Johner Institute

Functional Safety

With Mario Klessascheck, Prof. Dr. Christian Johner

Transcript

00:00:05 Speaker 1

Medical Device Insights, a podcast by the Ione Institute for medical device manufacturers, authorities and notified bodies.

00:00:18 Speaker 2

For more than a year now, there has been a so-called Interpretation Sheet in the context of IEC 606 and 1 line 1 and functional safety and

00:00:28 Speaker 2

Not all manufacturers have yet taken this interpretation sheet into account and we also observe again and again that there are anomalies in approvals and conformity assessment procedures, let's call it now, which then hinder the further steps.

00:00:42 Speaker 2

And it is precisely for this reason that in today's podcast with Mario Glesaschek I would like to shed light on what functional safety is, what is required by regulation in this context.

00:00:53 Speaker 2

And what can be done so that you don't have unnecessary trouble and can overcome these approval procedures quickly and without unnecessary effort?

00:01:02 Speaker 2

And Ario, that brings us to you.

00:01:04 Speaker 2

If you say maybe 2 sentences to yourself, especially of course in this special context, then our listeners can classify you particularly well.

00:01:11 Speaker 3

Thank you very much, Christian.

00:01:13 Speaker 3

Yes, my name is Mario Klesaschek.

00:01:14 Speaker 3

By background, I am an electrical engineer and have been working in the medical device industry for over 20 years.

00:01:20 Speaker 3

For more than 10 years, I have been helping companies at the Johner Institute to build safety architectures for medical devices, also to evaluate architectures and also to help manufacturers then test the products.

00:01:30 Speaker 3

In other words, also to accompany them through the test laboratories.

00:01:33 Speaker 2

So, the whole stack that you're taking care of, so now not just give any regulatory tips, but hands-on.

00:01:39 Speaker 2

as you said, also to participate in the design of the architecture of these products and to bring them through the tests.

00:01:46 Speaker 2

In other words, everything you need in this context.

00:01:48 Speaker 2

Yes, and that brings us to the middle of the topic, namely functional safety.

00:01:54 Speaker 2

If you would perhaps help us very briefly, perhaps with examples, to understand what this is, perhaps also with a definition and an idea of what would happen if this functional safety were not given.

00:02:05 Speaker 3

Exactly, so examples can be found again and again on products,

00:02:08 Speaker 3

that provide substances or energies.

00:02:10 Speaker 3

In systems theory, systems can only ever deliver information, substances or energies, and especially in the case of medical devices that supply substances or energies, such as the dialysis machine, it is important that the amount, the dose of this substance or energy delivered is appropriate for the medical purpose and that they can also lead to damage.

00:02:30 Speaker 3

And that would mean, in concrete terms, if we now imagine a dialysis machine,

00:02:34 Speaker 3

which pumps blood and then also has a dependence on blood pressure via the speed and with too high

pressure, which is then generated in the system, vessels in the patient can be injured, up to the flaking of blood tubes, which could then lead to blood loss in the patient.

00:02:51 Speaker 3

And accordingly, manufacturers have to build in certain safety functions that detect and prevent a similar situation.

00:02:58 Speaker 3

And functional safety now refers to this safety or protection function, i.e. not to the control function itself, but to this monitoring that then takes place.

00:03:08 Speaker 3

And if we now go into the definition, that is the ability of an electronic system to detect such systematic or random failures, which then have a dangerous effect, and to bring the device into a safe state.

00:03:20 Speaker 3

And so this functional safety is also part of the overall safety,

00:03:25 Speaker 3

which must then be classified, together with the terms basic security and essential performance characteristics.

00:03:30 Speaker 2

O.

00:03:31 Speaker 2

K., I think we'll look at a few other examples of functional safety or what happens when it is not given.

00:03:37 Speaker 2

But in our medical device context, we should perhaps first take a look at the regulatory requirements for this.

00:03:44 Speaker 2

What documents should manufacturers have studied in which they find functional safety requirements?

00:03:51 Speaker 3

Yes, so

00:03:52 Speaker 3

The International is of course the leading standard for medical devices or medical electrical devices and systems, precisely the IEC 60 601 which in different chapters, so now not in one place, but in different sections of the standards set requirements for this safety.

00:04:06 Speaker 3

So, for example, section 47 completely deals with the topic of first-error safety, i.e. how do I deal with the occurrence of errors, what does the topic cover, how do I evaluate the probability of errors and it also places requirements on the selection and reliability of components.

00:04:22 Speaker 3

But it even defines for the inspector how certain failures are to be simulated and also has requirements for the simultaneity of errors.

00:04:30 Speaker 3

There are also country-specific regulations.

00:04:32 Speaker 3

So our MDR, for example, explicitly mentions the first defect that the manufacturer should control.

00:04:38 Speaker 3

Other standards that play a role there are the risk analysis 14 971 for risk management, which sets requirements in the first error and even in IEC 62 304 we find requirements for first error safety.

00:04:49 Speaker 2

If you now expand the Scorp a bit, for example in the direction of the U.S.A., what else would manufacturers have to read?

00:04:55 Speaker 3

Yes, that's right, so the F.D.A.

00:04:57 Speaker 3

has various guidance documents.

00:04:58 Speaker 3

There is no explicit guidance document for functional safety, but there are guidance documents related to the software lifecycle or guidance documents related to the E.M.V.

00:05:08 Speaker 3

in which requirements for this security or first-fault safety are then listed.

00:05:14 Speaker 2

And the F.D.A.

00:05:15 Speaker 2

also recognizes the norms,

00:05:17 Speaker 2

like a 60 6 and a dash 1 or EEC 61010 in the case of in-vitro diagnostics OK, if we study these standards now perhaps a 60 6 and a dash 1, we will then already find concrete measures and perhaps already the follow-up question to them, what are the typical measures to achieve functional safety?

00:05:41 Speaker 3

The I.C.

00:05:42 Speaker 3

60601 defines measures quite well when it comes to passive measures in the field of electrical safety.

00:05:48 Speaker 3

So it has very clear requirements as to how insulation is to be designed, and also how insulation is to be designed, which should then be fail-proof.

00:05:57 Speaker 3

However, it is in the area when it comes to other measures, such as monitoring a temperature or, in our example, monitoring the speed of a pump, then it does not specify how the manufacturer has to deal with it.

00:06:10 Speaker 3

They

00:06:11 Speaker 3

only mentions the requirement that the manufacturer must be able to master this, but does not give any specifications for design or advice on how to build something like this safely.

00:06:18 Speaker 3

And that‘s where other norms come into play.

00:06:21 Speaker 3

We are happy to take this basic standard for functional safety, which is EC 61 508, on which sector-specific standards are then based.

00:06:30 Speaker 3

Even if the standard claims in the foreword that it does not feel for medical devices.

00:06:34 Speaker 3

, as it contains very concrete proposals for solutions, methods and approaches on how to deal with systematic and random errors.

00:06:43 Speaker 3

And then such indications appear, for example, that I have a certain multi-channel capability with an architecture that has to be fail-safe.

00:06:51 Speaker 3

So if one error does not lead to the failure of this whole function, that perhaps a second error does not lead to the failure of the entire function, but it also makes specifications for testing.

00:07:00 Speaker 3

So how do I recognize that a function, a security function is still

00:07:04 Speaker 3

is guaranteed.

00:07:06 Speaker 2

Can we give examples, yes exactly.

00:07:10 Speaker 3

Examples, we had the topic of syringe pumps or other fluid-pumping systems earlier, but where it is important that air bubbles are detected, then a safety function could mean that the system can detect air bubbles in a size X.

00:07:22 Speaker 3

Y.

00:07:23 Speaker 3

and within a certain time brings the system into a safe state, so that the air bubble is no longer promoted.

00:07:32 Speaker 3

and that typically makes a bubble sensor.

00:07:35 Speaker 3

Yes, so we now have monitoring, so a sensor recognizes the air bubble, logic decides, the air bubble has a certain size, I have to act and then reacts, for example, by switching off the pump, i.e. by pressing a switch, which is then the actuator.

00:07:48 Speaker 3

And this chain, that is, this, this monitoring, must now be built in such a way that it is reliable.

00:07:54 Speaker 3

If this chain were to fail, then this

00:07:56 Speaker 3

Pump still work, but if the pump itself has a fault, the function would not be requested.

00:08:02 Speaker 3

So the patient would be insecure and now the manufacturer has several options to make this chain of custody secure by perhaps saying, I'll build a second chain, so I'll do a complete redundancy of

00:08:15 Speaker 3

the system and now there are additional requirements for the detectability of failures, because if the first system fails, I am perhaps sure, because the second system is there, it will also fail after a while.

00:08:26 Speaker 3

I have to assume that I no longer have a protective function at all and therefore there are additional requirements for the recognizability of errors and this results in different architectural patterns that can be evaluated.

00:08:38 Speaker 3

which have also been assessed for their adequacy in accordance with the IEC 61 508 standard.

00:08:44 Speaker 3

I can refer to this because it also represents the state of the art.

00:08:48 Speaker 3

And furthermore, of course, I can also perform calculations on the reliability of components, which I can then also consider as a measure.

00:08:56 Speaker 2

So that means I'll try to summarize it again.

00:08:58 Speaker 2

I have now heard 3 different elements.

00:09:01 Speaker 2

So the first thing you do is, of course, find out what the

00:09:04 Speaker 2

Yes, safety-critical functions that we have at all.

00:09:07 Speaker 2

So in this case it was a bubble detection, for example.

00:09:10 Speaker 2

Then the possibility to achieve this was once a choice of appropriate architecture.

00:09:16 Speaker 2

So, you've now talked about multi-channel or an architecture that is able to find out, for example, whether the detection still works through self-testing.

00:09:25 Speaker 2

And the third building block was the selection of the appropriate components, which we

00:09:30 Speaker 2

which may have characteristics of certain reliability.

00:09:33 Speaker 2

Can you summarize it like this?

00:09:35 Speaker 2

Yes, very well, to the point.

00:09:37 Speaker 2

O.

00:09:38 Speaker 2

K., then I've got it, at least I've understood it.

00:09:41 Speaker 2

Now, everything we have just said directly concerns the products.

00:09:45 Speaker 2

This means that it was probably possible to find out directly by testing the product whether this was the case or not.

00:09:51 Speaker 2

Do you see requirements that must be met on the part of the organization, i.e. the manufacturer organization,

00:09:59 Speaker 2

that go beyond this product requirement.

00:10:01 Speaker 3

Yes, so the manufacturer is of course obliged to ensure that the knowledge is in the team that develops these products and must also prove through training and qualifications that this is available.

00:10:14 Speaker 3

These would be the organizational requirements.

00:10:16 Speaker 3

Of course, the manufacturer can then also seek external advice, which is of course also appropriate to bring in experts, security experts, who may then carry out assessments for an architecture assessment.

00:10:26 Speaker 2

Mhm,

00:10:26 Speaker 2

And test houses, what, what do we still have to look at?

00:10:29 Speaker 2

Or what should the manufacturer pay attention to?

00:10:31 Speaker 2

Or what are the prerequisites for these organizations that contribute to this?

00:10:35 Speaker 3

Test houses are usually, so not usually, test houses have to be accredited for a certain standard.

00:10:40 Speaker 3

This means that they must prove or show or prove to an accreditation authority that they understand and master the standard, and can also specify tests that provide this proof.

00:10:52 Speaker 3

Unfortunately, it is the case that in the area of functional safety or very specifically, perhaps even if you

refer to the essential performance characteristics of a product, the standards do not give very many specifications on how these are to be tested.

00:11:04 Speaker 3

There is usually an inspection of the documentation, the examiner does not have much time for it, so he cannot check in depth as he might want.

00:11:12 Speaker 3

And yes, that's why requirements for completeness or even requirements for documentation are derived from it,

00:11:21 Speaker 3

how a manufacturer can then also support this inspector in doing his job well.

00:11:25 Speaker 2

Mhm, O.

00:11:27 Speaker 2

K., so that means we have requirements, you have best practices out of this 1 60 508, you have requirements for the organization, there was somehow the hope, yes now everything will work out, but reality shows that not everything works out after all, yes and in several respects.

00:11:44 Speaker 2

So on the one hand, we find that that's why many companies come to us,

00:11:48 Speaker 2

because they have encountered problems or have become conspicuous in audits, in in in Tagfile Reviews.

00:11:54 Speaker 2

And on the other hand, we have the very extensive lists of risks that manufacturers had to report to the authorities or even really deaths that we find in these authority databases.

00:12:06 Speaker 2

The question is, what regularly goes wrong?

00:12:10 Speaker 2

So, where do we have there, do we have gaps in the system or what mistakes do the rulers make particularly often here?

00:12:18 Speaker 3

So, we often find in our consulting that the requirements are not clear.

00:12:23 Speaker 3

On the one hand, this is certainly due to the fact that IEC 166 and 1, which are a bit scattered throughout the document.

00:12:29 Speaker 3

In 2021, an interpretation sheet was published, functional, i.e. first-fault safety for essential performance characteristics, precisely on this topic.

00:12:37 Speaker 3

What this requirement of the standard summarizes again is that everyone is then summarized on one page, so to speak.

00:12:43 Speaker 3

This is the performance of the Interpretation Sheet

00:12:45 Speaker 3

And we find that if you go through these summarized requirements, that manufacturers who did not know and did not adhere to them, i.e. what are the limits of the security function, what is the reliability that I need, the evaluation of the architecture is missing.

00:13:02 Speaker 3

So, the products are developed according to best practice engineering, which are certainly good, but this systematic approach to derivation is very often missing and therefore it is perhaps more of a coincidence that the products were safe, but not not derived.

00:13:15 Speaker 2

Mhm, so I can actually hear 2 directions now, where it often doesn't work out that way.

00:13:20 Speaker 2

One is, so to speak, the link to risk management, which would then have to result in many requirements.

00:13:26 Speaker 2

Yes, for example, in the direction of essential performance characteristics and then also the knowledge, what are now very concrete proven measures, as we find them declined in 1 60508, for example.

00:13:39 Speaker 2

Yes, of course, that's a lot that you would have to know and that might go beyond the normal engineering know-how, so to speak.

00:13:47 Speaker 2

How can you, how can your team help make sure that I believe that's the most important thing, that the products are functionally safe?

00:13:54 Speaker 2

Yes, and as a pleasant side effect, that the approval procedures then flow smoothly even then.

00:14:01 Speaker 3

We usually carry out assessments by evaluating the security architecture or, first of all, the architecture in general, together with the manufacturer.

00:14:08 Speaker 3

So, we then built up an extensive catalogue of questions, which we then use, through which we systematically go through in order to then identify weak points.

00:14:15 Speaker 3

The vulnerabilities can be directly related to the architecture.

00:14:18 Speaker 3

However, we also check the completeness of the documentation to see if it is correct.

00:14:23 Speaker 3

In other words, that an auditor or an auditor can also understand.

00:14:26 Speaker 3

what these design decisions were, and we also check whether all requirements have been identified, i.e. whether the standards have been fully implemented, i.e. whether the right standards have been identified at all.

00:14:39 Speaker 3

And we then help manufacturers to create this documentation as well, which helps an inspector to get started quickly.

00:14:47 Speaker 3

We call it a security concept, so we then create a document, it's called a security concept, it can be part of the architecture or an independent document.

00:14:55 Speaker 3

and we would then also create test plans and test plans from them, which would then serve as preparation to then also get offers from test houses and would then also accompany them through the examination if there were any questions from the examiner about certain aspects.

00:15:09 Speaker 2

Mhm, so if I summarize that, is ultimately to achieve this evidentiary certainty or do they help to carry out this evidence really consistently, which of course really works, from risks, requirement to the end to the examination and

00:15:24 Speaker 2

to document this, to make it comprehensible, but also, if you then realize, oops, something is missing, then to help to document things, to correct them and, in the worst case, to adapt the architecture if it is unsuitable for achieving functional safety.

00:15:40 Speaker 2

Yes, so that's the complete program, so to speak.

00:15:42 Speaker 2

So my recommendation would be that if you still have any topics in this context of functional safety IEC 60601, it is best to contact Mario Klessaschek,

00:15:53 Speaker 2

We link you to the contact details below in the show notes so that you can come to him.

00:15:59 Speaker 2

We link you to the Interpretation Sheet and we link to the article on functional safety, so that you can perhaps read everything you have heard here again so that you know how to reach us quickly and easily.

00:16:13 Speaker 2

Yes, Mario, all that remains for me to do is to say thank you very much.

00:16:15 Speaker 3

Thank you, Christian.