Series of articles Functional Safety, Part 2

FUNCTIONAL SAFETY

Product lifecycle management – but how!?

The safe way

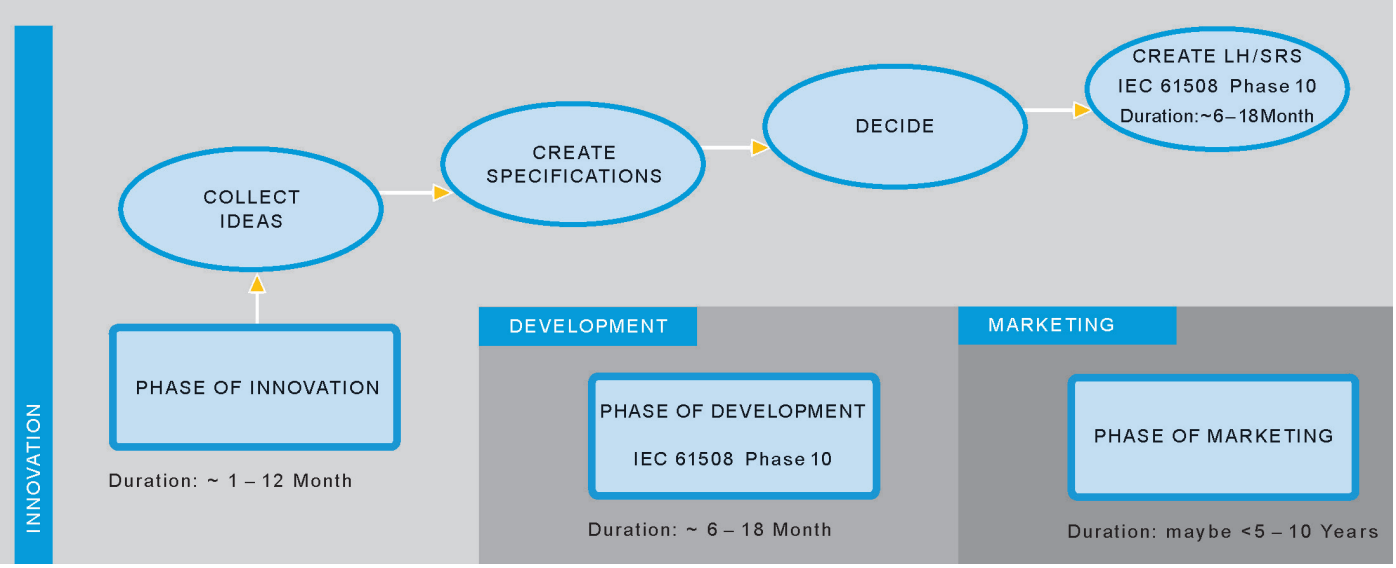

Figure 1: Innovation phase in the lifecycle

Motivation

Part 1 **of this article detailed individual standards and the relationships between them, outlined the safety lifecycle, and explored the tension between flexibility, agility, and the formal requirements stipulated in the standards. Projects to develop a functionally safe component start with the Safety Requirement Specification (SRS). If the process for finding these requirements is too flexible or unsystematic, it can lead to crucial elements being overlooked. However, the SRS may provide the basis for an investment of €500,000 or so. So, it's worth taking a closer look.**

This *second part* **serves as guidance for early project phases and addresses the question of what the** *right* **content of an SRS is. How do you make sure that marketable products are developed? Which products should be developed at all?**

Product strategies

Development resources are always limited, and in times of labour shortages, these resources need to be targeted with even more accuracy. The phases prior to the actual start of development also become more strategic. If the goal is ultimately to create a *me-too product*, the focus is on production costs, development costs, administrative overheads and technical features. Does it make sense to tie up your development capabilities for a me-too product? Does the manufacturer of the actuators or sensors actually need this product in its portfolio, or can the product be purchased from a market competitor? Is it necessary to develop a product that involves breaking new technological ground, or is intended for a market that is just opening up? Does the manufacturer of the actuators or sensors even have the market visibility to position such an *innovation* when compared to established solutions? Is it worth tying up your development capabilities for a customer-specific development or adaptation and in doing so delay products for the general market?

Taking the field of mobile automation as an example, there is currently a trend of subsystem suppliers requesting and integrating functionally safe actuators and sensors, as well as the corresponding functionally safe communication channels (e.g. CANopen Safety or J1939 Safety), into their solutions. System suppliers that have to demonstrate functional safety for the entire system prefer to use products that they can meaningfully integrate into safety assessments, but which can participate in further developments without re-certification. For the manufacturers of the sensors and actuators, this means developing a product that has the features of a functionally safe product, or in other words, an application description, diagnostic coverage, a value for the mean time to dangerous failure (MTTFd) and a common cause analysis. The customers of an actuator/sensor manufacturer can be found in both camps: system and subsystem suppliers.

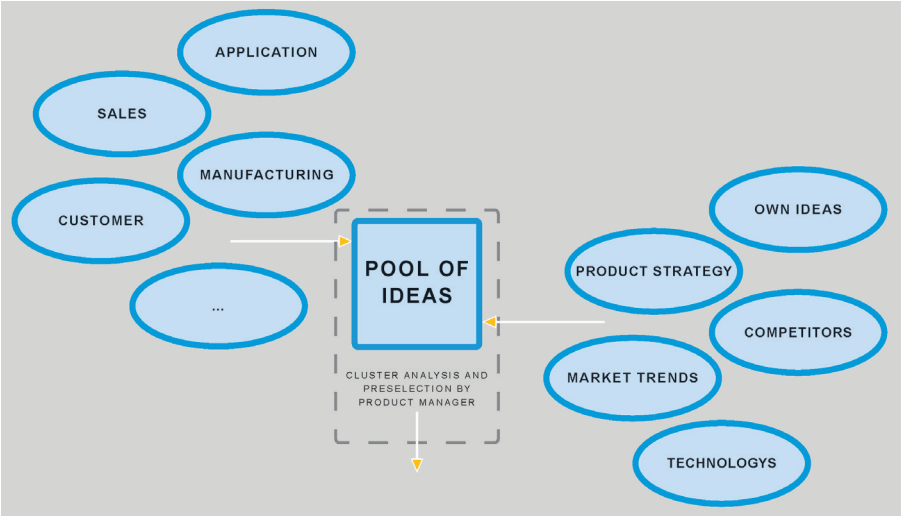

Figure 2: Factors influencing product definition

Another observable trend is the increasingly cheap and powerful synchronous motors and their use in safety-related applications. In this field, it is important to design a system that is functionally safe. The actuator (or in this case synchronous motor), the sensor (in this case the rotary encoder), and the control unit (or in other words the drive system) must be designed to be functionally safe as a complete system. Although standard products are the basis for potential integration, the goal of certification can only be achieved through close cooperation between the manufacturers of actuators and sensors. Requirements from the control unit or from the actuator can be found in the SRS of the rotary encoder.

Thorough analysis and discussion raise the question as to which parameters should be functionally safe. If you take a drive system as an example, does the position have to be functionally safe or the speed? Or perhaps both? Are there any other parameters that have to be functionally safe?

Ultimately, it's not just about *doing things right*, but about *doing the right things*. These strategic considerations about the overall portfolio, the development roadmap and the go-to-market, or in other words the sales presence in the market, are all decisions that have to be made at the highest levels of management.

Selection and decision-making processes

From a formal point of view, the development of a functionally safe component begins with phase 9 of the safety lifecycle and the creation of the Safety Requirement Specification (SRS). As described in Part 1 of this article, the SRS can best be compared to the specifications of a standard product development.

But before you create specifications, you have to decide which products are to be tackled. The following considerations should help you master the innovation phase – the beginning of the product lifecycle. The starting point is that *woolly* topics, such as innovation and product definition, can benefit from a process-driven approach before the actual product development.

Based on our observations, we have divided the innovation phase into the following subsections:

- Collecting product ideas
- Creating product characteristics
- Prioritising and deciding on product ideas
- Creating a specification sheet / SRS

Product profile

The product manager always collects ideas relevant to the portfolio. These may be new ideas or improvements to current products, and can come from the product manager themselves or be suggested to them. Typically, far more product ideas are created than could ever be implemented with the given resources. Once a comparison has been with the portfolio and product strategy, and the economic and technical feasibility has been deemed realistic, it is time to start designing product profiles. These profiles describe the product ideas, customer benefits, key requirements and deadlines, and an initial cost-efficiency assessment (quantity estimation, market price, target costs) is performed.

Formulating the product profile helps to identify any inconsistencies and serves an important basis for making informed decisions with the involvement of all affected business units. A commercially attractive functionally safe product may not even be implementable with the given R&D resources, perhaps because a functional safety manager is not available or the test engineers are tied up in other projects. In such cases, the purchase or integration of external resources may be a better alternative.

In addition to the standard questions and requirements involved in the development of a specific product, functionally safe products pose even more questions. On the one hand, a functionally safe product should be offered unmodified for a longer period time, as changes to the product usually lead to an expensive recertification. Incidentally, this makes it worthwhile, especially with these products and/or product ideas, to put a sufficient amount of care and structure into the discovery phase.

On the other hand, the longer commitment of resources for functional safety development must be taken into account. Does the business case stand alone or does the functionally safe product support non-functionally safe products? Is it necessary in a given market or even for given a customer? Does the functionally safe product have to be integrated into a platform strategy so that the expenses can be transferred to other products as well?

As product decisions have a cross-sectoral impact and a large number of ad-hoc decisions adversely affect day-to-day operations, a one-month turnaround for innovation meetings and decisions has proven to be a good lower limit. In general, these decisions should take place at a higher level of management so that the impact across the company is fully taken into account.

At the end of this phase, it is not uncommon for only a handful of product/improvement ideas to be left from the several dozen or so unfiltered ones you started off with.

For outsiders, it may seem trivial to actually put to paper the product requirements, but even for the most experienced product managers, this always represents a challenge. A classic mistake in this regard is that all conceivable requirements are simply accumulated. The art is actually in the omission of requirements, as only then can the important cost and time aspects be addressed.

Specifications / SRS

Ideally, there should be a template for the specification sheet and / or Safety Requirement Specification, which specifies a structure with minimum contents for the organisation's typical products. Since industrial products are generally not operated completely independently but are rather integrated into a superordinate automation system, many requirements arise from this, such as interfaces, bus systems, types of fastening, design forms, supply voltage ranges, etc.

If the specification sheet for a functionally safe product also includes the SRS, there are a few other requirements to consider. For instance, specific safety-related properties have to be defined and the formal requirements for the creation of the SRS are enhanced.

For a functionally safe product, it is also typically important to determine the safety function, SIL or PL, the safe state, the operating mode (Continuous Mode, High Demand, Low Demand), the maximum failure rate and the error response time. Again, the better the target system is known, the more aptly the product's properties can be formulated.

Formal criteria when preparing the SRS include clear, precise and consistent requirements that are both verifiable and testable. The requirements must be assigned a unique identification number in order to be traceable in all subsequent design documents and test protocols. The SRS then needs to be verified by means of a review, during which an SRS-specific checklist has proven useful.

With the release of the SRS, phase 9 of the IEC 61508 safety lifecycle is complete, and the transition to phase 10 can commence in order to develop the safety-related component.

Summary

Process orientation in product development has contributed significantly to avoiding development risks and improving product quality. This early phase of the product lifecycle is often excluded, as the prevailing opinion is that innovation and processes conflict with each other. On the contrary, processes and structures should not act as a hindrance, but rather serve to provide mental freedom from which innovation can emerge.

Autor: Dr. Johann Pohany
Managing Director
Medidtcine Consultants
www.medidtcine.com

Autor: Armin Götzmann
Managing Director
MESCO Systems GmbH
www.mesco.de