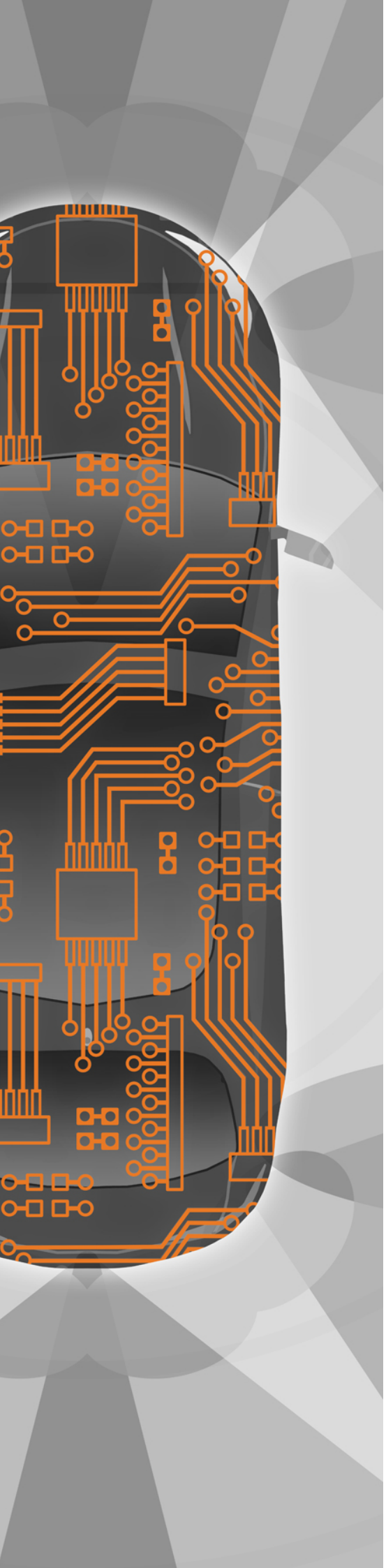

FUNCTIONAL SAFETY &
QUALITY EXPERTS GmbH

EchoScrum®

Version: 4.0

Datum: 26.10.20

FSQ Functional Safety & Quality Experts GmbH | Balanstrasse 14, 81669 Muenchen

Managing Directors Wolfgang Mickisch, Matthias Größler | @ contact@fsq-experts.com |

www.fsq-experts.com

Contents

1. EchoScrum® in a Nutshell

Throughout the automotive E/E-development community as the technological change from combustion engine to E-Mobility, and from traditional driver driven to highly automated vehicles continues, the need to render highly flexible and fast development processes increases, especially in their early phases. OEMs and Tier-1s require a thorough validation of their innovative products as early as possible in order to be able to identify false decisions and necessary changes in requirements, architecture, etc. speedily and reduce the risk of costly late changes.

This is the reason why, in the field of Automated Driving Development based on the scrum model or large-scale scrum models like LeSS® or SAFe®, Agile Development has widely been introduced. Unfortunately, however, regardless of the model followed, companies find it difficult, if not impossible to get the first Minimal Viable Product (MVP) not only functioning, but also safe and compliant to ISO 26262. Instead, discrepancies and widening gaps between the two development domains -- feature and safety -- are constantly seen, as if there were a law of nature behind it. After a delay of some, or even many, months, feature and safety development must then be adjusted and corrected ex post facto at considerable efforts, which often outweigh the savings in time and costs one had hoped to achieve with Agile Development.

EchoScrum® is the first agile development model specifically designed to systematically prevent such a fatal and costly course of events right from the beginning, and to ensure compliance with ISO 26262 as well as other relevant standards such as ISO 21434 (Cyber Security), ISO/PAS 21448 (SOTIF) and others with such a high degree of flexibility and efficiency as aimed for with agile development.

There are four fundamental rules are at the centre of this model:

1. The product is developed incrementally by iterating two distinct equally long sequential sprints inseparably tied together like a call and its echo in nature:
    a. the *feature-oriented Call Sprint*, where a functional feature is developed
    b. the subsequent *product safety-oriented Echo Sprint***,** where all product safety related aspects of the feature increment just implemented are being investigated and safety measures designed and developed.
2. *One single team* is developing both the feature (Call) and safety (Echo) results.
3. At the beginning of each Echo Sprint, depending on the project phase, *all applicable types of Safety and Security Analyses* (FMEA, FTA, FMEDA, DFA, Cyber Security etc) *are being performed incrementally in a holistic approach* as basis for an incrementally growing and validated safety plan and concept.
4. At the end of each Echo Sprint, checks of consistency, traceability and other standard compliance requirements, like confirmation reviews, are executed. In such a way, at each stage of the development *MVPs* and subsequent *product-increments that are compliant with the relevant standards are available*.

Following these four fundamental rules allows you to realize a closely connected incremental development of both; feature on the one hand, and product safety as well as cyber security on the other.

2. EchoScrum® Philosophy

To have a better understanding of the EchoScrum® concepts underlying those four rules, let us have a closer look at the root causes of the divergence of feature and safety development prevailing so often in industry with all of its disastrous consequences.

- The major factor is, that from the correct assessment, the two domains, feature and safety development, require two distinctly different engineering mindsets, the conclusion could be drawn that you therefore need two distinct development teams. This is not the case.

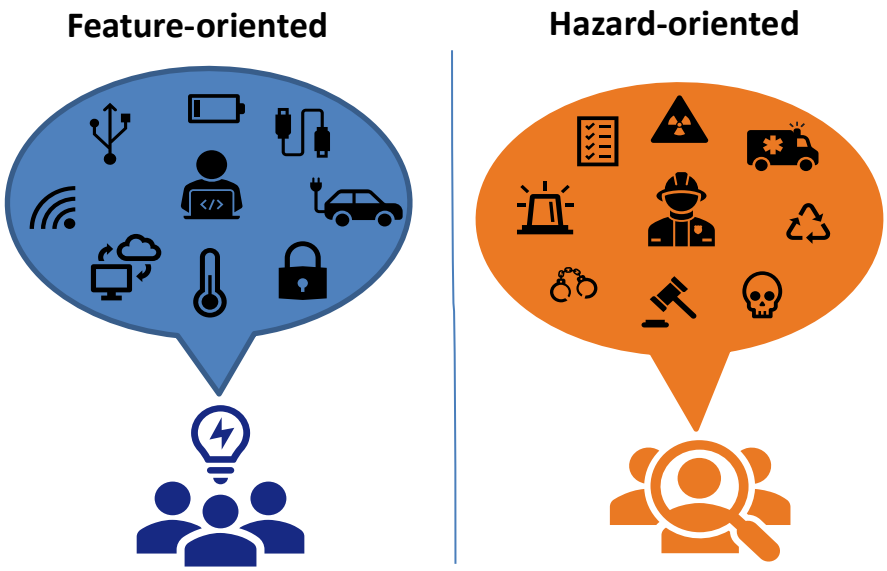

Figure 1 – Mindsets in many safety related development projects: Feature-oriented vs. Hazard-oriented

It is true that intelligent feature development requires openness towards new technological challenges, speedy thinking, and creativity with a certain readiness to strike new, unexplored paths.

It is also true that, in contrast, the identification of relevant hazards and the prevention of malfunctions, be it on system or be it on component level, demand conservative thoroughness and adherence to systematic approach in order to achieve the safety integrity level required.

Yet there is no compelling technical argument to go from this observation of two distinct engineering mindsets to establishing two distinct engineering teams, one for feature and one for safety development. Unfortunately, however, it is quite common in industry to proceed in such a way.

- Another reason for establishing a separate functional safety team is often based on the misguided assumption that costs could be saved by getting this team started some months later, after the first features have already been developed.

Compounding such a conception is a tendency at management level to prioritize feature development before safety – these results can be shown to higher managers or the customer sooner, and seem more tangible, than safety measures. Underlying such an approach is the false idea that functional safety is just another system feature that can be added anytime during an agile development.

For historical reasons, the traditional agile development models such as LeSS® or SAFe® do not focus on such ideas. They have been derived from studies in other branches of industry without safety relevant applications and thus from very different development cultures where the synchronous development of feature and safety is not required.

- Whatever the arguments or reasons given, once two distinct teams are working with a significant time-gap, and hence great difficulties in coordination, a growing technical divergence of both development streams seems unavoidable. It can only be healed with considerable efforts.

Compliance to relevant product safety standards such as ISO 26262 may be formally confirmed or even certified in the end. But that is often only achieved by developing safety work-products retrospectively instead of as essential requirements in parallel with feature development. The consequences are dire:

- Such post-factual safety work-products cannot serve as guidelines for the development as they are meant to do.
- Design will not be optimized for all requirements, whether they are safety or non-safety, in early phases.
- If late findings of the safety team require corrections in fundamental development work-products such as the software architecture, the consequences for the whole project may be far-reaching in terms of costs and efforts.

Based on the findings of practices in managing safety-related projects that are currently prevailing in industry, the following EchoScrum® principle has been derived as a solution:

The necessary switch between the feature mindset and the safety mindset for developing highly automated driving and other safety-related systems shall not be performed by a switch from one team to another, but within one and the same team. The EchoScrum® team has the competences for both, feature development and safety development, and is accountable for all call and all echo sprints.

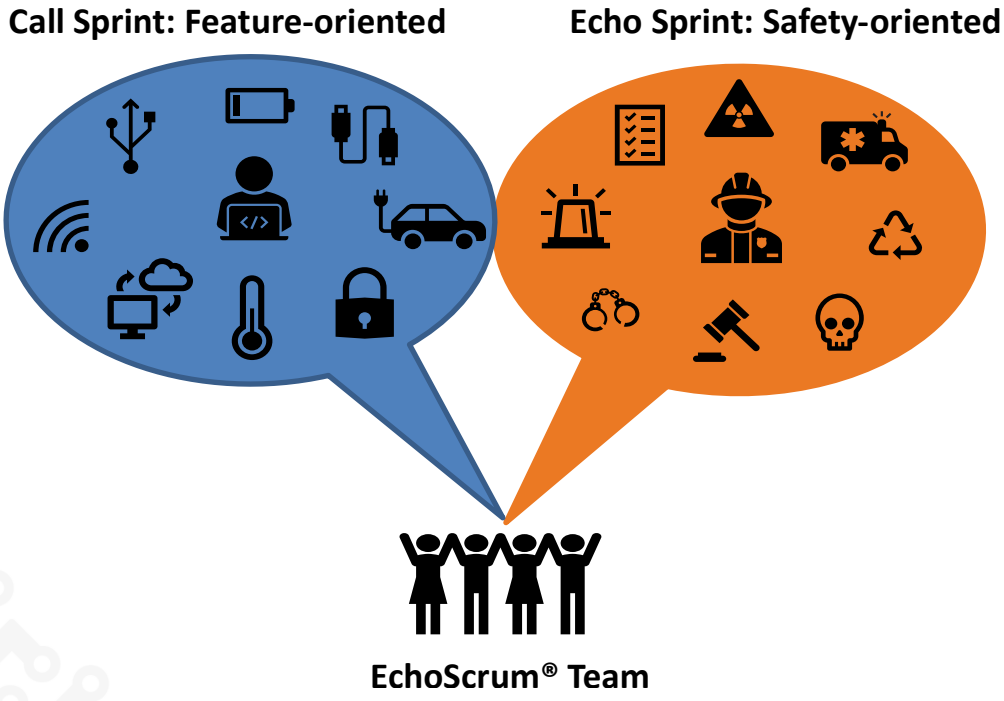

Figure 2 – EchoScrum®: unifying feature-oriented and safety-oriented development.

It follows, that the typical EchoScrum® team is comprised of development engineers with multifunctional competences; requirements engineers, architects, developers, and testers will all be on board. All of them are to be expected to think, manage and act consciously as safety engineers, even if for specialized activities, such as various types of safety analysis, external experts may be consulted. In this way, safety measures will be conceptualized based on a thorough knowledge of the technical features implemented, and vice versa, the feature will be developed based on a profound knowledge of the safety measures required.

3. EchoScrum® in Overview

From the EchoScrum® rules and principles described in Chapter 2, the following model can be drawn:

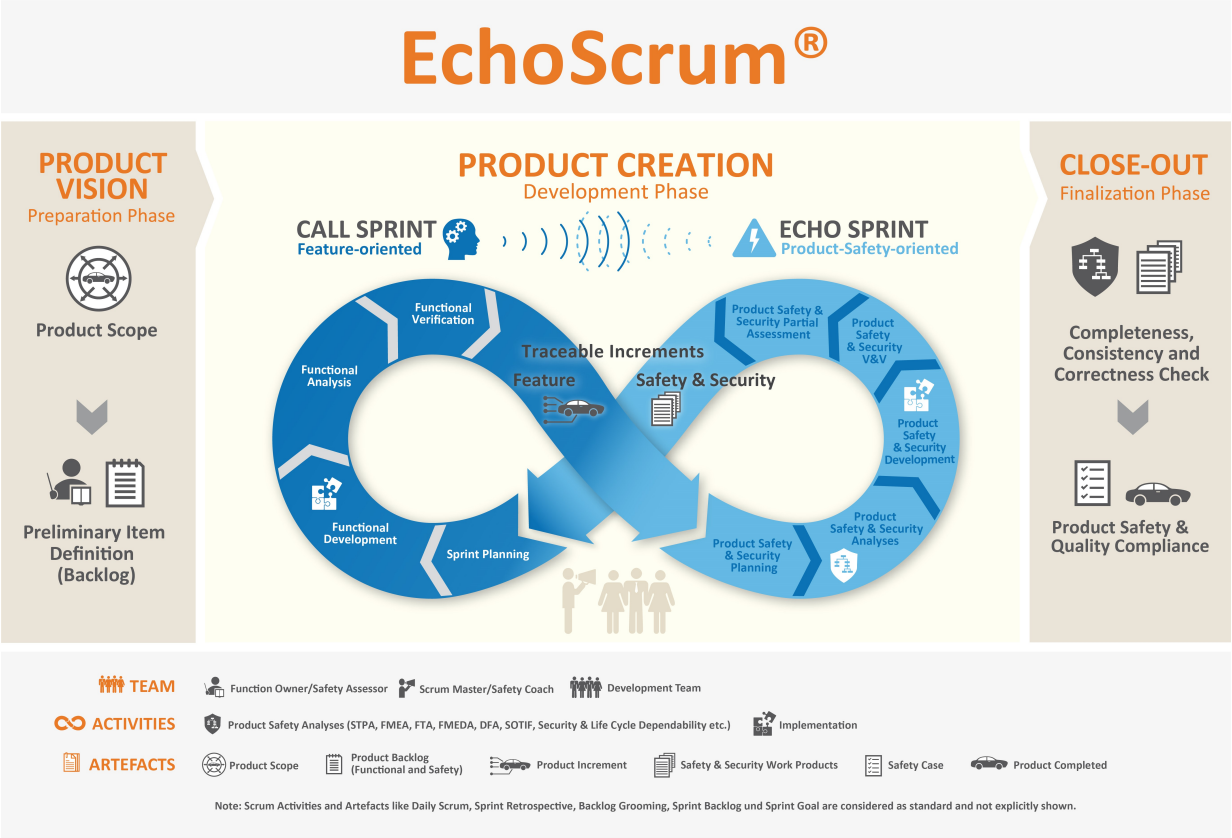

Figure 3 – EchoScrum® Landscape: Product Vision; Product Creation, Close-out Phase

From all activities in the echo sprint cycle, as displayed in Figure 3, attention is drawn to the block named Product Safety & Security Analyses. Here, FMEA, FTA, FMEDA, DFA are executed incrementally with a holistic approach. The same holds for activities safeguarding security (in co-ordination with functional safety) and all other aspects of product safety like SOTIF or life cycle reliability and dependability. System-theoretic process analysis (STPA) also may be docked on here.

Functional safety and other product safety, security and reliability work products are not created belatedly post-development just for documentation purposes, but to serve as guidelines for the subsequent development activities.

4. EchoScrum® Framework

EchoScrum® is derived from the scrum process framework, both share common aspects and principles such as team roles and responsibilities, scrum activities, and scrum artefacts. When applicable, we have redefined or extended the concepts for the EchoScrum® framework.

EchoScrum® specifics are defined in the following sub-chapters.

4.1. EchoScrum® Team

In the EchoScrum® framework, the product is always a safety related system, which generally requires cross-functional development activities for its realization. As discussed earlier, the EchoScrum® team will comprise experts with different areas of focus (requirements engineering, architecture, development, and testing). All of them will contribute during a whole sprint cycle, the couple of a call and an echo sprint. And they will be equally accountable for the sprint cycle results and the final product.

The roles in detail:

Product Owner – is responsible just as with the original scrum for managing the EchoScrum® product backlog and setting priorities. In the EchoScrum® framework there are additional types of product owner, for example, the roles of a **Safety Assessor**, or a **Quality Manager**.

Scrum Master – is responsible for promoting the values of scrum and supporting this way of working. This person acts as a communication channel for the stakeholders outside the EchoScrum® team.

Product Safety Coach – is responsible for coaching the team on how to apply product safety methods, analysis and techniques. This role can be merged with the Scrum Master role.

Development Team - multidisciplinary, cross-functional (including functional safety) and always accountable for the whole sprint cycle and its results.

Team Working Rules

- Team members commit to work in a self-organized way.
- The entire development relies on principles of transparency, mutual aid and knowledge transfer.
- The team remains unchanged during sprint cycles and executes both call and echo sprints. Specialists from other company divisions or from outside such as Safety Experts may be consulted if required.
- A sprint should not be interrupted, even if the purpose for the sprint has been changed.

Best practice

It is important that the team is large enough to cover the needed skills but not excessively large as to compromise team interactions and coordination. It is recommended to stick to a maximum of 10 team members. It must be avoided that sub-teams emerge and disrupt the working rules.

4.2. EchoScrum® Activities

The commitment to the activities described below enforces continuously improvement of the product, the team, and the working environment.

4.2.1. Overall

Sprint Cycle - defines one iteration of a sprint couple, call sprint (feature-oriented) and echo sprint (hazard- or safety oriented), each one of these lasts two weeks. Hence one sprint cycle lasts one month.

Increment – is the result of a sprint cycle where both feature implementation and safety requirements were addressed. The final product comprises all increments.

Sprint Review - the sprint results are inspected, and the product backlog refined to allow the preparation of the next sprint. In EchoScrum® there is a call-sprint review and an echo-sprint review.

4.2.2. Product Vision - Preparation Phase

For initiating the first EchoScrum® sprint cycle, it is recommended to execute a preparation phase. This is the product vision phase, where all information about the system is collected and the product backlog is created.

Typical activities that may take place in this phase are requirements elicitation and evaluation and the execution of a preliminary hazards and risk analysis. Additionally, as in any other scrum framework, it is important to evaluate the complexity of the increment to be developed. It may be necessary to break a feature down in smaller elements to ensure that the development matches the duration of the EchoScrum® sprint cycle (e.g. a total of four weeks with two weeks per sprint).

4.2.3. Call Sprint

The goal of the call sprint is to implement a minimum viable product (MVP) with certain characteristics and therefore requires a feature-oriented mindset. The activities within that sprint are:

Sprint Planning – defines the single tasks of the call sprint regarding content, efforts and responsibilities. Typically, a sprint backlog is developed within this activity, ascribing certain aspects of the product backlog to the imminent sprint or sprint cycle.

Function Development - is the core activity of a call sprint with the implementation of system, software or hardware increments.

Functional Analysis – serves to assure that the function just implemented meets its requirements and risks are identified.

Functional Verification – verifies, based on the product backlog, that the function just implemented complies to specification documents, state regulation or state-of-the-art procedures and standards (apart from safety standards which are dealt with in the echo sprint).

Call Sprint Review - reviews the sprint completed regarding its results, enablers and impediments, also as preparation for the impending echo sprint. It often involves acceptance and suitability with product owners or the end customers.

With the completion of the call sprint review, the basis is laid for the safety activities in the echo sprint.

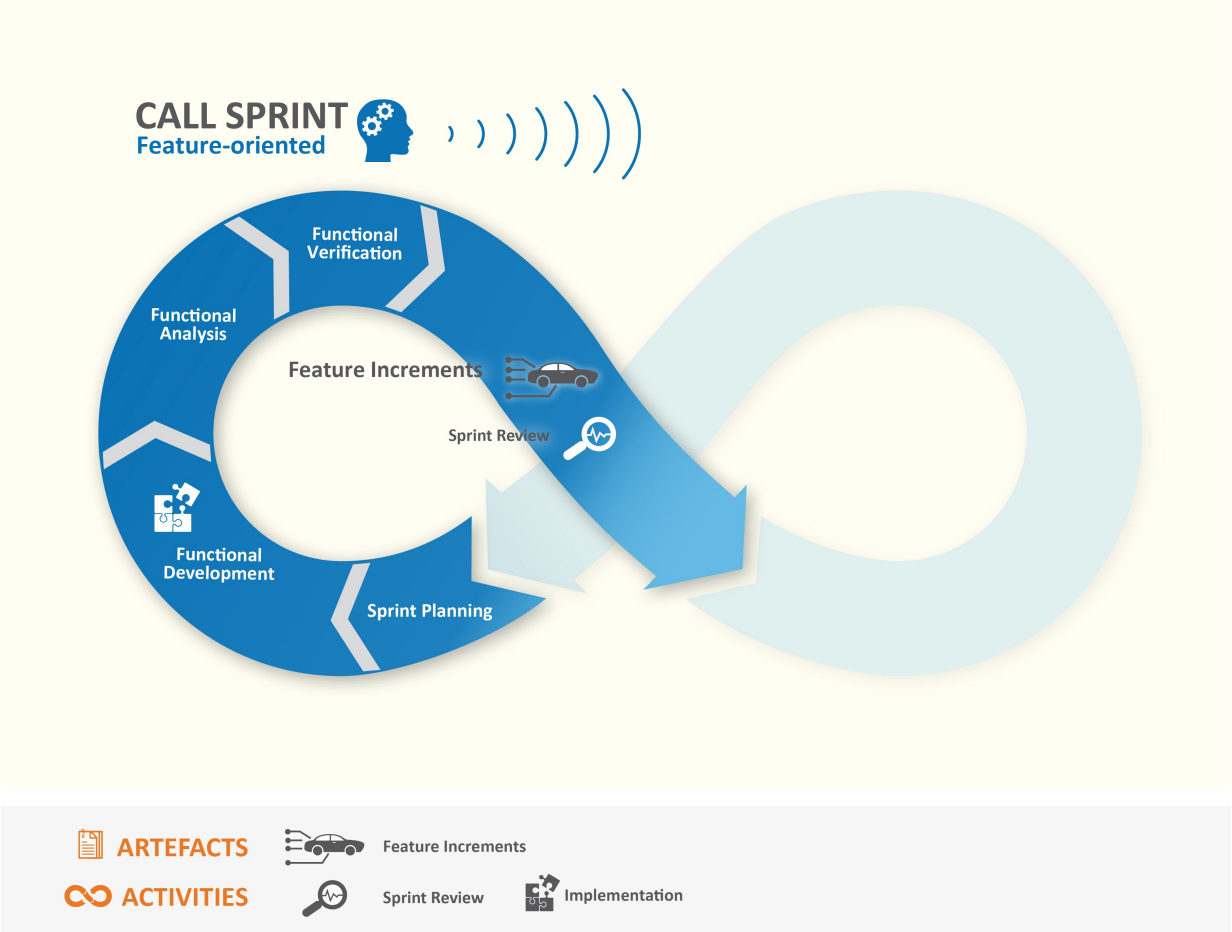

Figure 4 – Call sprint with its activities

4.2.4. Echo-Sprint

The Echo sprint incorporates the product safety activities and therefore requires a hazard-oriented mindset. We need to point out that this sprint does not start with a sprint planning, since these activities are implicitly driven from the characteristics of the developed feature. We recommend that the team recalls the already identified hazards and safety goals, to shift the mindset, before starting the following activities.

Product Safety & Security Planning – defines the single tasks of the echo sprint regarding content, efforts, and responsibilities. Typically, the sprint backlog is groomed within this activity, ascribing certain aspects of the product backlog to the imminent sprint.

Product Safety & Security Analyses – depending on the project phase all applicable types of safety analyses (FMEA, FTA, FMEDA, DFA, STPA), of security and of reliability analyses are being performed incrementally in a holistic approach as basis for an incrementally growing and validated safety plan and concept.

Product Safety & Security Development – implementation of system, software or hardware increments regarding product safety and security measures to be taken.

Product Safety & Security Verification and Validation - based on the product backlog verifies that the safety mechanisms and special safety-related characteristics just implemented comply to specification

documents, product safety & security regulations and norms (like ISO 26262, ISO 21434, ISO/PAS 21448 etc.) and state-of-the-art procedures and standards.

Partial Product Safety & Security Assessment – assesses the function and its product safety & security measures implemented regarding compliance with relevant product safety & security standards.

Echo Sprint Review – reviews the sprint completed regarding its results, enablers, and impediments, also as preparation for the next sprint cycle.

Backlog Grooming - product owner and the team review items on the backlog to ensure the backlog contains the appropriate items, that they are prioritized, and efforts are estimated.

Sprint Cycle Retrospective - the team evaluates the teamwork in a lessons-learned session and creates a plan for improvements for the next sprint cycle. This event takes place at the very end of the echo sprint and serves as the anchor for a continuous improvement process (CIP).

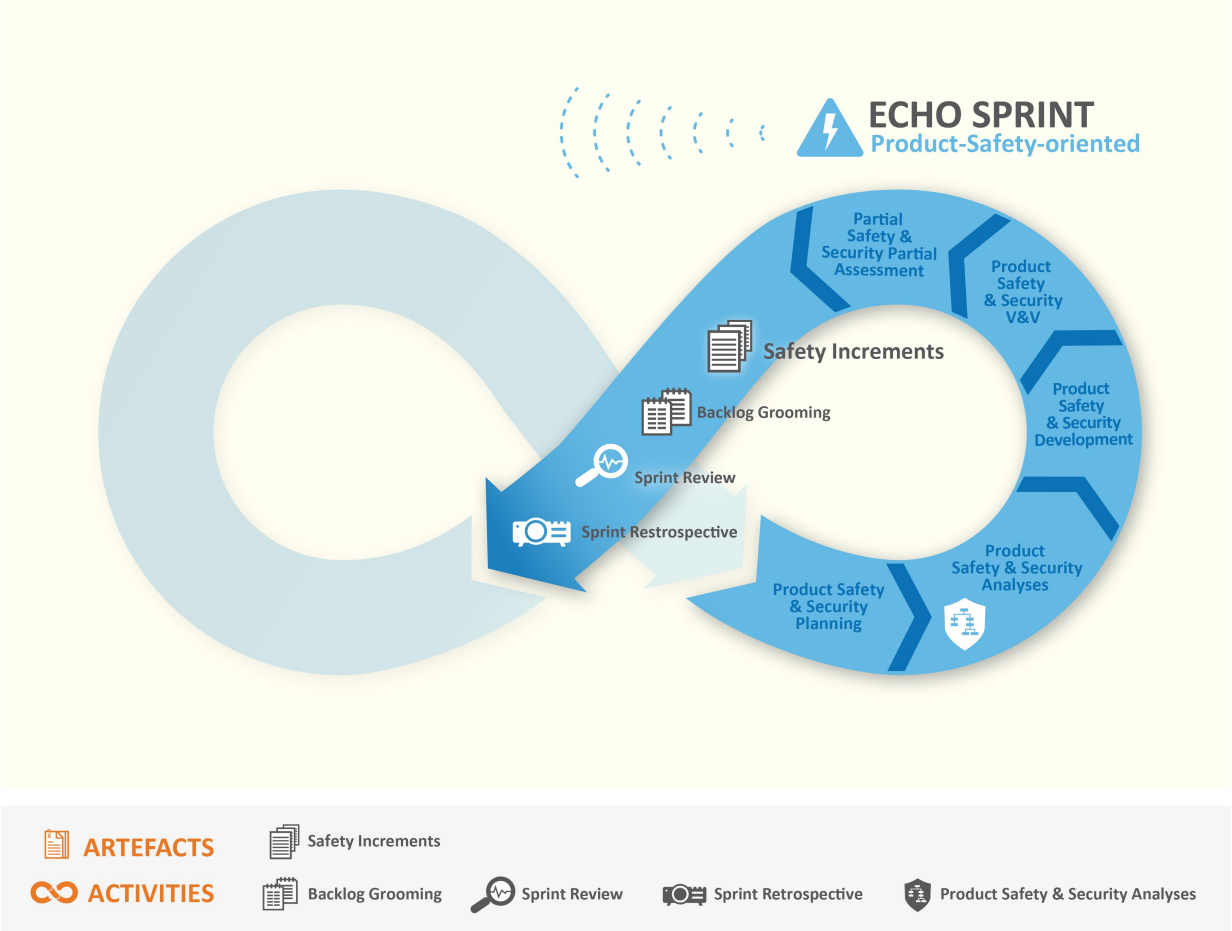

Figure 5 – Echo sprint with its activities

4.2.5. Close-out Phase

When all increments of the safety related system are complete, it may still be necessary to finalize the safety documentation, which was incrementally developed with each MVP and further product increment. The completion of this task may be accomplished outside the EchoScrum® framework or, as a wrap-up, in the close-out phase. We do NOT recommend performing an additional safety assessment, since the necessary steps of inspection, checks and results of such an assessment have already been incrementally assembled toward the end of each echo sprint. Hence it should be possible to prove in the safety wrap-up of the close-out phase consistency throughout all safety artefacts.

4.3. EchoScrum® Artefacts

Product Backlog - comprises all tasks and requirements concerning the product that are known at a particular point of time. The product backlog is dynamic and needs to be groomed after each sprint cycle.

Sprint Backlog - a subset of the product backlog assigned to the sprint. Functional related and functional safety related tasks are in the same backlog.

Agile Safety Plan - an incremental safety plan that shall meet the requirements of the ISO 26262.

Agile Safety Case - an incremental safety case that shall meet the requirements of the ISO 26262.

Both artefacts, agile safety plan and agile safety case, are living artefacts to be groomed and modified within each sprint cycle.

Best Practice

For the sake of clarity, we do not list all safety artefacts mentioned in the ISO 26262. We recommend tailoring safety activities according to the goals of the project and derive the safety artefacts which are adequate.

5. Recommendations for scaled-up solutions

The benefits from agile working environments are recognized among different industries. Different frameworks have been developed to offer scaled-up solutions for complex projects or organizations. One example is the Scaled Agile Framework® (SAFe®), which is organized in five core competencies. EchoScrum® can be integrated in the SAFe® environment at the level of the “team and technical agility” competence.

In a largescale agile approach, EchoScrum® should be used on the team level per scrum-team, not to synchronize more than one agile team. Synchronization between hardware and software development is currently not further described in EchoScrum®, but can be handled by a large-scale framework.

6. Summary of EchoScrum® Benefits

1. **Feature and Safety Development insolubly linked together.**
   - Two sequential sprints are tied together, the first (call sprint) devoted to feature, the second (echo sprint) to safety development.
   - One single team is developing both, feature (call) and safety (echo) sprints. An EchoScrum® team comprises development engineers of multifunctional competences with requirements engineers, system and software architects, software developers and testers as well as safety experts all on board.
   - Thus, safety measures will be conceptualized based on a thorough knowledge of the technical features implemented and vice versa, the feature will be developed based on a profound knowledge of the safety measures required.
2. **Holistic approach to all aspects of Product Safety, Security and Reliability**
   - At the beginning of each Echo Sprint, all applicable types of safety analyses (FMEA, FTA, FMEDA, DFA), system-theoretic process analysis (STPA) and security analysis are being performed incrementally in a holistic approach as basis for an incrementally growing and validated safety plan and concept.
   - Safety and security analyses serve as a supporting, pro-active guide for feature & product safety and security development and not for costly post-development documentation.
   - The minimum viable product (MVP) and its subsequent product increments are sound, completely developed, and investigated for all disciplines including product safety, security and reliability.
3. **Work products proving compliance with ISO 26262-2:2018, ISO 21434, ISO/PAS 21448 and other relevant standards are developed incrementally in each Sprint Cycle.**
   - Checks of consistency, traceability and other standard compliance requirements like partial assessments are executed and respective work-products groomed incrementally.
   - Thereby, the risk of safety aspects being tackled incorrectly, too late and too costly is being minimized.
4. **A Continuous Improvement Process is anchored in regular Sprint Reviews and Sprint Cycle Retrospectives to foster efficiency and professionality of the team and its activities.**

All four main benefits taken together, EchoScrum® with its highly adaptive agile development framework is designed to increase the safety and quality of a high-end safety relevant product significantly.