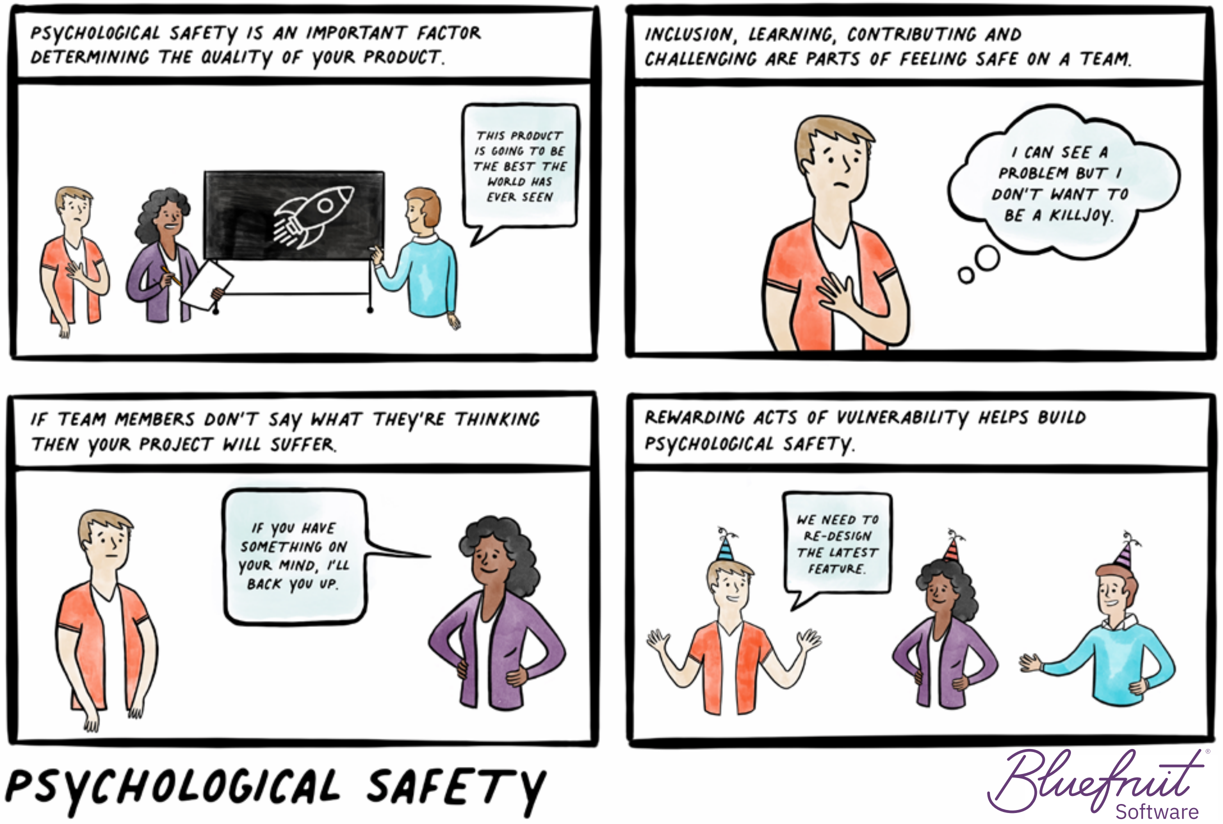
But first.

1 What is psychological safety?

William Kahn, of Boston University, first coined the term "psychological safety" in a 1990 journal article about employee engagement and disengagement in the workplace [2, p. 708].

In 1999, Amy Edmondson of the Harvard Business School wrote an article that further grounded the concept and later went on to describe it as:

"Psychological safety means an absence of interpersonal fear. When psychological safety is present, people are able to speak up with work-relevant content [3]."


PSYCHOLOGICAL SAFETY IS AN IMPORTANT FACTOR DETERMINING THE QUALITY OF YOUR PRODUCT.
THIS PRODUCT IS GOING TO BE THE BEST THE WORLD HAS EVER SEEN
INCLUSION, LEARNING, CONTRIBUTING AND CHALLENGING ARE PARTS OF FEELING SAFE ON A TEAM.
I CAN SEE A PROBLEM BUT I DON'T WANT TO BE A KILLJOY.
IF TEAM MEMBERS DON'T SAY WHAT THEY'RE THINKING THEN YOUR PROJECT WILL SUFFER.
IF YOU HAVE SOMETHING ON YOUR MIND, I'LL BACK YOU UP.
REWARDING ACTS OF VULNERABILITY HELPS BUILD PSYCHOLOGICAL SAFETY.
WE NEED TO RE-DESIGN THE LATEST FEATURE.
PSYCHOLOGICAL SAFETY
Bluefruit Software

1

But the definition we're most concerned with is provided by Timothy R. Clark. Clark said:

> **"Psychological safety is a condition in which you feel (1) included, (2) safe to learn, (3) safe to contribute, and (4) safe to challenge the status quo–all without fear of being embarrassed, marginalized, or punished in some way [1, p. 2]."**

It's these, as Clark describes them, four stages of psychological safety that have the most to offer to any organisation concerned with risk but also innovation.

1 Full psychological safety is the goal

When you think of psychological safety as a series of stages, you start to realise you can't have a later stage without the ones that precede it.

As a leader:	
Inclusion safety	You need to help individuals and teams feel included but encourage them to do the same with each other and the wider business [1, p. 39].
Learner safety	You need to create an environment that encourages learning, acceptance of failure, the exchange of knowledge, and to give people the time and space to learn [1, p. 62].
Contributor safety	You need to enable people to bring their ideas to the table and if they are showing competence and ability to deliver, give them the means and space to work without fear of micromanagement [1, p. 92].
Challenger safety	You need to make it acceptable for people to say what they see, but you also need to "protect the team's right to speak up" when someone tries to stop them [1, p. 121].

1 The complete stages of psychological safety

Here's how Clark sees the four stages.

Stage	Definition of respect	Definition of permission	Social exchange
Inclusion safety	Respect for the individual's humanity	Permission for the individual to interact with you as a human being	Inclusion in exchange for human status and absence of harm
Learner safety	Respect for the individual's innate need to learn and grow	Permission for the individual to engage in all aspects of learning process	Encouragement in exchange for engagement
Contributor safety	Respect for the individual's ability to create value	Permission for the individual to work with independence and their own judgement	Autonomy with guidance in exchange for results
Challenger safety	Respect for the individual's ability to innovate	Permission for the individual to challenge the status quo in good faith	Cover in exchange for candour

Challenger safety is key to the reporting of hazards and harms that will increase risk if unaddressed.
Meanwhile, **contributor safety** is what will help push teams and organisations further and help them innovate.
Source: Based on The 4 Stages of Psychological Safety by Timothy R. Clark [1, p. 103].

2 The benefits of psychological safety: Discretionary effort

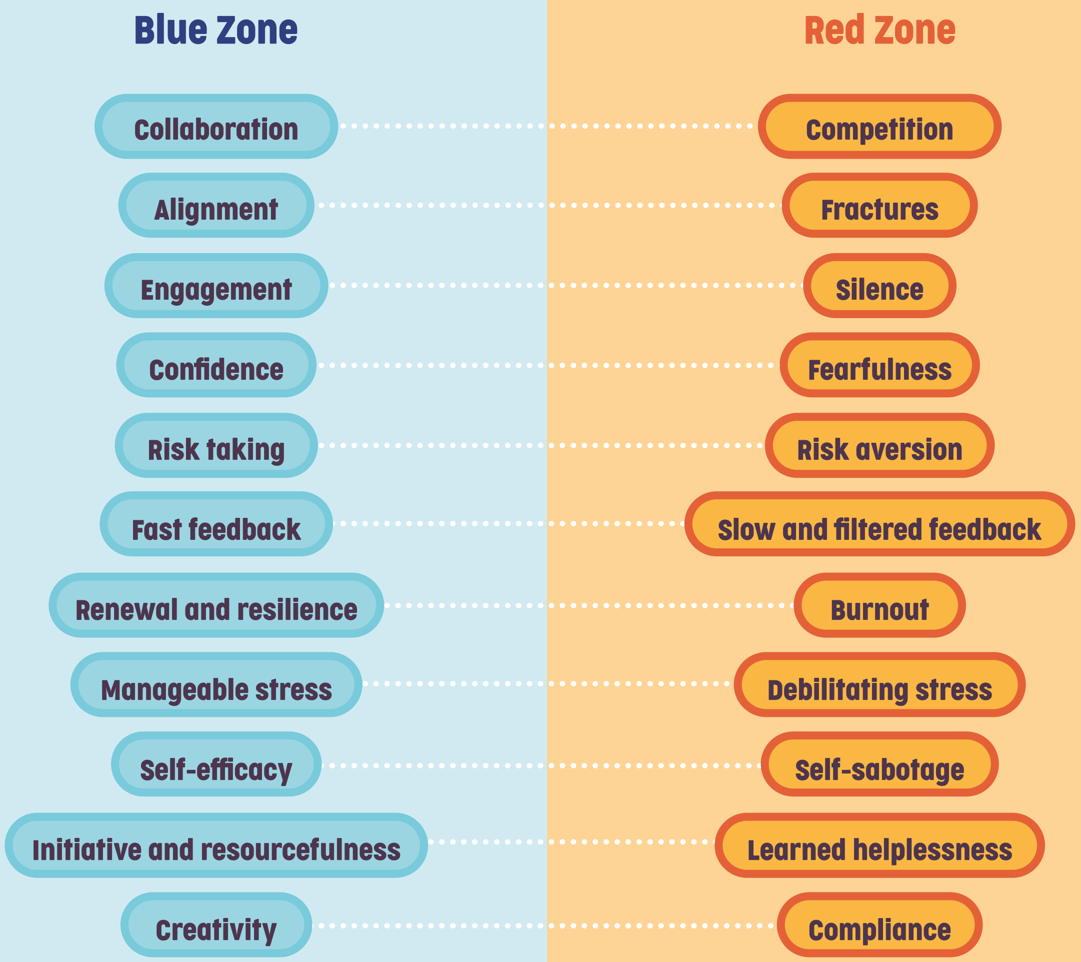
Challenger safety, as part of psychological safety, is certainly desirable in helping to ensure that people speak up about safety-critical issues during development. Enabling this can help reduce risk.

But contributor safety brings a host of benefits as well. Clark sees it as the difference between giving or withholding discretionary effort (where colleagues go beyond just delivering the bare minimum in their roles). He pictures this as the blue zone and the red zone [1, p. 78].

In the blue zone contributor safety is present, in the red zone it is absent.

In the blue zone, performance is higher, quality improves; ideas happen.

In the red zone, performance suffers, there's no collaboration, and people don't take any chances.



Blue Zone	Red Zone
Collaboration	Competition
Alignment	Fractures
Engagement	Silence
Confidence	Fearfulness
Risk taking	Risk aversion
Fast feedback	Slow and filtered feedback
Renewal and resilience	Burnout
Manageable stress	Debilitating stress
Self-efficacy	Self-sabotage
Initiative and resourcefulness	Learned helplessness
Creativity	Compliance

Source: Based on The 4 Stages of Psychological Safety by Timothy R. Clark [1, p. 78].

2 Discretionary effort

Where do you put your effort? Where's your attention spent?

When it comes to following standards and regulations, processes, and psychological safety, where does your organisation currently spend the most effort?

Are you in or out of balance?

The balance between standards and regulations, processes, and psychological safety

Many of us will be a part of organisations that are balanced against psychological safety. From leadership styles that push command and control to a belief that planning processes can uncover everything, and anything in between.

What we all need is for there to be balance, so that we can reap the benefits of teams that feel safe and are fully engaged.

Psychological safety
Processes
Standards and regulations

Psychological safety
Processes
Standards and regulations

Lessons from industry

The following pages look at two case studies from a failed startup (Theranos) and an industry giant (Boeing).

Each case study looks at risk situations created by hazards and harms that were not managed. And each case study considers whether psychological safety could have helped.

What we hope you'll see after reading these is that:
Psychological safety is not a nice to have. It's a must have.

3 Lessons from industry: Theranos

Employees silenced when risks identified

Former Silicon Valley darling Theranos, appeared to be on the fast track to becoming a new medtech gem in the early 2010s. With venture funding coming in and big names joining its board [4], it seemed like the blood-testing startup, founded by Stanford dropout Elizabeth Holmes, could do no wrong.

Inside this growing startup it was a different picture.

Fired and fed up

As far back as 2006, there were concerns as to the efficacy of the system that was being developed. Henry Mosley, CFO (at the time), tried to confront founder Elizabeth Holmes about Theranos 1.0 when he learned that the device didn't work anywhere near as well as they were telling investors.

When Mosley tried to talk to Holmes about the issue and tell her that they couldn't keep "fooling investors", Holmes response was to fire her CFO on the spot [5, pp. 3-8].

That was 2006. Over the course of the startup's existence, before it was finally wound up, numerous people working within Theranos would find themselves in a similar situation to that of Mosley after confronting Holmes. And if they weren't fired, they left when their doubts became too strong and without feeling empowered enough to speak up.

3 Theranos

What happened next?

Elizabeth Holmes's idea for a blood-testing device never reached the level of reliability or accuracy to make the product viable or safe for commercial use.

It took nearly ten years from Mosley's departure for Theranos to be held accountable in the public sphere. From journal articles to newspaper coverage, FDA pressure, investors and buyers dropping out, lawsuits—the startup started to unravel.

Investors in the startup lost over $600 million with the company's demise in 2018 [6].

In January 2022, a jury found Holmes guilty on multiple counts of fraud; sentencing is due in September 2022 [7].

Would psychological safety have helped?

There is no doubt that psychological safety could have helped prevent or lessen the fallout from Theranos.

With no one in the startup able to push past the command-and-control nature of Holmes's leadership and those who mimicked it within the business, opportunities were missed everywhere.

From the chance to improve the design of the device and the development to make it work, to cut risks to patients and investors, or to find opportunities to successfully pivot beyond the original idea and deliver a working product and return on investment—psychological safety could have helped.

3 Lessons from industry: Boeing

A culture of quality and safety lost

For decades, Boeing had been seen as a stalwart of aircraft quality and safety. A workplace that listened to its engineers rather than Wall Street, while it designed and built some of the world’s most well-known airplanes.

But that began to change after its merger with McDonnell Douglas in 1997.

Fighting off Airbus

Over the course of the 1980s and 1990s, Boeing began to lose market share to European competitor Airbus. Ongoing changes at the top of Boeing’s leadership after its merger with McDonnell Douglas, alongside a desire for the commercial-aircraft side of the business to be as successful as its defence side, saw a steady erosion of the quality and safety culture on which Boeing had once prided itself.

In the 2010s, as it lost more market share to Airbus, Boeing was keen to find a successor to the 737 lines that had sold so well in the 1990s.

3 Boeing

What happened next?

In 2011, Boeing proposed a new version of the 737 that would come to be known as the 737 MAX 8 [8, p. 112].

Much of its design was done in a way that meant it wouldn't have to go through full certification again, or require pilots to retrain [8, pp. 136-138]. But this all created a problem. The MAX's new fuel-efficient engines meant the plane could pitch up dangerously [8, p. 139].

Rather than spend money on a hardware solution, Boeing opted for a cheaper software fix that relied on existing sensors. Dubbed the "Maneuvering Characteristics Augmentation System" or MCAS, the software would pitch the plane downwards if it felt it pitching up too much, too suddenly. It was treated as a "program directive" to avoid recertification issues [8, pp. 139-140].

Engineers warned about the safety of the 737 MAX 8. Managers rejected calls to put in "safety enhancements" that would have added fallbacks to the MCAS [8, p. 141].

Other safety measures for different parts of the plane were called for and rejected, again and again. The plane eventually went into production, no mention of MCAS was explicitly made in the MAX's user manuals.

On the morning of October 29, 2018, Lion Air Flight 610 boarded in Jakarta. At 6:32 am, 12 minutes after take-off, all 189 lives on board were lost as the jet crashed into at the sea at 500 mph [8, pp. 3-4]. Five months later, another crash happened. In the early hours of March 10, 2019, Ethiopian Airlines Flight 302 crashed 6 minutes after take-off from Addis Ababa, killing all 157 on board [8, p. 6].

In both cases, the MCAS was responsible for incorrectly assuming, based on false angle-of-attack readings, that the planes were pitching upwards when they were not. While Flight 610 did not have the benefit of knowing about MCAS and a checklist that was subsequently released, Flight 302 did.

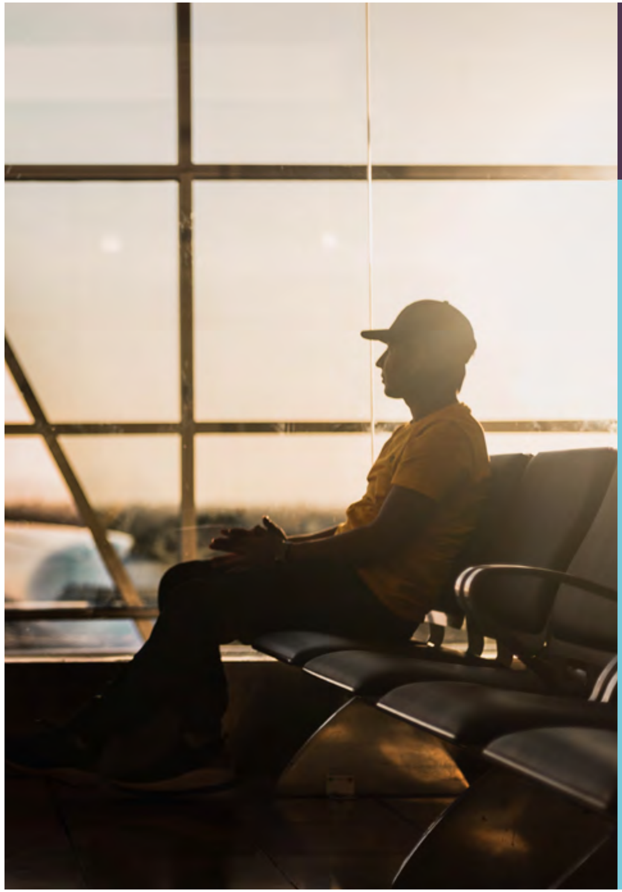
But the checklist did not help prevent the second crash as, to counteract, MCAS pilots only had seconds to address something that required a high level of recall [8, p. 182].

3 Boeing

Both flights had the actions of pilots overridden by software, causing deadly consequences.
It took the second crash for aviation authorities worldwide to ground 737 MAX 8s.

The US House Committee on Transportation & Infrastructure began an investigation into the 737 MAX 8 crashes in May 2019. Its hearings included testimony from witnesses across Boeing and the aviation sector, as well as the Federal Aviation Authority (FAA) [9].

Dennis A. Muilenburg who was the CEO of Boeing during much of the 737 MAX 8's formative years, was fired at the end of 2019 [10]. In January 2021, Boeing was charged with fraud conspiracy by the US Department of Justice and Boeing agreed to pay over $2.5 billion in reparation for the fraud [11].



Would psychological safety have helped?

While the decreasing oversight of the FAA played a role in these tragedies [8, p. 126], it is clear that the culture change at Boeing after its 1997 merger with McDonald Douglas ruined what psychological safety had been present in the business.

With challenger safety no longer supported at the organisation by 2014, hundreds of lives were subsequently lost in the pursuit of ever-growing efficiencies and profits.

4 Lean-Agile practices and techniques that work well with psychological safety

Lean-Agile is based on principles and practices from Lean and Agile software development. It asks for teams and organisations to have openness and empowerment. These are all key components of the four stages of psychological safety.

Lean software development asks, within its seven principles, that you “empower the team” and “amplify learning” [12, pp. xxv-xxviii]. Meanwhile, the Agile Manifesto proclaims:

Individuals and interactions over processes and tools

Working software over comprehensive documentation

Customer collaboration over contract negotiation

Responding to change over following a plan

That is, while there is value in the items on the right, we value the items on the left more [13].

4 What is Lean-Agile?

Clearly, ensuring psychological safety is a massive benefit to Agile and Lean-Agile teams.

While not a panacea to the challenges described in the earlier case studies, the following practices can help teams regardless of whether they're Agile or not. They also work at their best when there's psychological safety present.

Principles

Lean-Agile principles put adaptation over prediction and have seven core ideas, such as eliminating waste, amplifying learning, empowering the team, and more. Borrows from Lean software.

Project management practices

Sprints, retrospectives, points, user stories, and so on. Often other businesses who see themselves as Agile are already focused on these practices and are using them.

Technical practices

Frequent/continuous integration, TDD, BDD, and so on. These processes are highly centred on achieving quality in software and are focused on ensuring effective software development.

Lean-Agile is a hybrid between Lean principles and Agile practices.

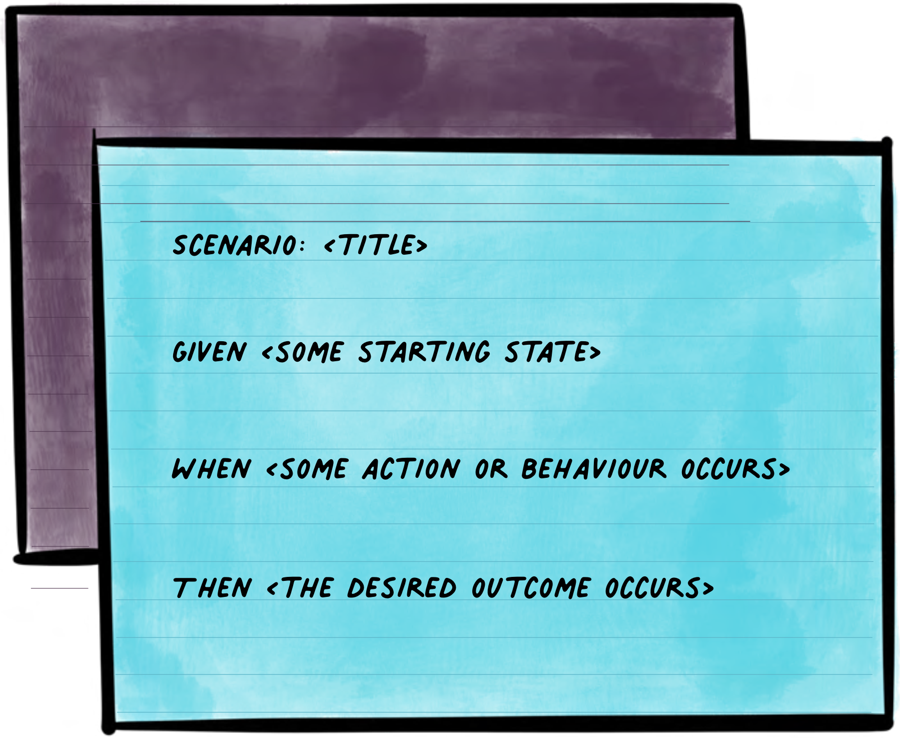
4 Three Lean-Agile practices that pair well with psychological safety: Behaviour-Driven Development (BDD)

What is it?

BDD involves writing tests that test the behaviour of software. It seeks to analyse how user journeys affect software behaviour. These tests are written in a human-readable format (no code).

Why is it useful?

It helps boost communication across stakeholders and the development teams. How? By encouraging them to collaboratively discuss the system's required behaviours and write the BDD tests together and in a format and language everyone can understand. Also, as part of those conversations, questions will come up, which will help all those involved clarify what is expected of the software.



```
SCENARIO: <TITLE>

GIVEN <SOME STARTING STATE>

WHEN <SOME ACTION OR BEHAVIOUR OCCURS>

THEN <THE DESIRED OUTCOME OCCURS>
```

4 Behaviour-Driven Development (BDD)

It’s also possible to use BDD tests as requirements, which is helpful for projects where traceability between tests and requirements are important. It can benefit medtech projects needing to fulfil IEC 62304, for instance.

BDD complements Test-Driven Development (TDD), which looks at technical function rather than behaviour.

For more information on BDD, read this blog post on BDD and Gherkin (a popular way of writing features in BDD).

How does BDD help?

Symptom:
Difficult to test your software and ensure tests are linked to requirements.

Cause:
Testers weren’t given a voice early in the process (contributor safety affected).

Solution:
BDD ensures testability is built into requirements and the software.

4 Retrospectives

What are they?

Not to be confused with reviews, retrospectives can either look at how features have been delivered during a set space of time (a sprint or a project), or they can be used to troubleshoot. Retrospectives come in many different shapes and forms, some more suited to general project work and some more suited to troubleshooting.

Why are they useful?

Retrospectives are incredibly good at bubbling problems to the surface mid-project or helping you uncover the cause of a problem. When done as part of frequent iterations, retrospectives can help teams and stakeholders communicate and work towards ways to fix any problems that surface.
Formats like a sailboat retrospective enable teams to look at the good and the bad of a sprint and identify future risks. Whereas a Five Whys would help you answer any hard questions and get to the root cause of any problem, regardless of whether it's identified during a retrospective or mid sprint.

In fact, if you only ever had retrospectives available in one format, make sure it's Five Whys. **See the next page for an example of Five Whys.**

For more information, check out this blog post on retrospectives for ideas on formats and how to run them.

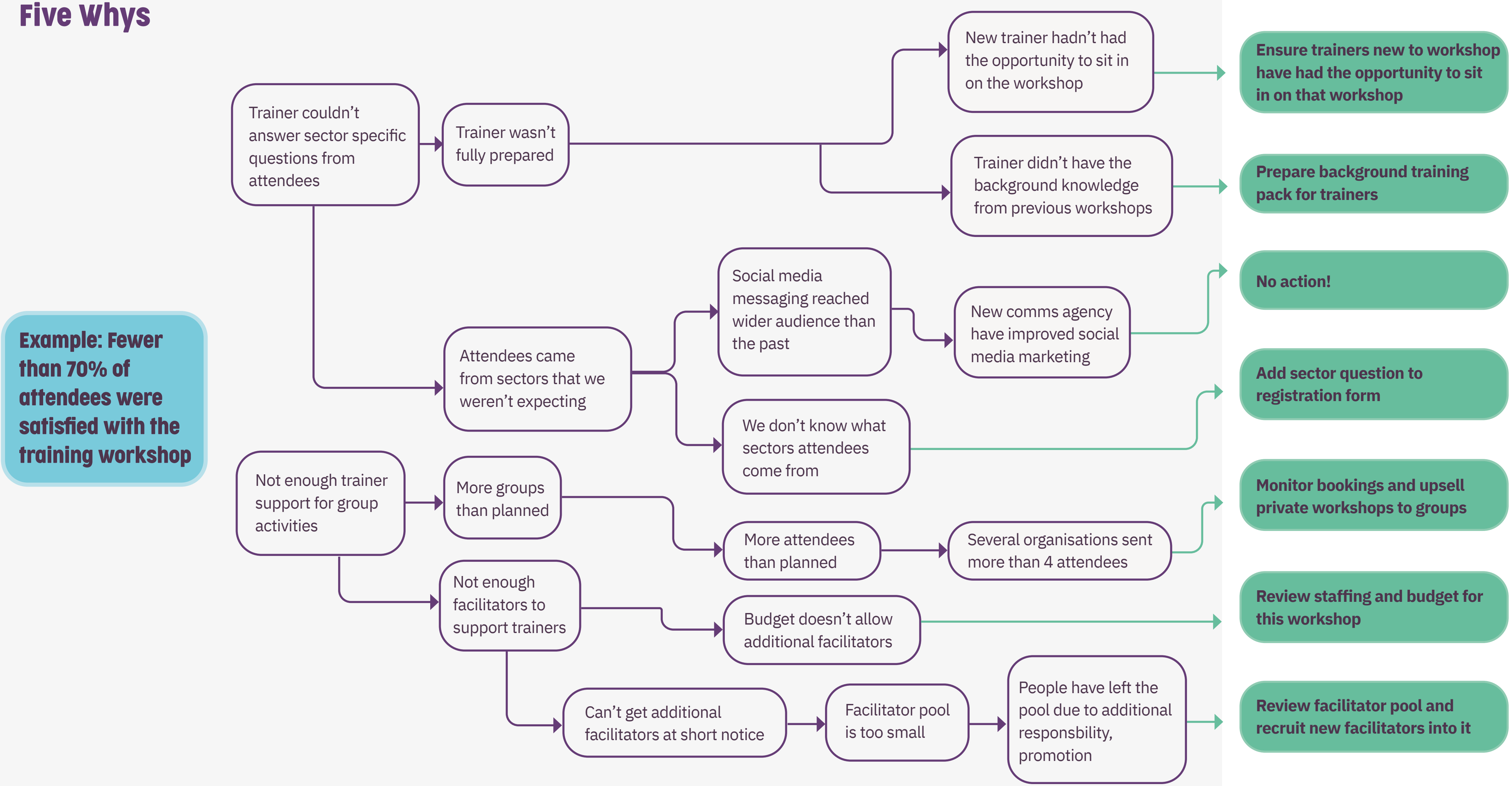
Retros

Symptoms:
Same problems keep recurring.

Cause:
Unempowered team members know of a problem but aren't speaking up (inclusion safety affected).

Solution:
Ensure everyone has an opportunity to contribute and that there are actions coming from all team members.

Five Whys



Example: Fewer than 70% of attendees were satisfied with the training workshop

Trainer couldn't answer sector specific questions from attendees

Trainer wasn't fully prepared

New trainer hadn't had the opportunity to sit in on the workshop

Ensure trainers new to workshop have had the opportunity to sit in on that workshop

Trainer didn't have the background knowledge from previous workshops

Prepare background training pack for trainers

Attendees came from sectors that we weren't expecting

Social media messaging reached wider audience than the past

New comms agency have improved social media marketing

No action!

We don't know what sectors attendees come from

Add sector question to registration form

Not enough trainer support for group activities

More groups than planned

More attendees than planned

Several organisations sent more than 4 attendees

Monitor bookings and upsell private workshops to groups

Not enough facilitators to support trainers

Budget doesn't allow additional facilitators

Review staffing and budget for this workshop

Can't get additional facilitators at short notice

Facilitator pool is too small

People have left the pool due to additional responsbility, promotion

Review facilitator pool and recruit new facilitators into it

4 User story mapping

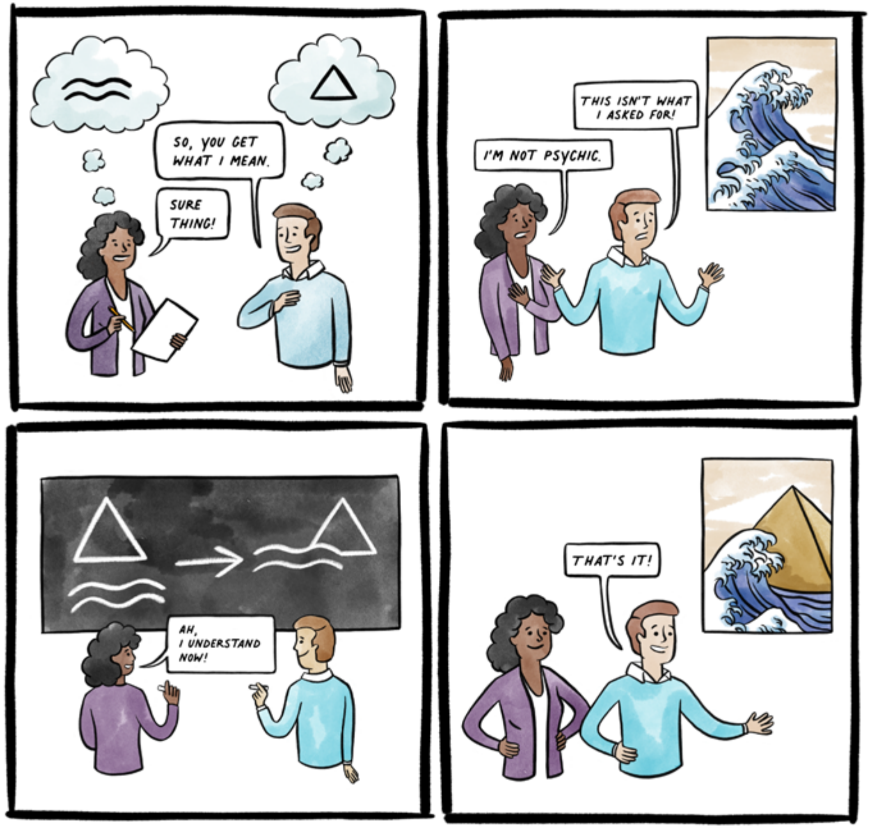
What is it?

User story mapping is a process where product and software teams, and stakeholders, tell stories (have conversations) about your product so that you can gain “shared understanding” and discuss how you get to where you want to be [14, p. xxi].

Why is it useful?

User story mapping can help all involved build an understanding that ensures teams build the right thing, for the right people, for the right reasons. It also ensures that everyone is on the same page about this.

It is, at its core, a fantastic communication tool to understand users, what they’re doing, what’s involved in these activities from a user and product perspective, and how everything links to desired user and business outcomes.



SHARED UNDERSTANDING

Bluefruit Software

4 User story mapping

By focusing on communication and building what's valuable and needed, user story mapping can help teams cut back on waste while adding value to a project.

[If you want to give it a go, try our free template on Miro.](#)

[And for a more in-depth exploration, read this blog post on how to use user story mapping.](#)

How does user story mapping help?

Symptoms:
Deadlines are frequently missed.

Cause:
You have a single fixed scope Minimum Viable Product (MVP) with a single fixed deadline, therefore "failure is not an option" (challenger safety impacted).

Solution:
A story map gives you alternative coherent release candidates that make it safe for colleagues to flag when the original scope is going to cause missed deadlines, from all team members.

Find out more

Do you have a project you need help with? Our software and hardware experts can tell you all you need to know.

Email us at hello@bluefruit.co.uk.

We're also happy to speak on the phone during office hours (9 am to 5 pm GMT, Monday to Friday). Call us on +44 (0) 808 18 000 55 (FREEPHONE) or +44 (0) 333 577 7111.

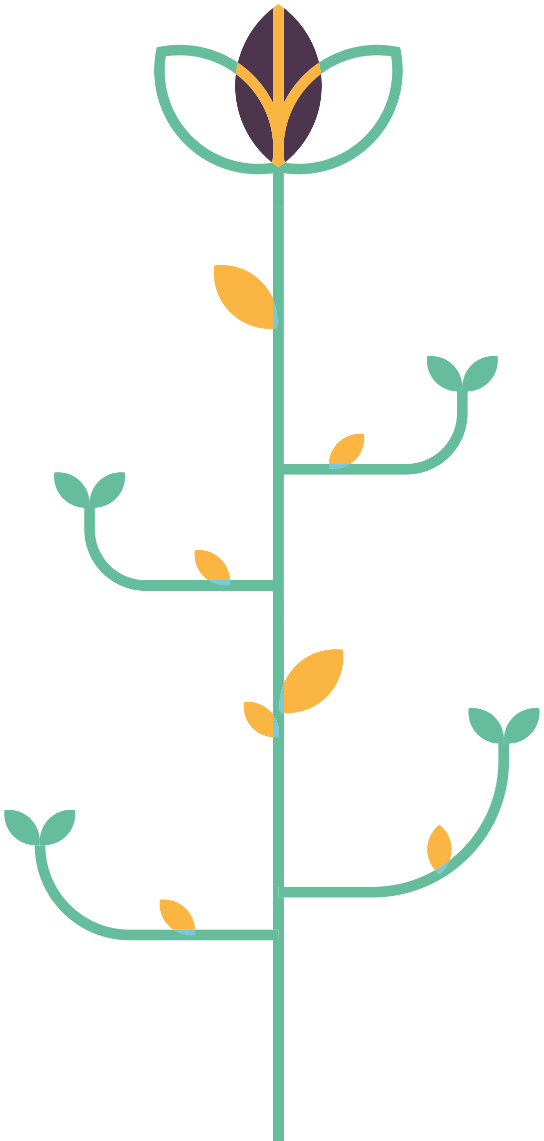
About Bluefruit Software

For over 20 years, Bluefruit has provided clients across safety-critical sectors with high-quality software and insights for their products.

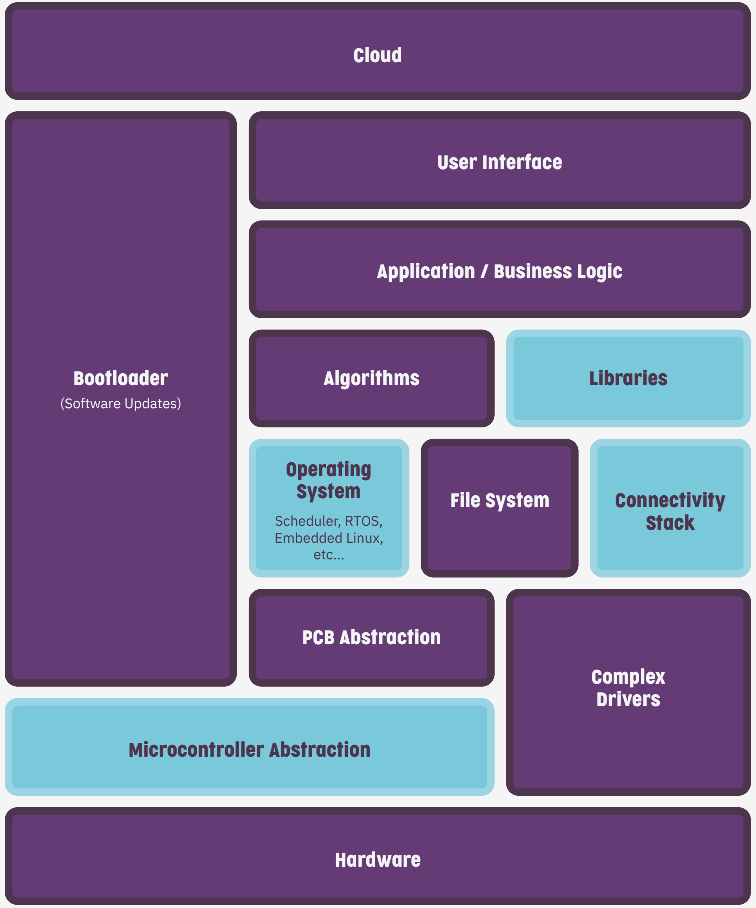
Our other services include:

- Consulting
- Help with compliance
- Software development, from firmware to user interfaces and applications
- Software testing (including Verification and Validation)
- UX design and development
- Hardware design services
- Lean-Agile training, and more.

Our software teams work alongside your in-house teams and existing outsourcers to help you achieve the best-in-class outcomes your medical device needs.



Where does Bluefruit Software fit in embedded development?



Key:

- 🟦 Usually off-the-shelf, but we can/do write
- 🟪 Standard services offered by Bluefruit

References

[1] T. R. Clark, The 4 Stages of Psychological Safety: Defining the Path to Inclusion and Innovation, Oakland: Berrett-Koehler Publishers, Inc., 2020.

[2] W. A. Kahn, "Psychological Conditions of Personal Engagement and Disengagement at Work," Academy of Management Journal, vol. 33, no. 4, pp. 692-724, 1990.

[3] McKinsey & Company, "Psychological safety, emotional intelligence, and leadership in a time of flux," mckinsey.com, 2 July 2020. [Online]. Available: https://www.mckinsey.com/featured-insights/leadership/psychological-safety-emotional-intelligence-and-leadership-in-a-time-of-flux. [Accessed 16 August 2022].

[4] The Straits Times, "A timeline of the rise and fall of Theranos founder Elizabeth Holmes," straitstimes.com, 9 January 2022. [Online]. Available: https://www.straitstimes.com/world/united-states/a-timeline-of-the-rise-and-fall-of-theranos-founder-elizabeth-holmes. [Accessed 17 August 2022].

[5] J. Carreyrou, Bad Blood: Secrets and Lines in a Silicon Valley Startup, London: Picador, 2019.

[6] J. Carreyrou, "Theranos Cost Business and Government Leaders More Than $600 Million," wsj.com, 3 May 2018. [Online]. Available: https://www.wsj.com/articles/theranos-cost-business-and-government-leaders-more-than-600-million-1525392082. [Accessed 2022 August 2018].

[7] BBC News, "Elizabeth Holmes: Theranos founder convicted of fraud," bbc.com, 4 January 2022. [Online]. Available: https://www.bbc.com/news/world-us-canada-59734254. [Accessed 17 August 2022].

[8] P. Robinson, Flying Blind: The 737 MAX Tragedy and the Fall of Boeing, Dublin: Penguin Business, 2021.

[9] The House Committee on Transportation & Infrastructure, "Boeing 737 MAX Investigation," transportation.house.gov, 2021. [Online]. Available: https://transportation.house.gov/committee-activity/boeing-737-max-investigation. [Accessed 19 August 2022].

References (continued)

[10] L. Josephs and A. Lucas, “Boeing fires CEO Dennis Muilenburg, as the company struggles with 737 Max crisis,” cnbc.com, 23 December 2019. [Online]. Available: https://www.cnbc.com/2019/12/23/boeing-stock-halted-pending-news-company-battles-fallout-737-max-crisis.html. [Accessed 19 August 2022].

[11] Department of Justice - Office of Corporate Affairs, “Boeing Charged with 737 Max Fraud Conspiracy and Agrees to Pay over $2.5 Billion,” justice.gov, 7 January 2021. [Online]. Available: https://www.justice.gov/opa/pr/boeing-charged-737-max-fraud-conspiracy-and-agrees-pay-over-25-billion. [Accessed 19 August 2022].

[12] M. Poppendieck and T. Poppendieck, Lean Software Development: An Agile Toolkit, Crawfordsville: Addison Wesley, 2003.

[13] M. Beedle, A. van Bennekum, A. Cockburn, W. Cunningham, M. Fowler, J. Highsmith, A. Hunt, R. Jeffries, J. Kern, B. Marick, R. C. Martin, K. Schwaber, J. Sutherland and D. Thomas, “Manifesto for Agile Software Development,” agilemanifesto, 2001. [Online]. Available: https://agilemanifesto.org/. [Accessed 18 August 2022].

[14] J. Patton and P. Economy, User Story Mapping: Discover the Whole Story, Build the Right Product, Sebastopol: O’Reilly Media, Inc., 2014.

Bluefruit Software

Bluefruit Software
Gateway Business Centre
Barncoose Gateway Park
Redruth
Cornwall,
United Kingdom TR15 3RQ
+44 (0) 808 18 000 55 (FREEPHONE)
+44 (0) 333 577 7111

www.bluefruit.co.uk
hello@bluefruit.co.uk