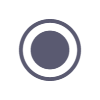
**Continuing Isolette arg. discussion-20250725\_160851-Meeting Recording**

July 25, 2025, 2:08PM

58m 6s

 **Péter Kárpati** started transcription

 **Péter Kárpati** 0:03  
It you too.  
So it started.  
And.  
Please unmute yourself so I can hear. I hope I am unmuted. Yeah.  
Don't please unmute yourself. I don't know whether you.  
Hear me. I hope you hear me.  
I will write it.

 **John** 1:14  
All right, all right. It only took me like 3 minutes to find the little unmute button. I don't know. I'm sorry. Sorry. OK, all right.

 **Péter Kárpati** 1:15  
June? Yo, okay, good, good.  
Let's see. Yeah, that's always tricky. No problem. No problem. I, you know, I just haven't had the feedback, so I I was uncertain about what's happening.

 **John** 1:29  
Yes, I know. OK, all right. So the idea is that we are interested in the concept of form formal methods, integrated model based development.  
And what is important conceptually in this context is that the models themselves.

 **Péter Kárpati** 1:46  
Yes.

 **John** 1:55  
Become formal abstractions of the deployed system, and as formal abstractions, they're analyzable in various ways as mathematical objects.  
And they can become the scaffolding. Let's see the skeleton on which many notions of semantic intent.  
Um and let's see.  
And constraints on the design with respect to its function, its resource utilization, etcetera, are captured.  
And by having this, you know, notion of a formal model, it becomes, let's say, use the overused term, the single source of truth by which analysis.  
Audit system construction through code generation or whatever can be organized.  
All right. So then the purpose of our explicit current activity with the assurance case is to assess the usefulness and impact of this formal.

 **Péter Kárpati** 3:06  
Yes.

 **John** 3:22  
Methods integrated model based development by considering.  
The impact on the assurance case itself or on the assurance process, let's say.  
And so important questions are here is, you know, does this pro approach result in greater assurance, by which we mean all stakeholders agree that?

 **Péter Kárpati** 3:36  
Yes.

 **John** 3:52  
They have greater confidence that the system meets its specifications, or more importantly, the stakeholders intent for the system.

 **Péter Kárpati** 4:02  
Yes.

 **John** 4:03  
All right, it should also. Maybe it also means that the the evidence for insurance assurance is more easily gathered or and or the arguments.  
For the assurance are more easily constructed or constructed in a more systematic way.

 **Péter Kárpati** 4:27  
Yes.

 **John** 4:28  
Perhaps it also means that the assurance is more easily audited in the in the in the conformity assessment process.  
Maybe it also means, especially through the way that the architecture is set up in the development of the system of these frameworks systems, that the assurance is more easily reused.  
Across the different systems or you know, different aspects of the assurance, you know, looking looking forward perhaps because we are being careful in establishing a framework of.

 **Péter Kárpati** 4:57  
Yes.

 **John** 5:14  
Constraints from top to bottom. This would allow AI to, you know, to be employed to aid in the design, aid in the analysis, but because we have the semantically analyzable.  
Strengths built into the entire system. We have the ability to more easily check.  
That the A I did something that is semantically correct. It's not hallucinating, right? And because the A I may itself understand these semantic constraints or be informed about them.  
It can itself guide its reasoning towards the fulfillment of these Uh constraints.  
So that's that's kind of the way that I would summarize overall, you know why. Yeah, OK, go ahead.

 **Péter Kárpati** 6:09  
Yes.  
Yes.  
The A I aspect is not so in focus from in the in the 2.2 activity, but in general we are interested in the A I aspect.

 **John** 6:31  
OK.  
OK, so feel, you know, feel free in whatever summary it is to strike these A I comments. I just yeah, I'm not. I won't be offended if you don't mention the A I so.  
All right.

 **Péter Kárpati** 6:51  
And we stop. I'm sorry.

 **John** 6:52  
So.  
So like in the update that I'm sending you, it's not like I got tons done. I actually spent some hours thinking about it and I met with the Collins team.  
But one of the things that I'm trying to do is to take one particular section of the assurance case and develop it out in greater detail to kind of illustrate the types of things that I think we should be looking at. That's that's right, that's that's there and you'll see one of the several of the columns.  
Over you see that model based development impact.

 **Péter Kárpati** 7:33  
Um.

 **John** 7:34  
The column, the column like column. Yeah, all right. So what I'm trying to do here is to summarize for each claim in the assurance case, how model based development.

 **Péter Kárpati** 7:35  
Other based development, yes, I see.

 **John** 7:50  
Supports that or improves that.

 **Péter Kárpati** 7:56  
Yes.

 **John** 7:56  
And so it's not OK what I have to be careful doing and you know you both you and I.  
We don't want to oversell it, you know, so we want to only claim what we can really substantiate.  
And then we also we want to note, you know where the gaps are.

 **Péter Kárpati** 8:19  
Yes.

 **John** 8:21  
You I've also added another column which.  
I think OK.  
I think it would be most effective if there's. This is why I asked, you know, some weeks ago if there was a.  
An existing development process, standard or conformity assessment, you know, standard or guidelines that the NRC follows where you know for each one of these steps.  
Or claims that are showing up in the assurance case. There can be some sort of association or relationship with the particular claims or requirements in the NRC context like.  
I could, you know, I could sit down and map, you know, each one of these claims that I I've sketched out here in this portion of the assurance case. I could fairly easily map this to, for example, the automotive 26262.  
Steps. You know some of the steps or a medical device standard steps and it would be. I would consider this to be the most effective way of explaining to your stakeholders.  
Why this is useful because they're going to want to know why model based what exactly it helps in their context.

 **Péter Kárpati** 9:56  
Yes.

 **John** 9:57  
And so if there's any way like I I just don't know the new, you know, this is something that.  
Basically you're gonna have to do or you know, if you have these documents, you could. If it's possible that they're open publicly available, then I can also look, but this is the way that I would.

 **Péter Kárpati** 10:14  
Yes.

 **John** 10:20  
Um.  
Try one of the ways that I would try to argue for the relevancy in the impact of this stuff. Just so you know, I'm facing the same issue right now with in this DARPA program, the DARPA.  
Manager and assistants and many other people on the program.  
They don't have systematically laid out an understanding of the impact of this approach. And so at the highest level of the DARPA program, you know, I'm, I'm getting sort of.  
Instructions that we should try to justify our approach by saying, well, here's the, you know, this all the NIST common vulnerabilities. Here's the NIST common vulnerabilities that are addressed, right. You know, here's, you know the.  
You know, the numbers of errors in the source code are low, you know, so it's it's it's not that those things aren't important, it's just that there's what's happening here is much more holistic than these sort of lower level conventional metrics of quality.

 **Péter Kárpati** 11:35  
Yes.

 **John** 11:36  
That are being pushed at various levels of the government. So an important, I'm just like torn up about. So an important thing that we're doing, I mean this is actually really important. So people understand what is the model based development process with integrated formal methods and what are the claims?

 **Péter Kárpati** 11:42  
I see.

 **John** 11:56  
Claims that you're using to justify answer and how to each one of those claims in the you know, the ability to provide evidence for these claims, whatever, how do they impact the holistic, you know, development and assurance process in particular safety critical domains?

 **Péter Kárpati** 12:13  
Yes, yes. So this is these things as I see, let me just say so component specification interface and requirements so.

 **John** 12:26  
So let let I can, I can, I can try to explain. All right, So what I'm trying to do, and this is also the thing that I've chosen to work on, is also influenced by the ongoing priorities in the DARPA program.

 **Péter Kárpati** 12:27  
Some of them, sorry.  
This time.

 **John** 12:42  
So, for example, what we've done over the Yeah, sure.

 **Péter Kárpati** 12:44  
Sorry to interrupt you, John, just for a second. So now I am currently considering the things like the contextual argument which are not not directly level relevant for our promises about the about the.  
Model based formal method integrated assurance but but they're necessary for them but they that won't be the meat of the thing but they are important as you see to explain.

 **John** 13:08  
Right.

 **Péter Kárpati** 13:17  
How how they can benefit from it. So what I wanted to to ask or or see here that how do you see what is relevant for the?  
For the insurance case about the model based formal method supported assurance and what is in the contextual argument which is important to explain what we are doing to explain how they how the.  
Stakeholders benefit. I'm not sure whether you wanted to speak about that, but if you could, if you could highlight that aspect as well.

 **John** 13:53  
OK.  
Well, I I I want to try to.  
OK, so.  
What I've OK.  
So as we've discovered over the last several weeks in our discussions, there's two main, at least two main aspects of the assurance case. One is the safety reasoning itself, you know.  
Identifying the hazards, designing the hazard mitigations, reflecting the hazard mitigations in the requirements. And then what what is being addressed here is the actual.

 **Péter Kárpati** 14:34  
Yes.

 **John** 14:39  
Construction of the system, you know, assuming I'm leaving, you know, this is just a little fragment of the assurance case. We're assuming that someone has done the safety process and has come up with system requirements to establish the safety.  
And has even gone through the process of allocating safety requirements to some notion of component, right?

 **Péter Kárpati** 15:07  
Yes.

 **John** 15:08  
And and I'm drilling down to this level. I I've chosen to present this to work on this in the assurance case because it's exactly what our team is currently doing on the formal method side. So currently in the last six months we've focused on the formal methods and verification of a particular.  
Unit, not the system. So I kind of realized that I'm jumping around here, but but this was one I wanted to, you know, cross leverage the work. So whatever you and I were working on, it also benefited.  
The the DARPA project and vice versa. So what what I hope will happen, you know when we met yesterday they had in their tools the skeleton outline for these insurance case claims and so I'm hoping that to complement your effort.

 **Péter Kárpati** 15:47  
Yes.

 **John** 16:03  
We will actually be stating some of these claims in in resolute.

 **Péter Kárpati** 16:11  
Yes.

 **John** 16:12  
Then we can cross compare. And So what I'm trying to illustrate here is not just the pieces of the assurance case, but what I would consider the process and the organization for the assurance case.  
And to be able to speak to.  
The benefits of model driven development.  
So here in this spreadsheet, what I'm talking about specifically is the the slice of the development process dealing with a component. And so this is a template of claims that you can imagine that hammer would generate.  
Or instantiate for each component.  
So this is already one benefit of having the formal architecture is from the formal architecture, the outline of the assurance case itself, or at least you know, part of these part pieces of the assurance case can be automatically generated.

 **Péter Kárpati** 17:15  
Yes.

 **John** 17:17  
And so this is the template which we would imagine being automatically generated for each component in the isolate.

 **Péter Kárpati** 17:28  
Mhm.

 **John** 17:28  
And so you can see that what I did was I, you know, I started with there's there must be some notion of informal requirements, natural language requirements. I think that's at the very top, right? Oh, even before that is what is the thing that we're.  
What is the component? And by that I mean what is at least what is the boundary of the component? What are its interfaces, its inputs and outputs? Because the key aspect of the.

 **Péter Kárpati** 17:59  
Yes.

 **John** 18:04  
Of functional safety is to constrain and define the functions being computed by the system and then the components. So you're right in clicking back to that because that is a denif, you know that's.  
Talking about the boundary of the system, so we can begin to talk about its functional behavior and constrain it. And then so when I'm then showing, when I'm then showing is the assurance case at the level of a individual component, right? So.  
There's the idea of, you know, the interface itself is defined and the interface, because it's defined formally, is already shows benefits, right? So if we go column by column, what I'm trying to do is to say.  
When would we expect this step to be done in the development process, let's say component design, who's responsible for it producing this insurance assurance, the component developer. So somewhere these these roles.  
Should be officially, you know, enumerated the same with the development plan. And then who's responsible for assessing the quality of these things?

 **Péter Kárpati** 19:19  
Yes.

 **John** 19:29  
So for example, somebody could say, oh, I have requirements for this component and you are are attempted to check it off the box or check the box. Oh, it's done. Well, no, it's not done unless somebody assesses the quality of those requirements. Now some things that are checkable by formal methods.

 **Péter Kárpati** 19:29  
Yes.  
OK.  
Yes.  
Yes.

 **John** 20:10  
And so, you know, what's what's important here is to not necessarily get exactly right all of these pieces, but to identify that these pieces are necessary.  
All right. And OK, so then the next, the next column is what is the evidence artifact for this? So to Support this particular claim in the insurance case, what piece of, you know, what artifacts are going to be linked to?

 **Péter Kárpati** 20:24  
Did.  
Yes, indeed.

 **John** 20:42  
And you know 26262 does a great job at this. You know with every development step in 26262 it says exactly where you're what's what artifact is being changed or updated.  
And it's super, I I just really like it. And So what I'm trying to do is to emphasize that concept here. So we will also eventually have some enumeration of the of the different categories of artifacts that are being, you know, so this is.  
The models, the requirements, the test plan, you know, the test, the the test cases, the test vectors, right? The you know, all of the all of these things need to be enumerated.

 **Péter Kárpati** 21:31  
Yes, these are the the square brackets, right? Model infrastructure code and so on requirements do code, yes.

 **John** 21:36  
Yes, right.  
Right, right. And some of these, yeah. And then let's see, what did I, what was the next column over? OK. So this is a a something specific to our DARPA project where we have a.  
If one of the teams is developing A framework where the general purpose of the framework is to assess.  
The let's sort of say the fidelity of the steps in the development process. One easy example to understand is assessing the fidelity of the code with respect to the models.  
In other words, once Hammer runs and generates the code, you're relying on the fact that the code is in line with the models, and you don't want someone to go in and change the interfaces generated by Hammer without changing the models.

 **Péter Kárpati** 22:39  
Yes.

 **John** 22:39  
Right. Without without the the models being In Sync. And So what their tool does is it basically uses, you know, cryptographic signing and fingerprinting and hashing to try to provide some sort of guarantee that for example.

 **Péter Kárpati** 22:52  
Mm.

 **John** 22:58  
The code or the interfaces. I'm just taking I'm continuing to go with this one example. The interfaces that are generated are in line with the hammer processed model. So when hammer runs, it produces hashes or fingerprints of these things.  
So it can tell if somebody modified one or the other behind the scenes without rerunning the code generation.

 **Péter Kárpati** 23:23  
Very clever.

 **John** 23:25  
Yeah. So this is also an important concept because the whole fidelity of the assurance, you know, the the benefits that we're claiming for all of this depend on the fact that the model is an accurate abstraction of the code.  
And or the implementation. And so that claim itself must be justified, right? And so the attestation step is a way of providing machine guarantees. You know, it doesn't do everything, but it's a way of.

 **Péter Kárpati** 23:46  
Yes.

 **John** 24:03  
Substantiating these claims like for and as a second example, what it also does is or it will do is ensure that if you have a a contract in the model that formalizes A requirement and that contract gets translated down into code contracts in Hammer.

 **Péter Kárpati** 24:07  
Yes.

 **John** 24:23  
Right. You can check that the developer didn't hand edit the, you know, the contracts in the code and introduce an inconsistency between the code contract and the model contract.

 **Péter Kárpati** 24:25  
Yes.  
I see. So it's also the contracts. It's also extended for the contracts.

 **John** 24:48  
Yes, and it will be extended for a number of aspects, the which we haven't figured out yet everything that we can do or we want to do, but this attestation column is a way for me to.  
To keep track of oh, where, you know, where do we need to do this attestation and is it possible to do it and what might it look like? And I I I probably haven't filled that in yet.

 **Péter Kárpati** 25:11  
I see.  
So all the the generated things and the base of the generator since they are in sync, that's.

 **John** 25:22  
Correct, correct.

 **Péter Kárpati** 25:25  
Yes.

 **John** 25:26  
And then the next column is a related column, which is, you know, the traceability. For each thing, for each claim that's being made here, are there notions of traceability involved?  
That are relevant for that particular claim. So what we and this often corresponds to the attestation in the sense that oh, if you have code contracts, they should trace to the model contracts and then the attestation itself should.  
Somehow then provide a a verification of that traceability or you know, as you said, the In Syncness of the things that are being traced to.

 **Péter Kárpati** 26:11  
I see. So this traceability is more limited traceability. It's not the generic traceability that you want to provide traceability from the requirements or from the.  
Yeah, from the requirements to the evidence to the.

 **John** 26:29  
So.  
This is, I would say it's it is more limited so to speak, but I would choose to phrase it as it's more fine grain because what you want, what you want then is that these individual pieces of traceability here in some sense compose.

 **Péter Kárpati** 26:41  
Bye, thank you.

 **John** 26:50  
To give you your big picture traceability, right? That you know, for example, the contracts in the code should ultimately trace to the requirements, but.

 **Péter Kárpati** 26:54  
Yes.

 **John** 27:03  
But that is a series of trace of smaller traceability steps.

 **Péter Kárpati** 27:03  
Yes.  
Yes.

 **John** 27:09  
So what I hope to have done before I retire.  
What I hope it comes out of this project is some sort of tool that allows you to display in a graphical form the traceability, right? So you you can it will produce a let's say a traceability view, a clickable traceability view where it.  
Shows you, you know in a graph, right? Or you know some other easily digestible notion, these important traceability claims. And then if you if you're at the particular, you know if you're looking at the code and you want to say oh.  
What natural language requirement does this correspond to? You know you can click somewhere and then you get the requirements document.  
Etcetera. All right.

 **Péter Kárpati** 28:07  
Yes, is it? Is it traceability only for the generated stuff or in a more generic way?

 **John** 28:17  
No. So it it's it's also more in a more generic way because there are there are places. So that's a great question that you ask. So there are places of course where the mechanized aspects of model based development are being linked to the human.  
Constructed in informal aspects. And so this is, as you're hinting, this is exactly where traceability is extremely important because you it is very hard. If in fact it's, I guess we would say philosophy in a philosophical terms.

 **Péter Kárpati** 28:39  
Yes.

 **John** 28:54  
It's impossible to make a formal connection between the informal and the formal, and so the best that you can do is to establish these sort of, let's say, semantic hints or semantic intentions of the alignment that must be verified by human inspection.

 **Péter Kárpati** 29:12  
Yes, and in that case is the up the up the station will be not not.

 **John** 29:22  
Correct.

 **Péter Kárpati** 29:23  
Interpretable because that's not the. Yeah, OK.

 **John** 29:26  
Correct. Although you know there may be some notion of.  
You know, bits and pieces of it like might be a test. You might be subject to attestation. Like for example, let's assume that in your requirements you adopt.  
A structured approach by which, for example, important nouns and verbs in your natural language requirements refer to either a data dictionary or, you know, a what do I say?  
An ontology or you know A and it's a glossary, you know, established collection of terms and you can also use potentially automated attestation in those.

 **Péter Kárpati** 30:08  
OK.

 **John** 30:24  
Fragments of the informal thing to say, you know, if something has changed over here, you know, then we see, then we must ensure consistency over here, but and.  
Right.

 **Péter Kárpati** 30:48  
And then that the attestation would kind of say that OK, that definition what we used in this version of the requirement, it doesn't mean anymore the same because.

 **John** 30:49  
Right.

 **Péter Kárpati** 31:05  
The there was a change in the concept of what the requirement uses.

 **John** 31:14  
Yeah, that's correct. And you know, I'm sort of reaching here. Maybe not all of this is possible, but what I imagine in those cases is the attestation process might be doing something.  
Like saying, you know there needs to be some manual check or manual audit or manual review of the requirements to make sure that the change in the definition that you're referencing is appropriate for, you know, the current way that.  
The requirement is phrased, you know, so it could be just like an automatic generation of an audit obligation.

 **Péter Kárpati** 31:59  
Yes, very interesting.

 **John** 31:59  
Yeah, but you're right in, you're right in general that the attestation is primarily.  
Primarily focused on the automatically generated artifacts.

 **Péter Kárpati** 32:15  
I see, yes.

 **John** 32:17  
And so then you know the final column is.  
You're not necessary. OK. So this is where I'm, you know, we're trying to explain, yes, what is the impact of of model based and how is it helping us?  
And by model based development of course you know that includes the I I I maybe want to rephrase you know the the formal methods.  
Integrated model based development. So here you know is my first attempt to and I've only gotten through maybe six or seven of these, but to to describe for each one of these claims.

 **Péter Kárpati** 32:46  
Yes.

 **John** 32:58  
You know what? What is the benefit? You know why is this important? How is model-based development supporting this? Et cetera, et cetera.

 **Péter Kárpati** 33:10  
Yes, probably it could be like you have a, you have a collection of the benefits, right? And then you could just say that for this step this, this or and so, so just listing the benefits code so to say.

 **John** 33:10  
Um.  
Yes.

 **Péter Kárpati** 33:30  
Or maybe you need to explain it more granularly that this benefit is applied or or applies here because of that and that.

 **John** 33:41  
Right. You know, so at at this point of course you know I'm I'm thinking about your your customer, you know your Sushil and others and so it's at this you know.  
This is the types of material that they should ultimately review, you know, because now we're getting to, I'm claiming that there are benefits, but there's, I'm sure there's things that you and you know, the NRC folks.

 **Péter Kárpati** 34:04  
Yes.

 **John** 34:13  
Know that.  
Manufacturers have to do and struggle with than I am missing here, right? Or they may have things. Maybe I'm overselling a particular point because they already have tools to support.  
Some aspect of it.

 **Péter Kárpati** 34:35  
I see.

 **John** 34:36  
So you know, when I imagine the, you know, a report.  
8.  
That you know we produce and then you know you customize it for your particular domain.  
You know, these aspects here that I'm listing in this column are are super important I think. And then what we would try to do is you know there this is low level what I have in this column, what we would try to do you know in the opening of such a report is.

 **Péter Kárpati** 34:55  
Yes.

 **John** 35:14  
Is to distill key concepts that show up repeatedly, you know, in these little cells of the spreadsheet to describe overall.  
You know the benefits of the model based development and then you would further substantiate these claims by direct link in the next column to any sort of existing.

 **Péter Kárpati** 35:34  
It's.

 **John** 35:43  
You know, doc documented, yeah.

 **Péter Kárpati** 35:44  
Yes, yes, in the regulations what they want to need to comply that which regulation criteria it relates to or or exemplify maybe with.

 **John** 35:48  
Yeah.

 **Péter Kárpati** 36:00  
Then something these mishaps, examples of mishaps that was caused because this was not not fulfilled or these benefits. Yeah, that that that they weren't.  
That they they cause problems so to say if if the the ambiguity or.

 **John** 36:18  
Yeah.  
Right.

 **Péter Kárpati** 36:28  
Whatever. Or maybe not just disadvantages, but or not, not just mishaps, but disadvantages as well, like they started the the development of an.  
Planned and then WJ was X million or milliard and then million and then when they finished it was double time, double BJ.

 **John** 36:50  
Yeah, yeah.  
Yeah, exactly. So these, you know, these sorts of you're getting to the point that we we can be more convincing in our presentation if we have these interesting anecdotes.  
You know, backed up by, you know, actual reports or links or is Even better. But yes, and this is something that is, I don't know and you know it would only be you and the NRC folks that are able to.

 **Péter Kárpati** 37:15  
Yes.

 **John** 37:27  
Um.

 **Péter Kárpati** 37:28  
Support these ideas. Support, yes.

 **John** 37:29  
Supply these sorts of anecdotes. OK, so thank you for listening while I've just like did a total brain dump of everything. So should we go back to your e-mail and see if now?

 **Péter Kárpati** 37:40  
Thank you.

 **John** 37:42  
We have a tell me again, let's start. You know, are we getting at the right things for you?

 **Péter Kárpati** 37:45  
Yes.  
Definitely. I intend to to to intend to to to outline the foundations too much and then maybe too too much time, spend too much time on on this contextual argument like what is here.

 **John** 38:03  
Mhm.

 **Péter Kárpati** 38:10  
Year that that.  
Introduce the that we start with the isolate system and then we move to the component and then you know this maybe caring too much about these parts because because I I want to see clearly how, how, how, what is the context.

 **John** 38:28  
Well.

 **Péter Kárpati** 38:33  
Where we use it.

 **John** 38:35  
No, I think that's fine. I don't. I think that's fine. I mean, I haven't gone through what you've written in this assurance case here on the screen in detail yet, but I think, I think it's important to have them understand again.  
How this, which essentially how this engineering technique maps on to, you know, the development process and the the safety, the safety assessment, you know, the safety process.

 **Péter Kárpati** 39:07  
Yes. So yeah, yes, exactly. And that's that's one of my struggles or troubles. I I will show that later. I'm just quickly showing it to you that here I have a claim so.  
I went from the the isolate to the thermostat component and the thermostat requirements are adequate. The other requirements related to its safety objective are adequate because it's so it's just focusing on the safety. Basically that's what I say here.

 **John** 39:27  
Right.  
Right.

 **Péter Kárpati** 39:41  
And then here I started to introduce your.  
Your your boundary goals, TTL. What was the TL? Sorry, the system requirements, the top level system requirements, the subsystem requires component requirements. So that's where I started to to include that the boundary and.  
Context the top level goals, top level environment deployment assumptions, the system level, subsystem level, component level. So that's how I started to consider, but naturally these.  
So, so one of the struggle is that the system level, subsystem level stuff that might be might be handled and outlined a bit higher and then here we might just want to refer back to them that OK, there is an argument about that.

 **John** 40:27  
Yes.

 **Péter Kárpati** 40:39  
A subargument somewhere there and then we we we don't detail it here. We just state that these are OK as a precondition or and then here the component level.  
Must.

 **John** 40:55  
Yeah, I I have to say, I mean, I I of course did what I did in the spreadsheet at the component level because that's what I understood the most. I don't understand exactly how this part that you're dealing with should be stated. And so I I sympathize with you. I I don't know how to.  
To do it, I mean one one thought that you know it's it's already kind of showing up here is that I chose arbitrarily some of these words related to the architecture like system, subsystem, component. I don't the the issue is.  
In general, that these concepts are are.  
They're not necessarily, they're they're somewhat arbitrarily chosen.

 **Péter Kárpati** 41:41  
Luis.  
Yes, yes, that how how you how you what what are your abstractions of the architecture that's.

 **John** 41:52  
Right. And so for example, the way the way that 26262 does it and other, you know and other standards which I haven't reflected at all in any of my writings for you is that 26262 introduces in in general a notion of an.

 **Péter Kárpati** 41:59  
OK.

 **John** 42:12  
Item, right? It's a generic unit and it's recursive, you know? So you don't. It avoids getting locked into this notion of a system and a subsystem. And OK, now do we have a sub subsystem?

 **Péter Kárpati** 42:14  
Yes.

 **John** 42:31  
In a sub sub subsystem, you know. So yes. So in general at at some level they introduce a notion of a generic notion of an item, which is then recursive.

 **Péter Kárpati** 42:33  
Yes.  
I see.

 **John** 42:47  
And so it it avoids, you know, then some items are leaf items, you know, because you don't decompose it anymore in the safety reasoning or it may be a unit that a manufacturer develops as a product, right. So you stop, you stop decomposing because it is a single distributable thing.

 **Péter Kárpati** 43:01  
Yes.

 **John** 43:07  
Saying that's being you know in the broader development ecosystem being shared and talked about as a single unit. So I I just give this remark to say that I the part that you're outlining here in you know you're saying well should I don't. Yeah this is for us to discover to some extent and of.

 **Péter Kárpati** 43:14  
Yes.

 **John** 43:26  
Course, some of these aspects can be explained in terms of the isolate, but again, because we're making the explanation in terms of one system only, we may not be being sufficiently general and so.  
We have to, we will have to acknowledge up front that as we're illustrating this for the isolate is 1 case and it may not be a sufficient basis for generalization.

 **Péter Kárpati** 43:54  
Yes, but but that's I think from a practical point of view it will be still a very good, good experience even if we don't make everybody fits example which we can develop a generic template. So that that's I think that's not the problem.

 **John** 43:55  
OK.  
Yeah.

 **Péter Kárpati** 44:14  
The thing is that we somehow show that there are some stuff which are preconditions that they are done for us to the component and we kind of identify not at this level that is system, subsystem, but that those requirements.  
Those context, environmental context, deployment assumptions and so on that they they are stated somewhere. So and as you said you if I remember correctly that you want to outline a bit the system level.  
Requirements for for the isolate and what I tried to do was to we have two processes now, right? We have the, we have the requirements engineering management process.

 **John** 45:06  
Right.

 **Péter Kárpati** 45:07  
And we use the risk management process and which of your?  
Artifacts or or yes, let's say artifacts are coming from which one and and how how I think they that that would be important for the contextual argument like saying that.  
That they are not just hanging in there. You know that the the developed the boundary context because then one might ask OK, but you might have missed here something or or or how do I know that?

 **John** 45:38  
Right.  
Yeah.  
Right.

 **Péter Kárpati** 45:49  
They are well established things and and what I what I got confused first that OK when do we use the.  
Where is it?  
That is the PDF. When do we use the requirements engineering management steps and when we are using the the risk management steps because they are kind of.

 **John** 46:12  
Yeah.

 **Péter Kárpati** 46:22  
Intervened so so like sometimes from here, sometimes from there and then I asked the the the pilot, the copilot to to do something here.

 **John** 46:34  
Yeah.

 **Péter Kárpati** 46:37  
And and then it came up with something. It sounded good.

 **John** 46:38  
It.  
OK, this I have to admit I haven't looked at this yet, so this seems like interesting to see because so how did how did you feed the the PDFS?

 **Péter Kárpati** 46:48  
I.  
I I add that to public this is a copilot which is private for us. So it's a it states that it doesn't you it doesn't share anything and and if I said so my company said that that we can.

 **John** 46:54  
To what was?  
Yeah.

 **Péter Kárpati** 47:14  
And use it for our private documents. But I haven't done that. I just used the two public links because the requirements Engineering Management handbook that is a public source. So I just added the link.

 **John** 47:16  
Yes.  
Yeah.

 **Péter Kárpati** 47:30  
That here is the link and the other is I found this white paper. This was another other white paper and this speaks about the requirements risk management for medical device. So so the.

 **John** 47:38  
Right.

 **Péter Kárpati** 47:45  
The this standard so and it was quite verbose so I I added the link to this one and based on that.

 **John** 47:54  
Yeah, can you can you also send me the the PDF or the link for that in the e-mail?

 **Péter Kárpati** 48:00  
Sure, sure it's I will do that. I think it is also in the document what I sent you, but but let me check.

 **John** 48:09  
Oh, OK, OK, well, OK, then don't don't bother then.  
So this is very interesting, I mean.

 **Péter Kárpati** 48:15  
No, no, I will send it to you. It's not here. So and then I ask it to combine and and see and and also see which step is coming from which document. You see this is the origin, but I started to add the green parts which means that I identified the exact.

 **John** 48:23  
OK.  
Right. Okay.

 **Péter Kárpati** 48:34  
Source more or less for the for for the step that is coming from here is coming from here then it identify that here is OK.  
Yeah, that he this, this step also relates to the REMHA book, not just to the stand to the other standard. Then this step probably should be the document risk management plan. It's kind of.

 **John** 48:47  
Oh.  
Yeah.

 **Péter Kárpati** 49:04  
Speaks about it kind of late, so it might be needed to be before, but my my main point is that that I I think it would be useful to see that.  
What you generate here that how how do they relate to the process what we follow?

 **John** 49:30  
Yes, I totally agree. I mean, I'm super happy that you've done this. Super happy. You know, when I when I was working on this medical device interoperability standard a number of years ago, I did something similar to this.

 **Péter Kárpati** 49:31  
I need, yeah.

 **John** 49:46  
And and here's at you, you have uncovered the challenge in in the sense that in a particular domain like the medical domain, there is not a single standard that integrates everything. You know there's the 14971, the the risk management standard. There's another standard for 62.  
2304 I think for the software development process. So it's in that document, for example, that you see things like, oh, you define the architect, you define your interfaces, you decompose A component into its units and.  
And so it's always a struggle for people coming into the domain that are new to understand how to weave these things together. So it's exactly the problem that you've attacked here. So I I'm, I'm speaking a little fast because I I have another meeting now, but I think this is so.

 **Péter Kárpati** 50:33  
Yes, yes.

 **John** 50:43  
So important to say. So what we might do is, is so this requirement engineering management handbook, it's more like, you know, it's not an official process. It's more like a collection of ideas. It's like in a textbook, right? And So what we might.

 **Péter Kárpati** 51:02  
Yes.

 **John** 51:03  
Choose to do is to instead of making the traceability here to that document, we may emphasize more like the 62304 document or some other document that you know that outlines more the development process.

 **Péter Kárpati** 51:22  
I don't mind that then we can discuss that maybe in the next. If you are in a hurry then we can discuss that in the in the next meeting that what we use or you can write an e-mail about and then and yeah.

 **John** 51:23  
Yeah.  
Mhm.  
Yeah.  
But this I I just want to say this is super important, Pete. I'm I'm so glad that you've done this because when I did this before for other purposes, I mean, it wasn't for the isolate, it was, but I spent months making a huge Microsoft Word document and I did exactly this.  
In the sense that I I had to come up with my own steps like we have, like you have in the left column. And then I had to establish the links in the compliance artifacts. And you can see that you and I have sort of independently arrived at the same need because it's kind of what I'm trying to get at the spreadsheet, right. I had that last.

 **Péter Kárpati** 51:58  
Yeah.  
OK.

 **John** 52:12  
Last column where I was suggesting that you know you you connect to in the nuclear domain and of course you know what you've done is this is to illustrate, start to illustrate the same concepts for the medical domain.  
But if if we're trying to convince the broader community of the utility of this approach.  
This this what you're doing is extremely important and I think we should emphasize it because if if people, I'm just so into this cause I had this all of these things happening to me this week.  
Unless these and like the people like this guy sends me an e-mail. He says, oh, I need to convince Lockheed Martin of why what you know you're doing here with hammer is important. And again he had it was so it was wrong in the way that he was trying to sell it was like, oh, we eliminate buffer over.  
Flows and it's like, no, that is not the main, you know, it's this, you know, it's it's how does the whole thing fit within the development process? How does it Support the compliance arguments, the overall safety arguments? And so if we can.  
You know, you know, you and I, this is a huge job. But if you and I can, you know, get the get illustrate this for the medical domain and then you can, you know, also map it to the nuclear domain. I think this is super important.  
Yeah.

 **Péter Kárpati** 53:45  
It would be good to to establish a framework for it like maybe step description, origin, MBSE formal method benefits and I don't know assurance something that that could be.

 **John** 53:49  
Yeah.

 **Péter Kárpati** 54:01  
That could be interesting to to to. So we can we can continue. I just would like to say one last thing here that here we have the steps like as a thermostatic, let's see the isothermostatic requirements.

 **John** 54:04  
Yeah.

 **Péter Kárpati** 54:19  
The the same object we are adequate and then we decompose and here I want to focus on the products on the on the on the performance so to say and here on a cycle I say that this is right decomposition because we use this and that process.

 **John** 54:29  
Mhm.

 **Péter Kárpati** 54:37  
And we claimed that the process was adequate and we used it adequately. So this is a side argument and that's that's the way I want to to to be not process focused but product or or performance based.

 **John** 54:45  
Right.

 **Péter Kárpati** 54:53  
And and that that's that's where I would use these these description of the of the process and and then relate that these artifacts come from this process or this step of the process, this argument, this artifact came from this.  
Step of the process and so on. I just wanted to add this for for the application.

 **John** 55:16  
Yeah. OK. That's that's great. I'm sorry that I haven't had time to to look at these things yet, but my main comment to you is thank you so much for for doing this, for identifying it. That's a need because I totally agree and.  
Let me say something else. I work with so many other people.  
That tend to focus on the fine grain application of formal methods and sometimes this stuff that we talk about right here they view as boring or not something that they want to work on.  
But it's crucial to explaining to, you know, the ultimate stakeholders, the regulatory agency, the manufacturers, why this is important and how to use it. So thank you so much for for working on this.

 **Péter Kárpati** 56:10  
Yes.  
No, I'm glad that we can work together on this end and it's it's it's very interesting. So I will send you then this updated document and I will send you the PDF and the link to the public risk management document.

 **John** 56:17  
Yeah.  
OK, great. And if you can also you, you will send out a link to the recording or the transcript or something.

 **Péter Kárpati** 56:30  
Yes.  
Yes, I will send the transcript.

 **John** 56:37  
OK, good.

 **Péter Kárpati** 56:39  
And and I don't know the the link to it's it for me. I will show you for me it shows in the chat. If you get back to it then you see I have this few recap and transcript so you you can you can't download the transcript. That's why I'm sending to you. But if you come back this is or.  
Chat on on the 16th of July and then you can, if you can get back to this meeting, you join again the meeting, then I think you can see the recap as well.

 **John** 57:03  
OK.  
OK, I may maybe I need the the Teams app for that 'cause now I'm just using the web interface. I'm not sure I see all of this stuff.

 **Péter Kárpati** 57:16  
OK.  
Try and if not, I I I can try to help. I I'm not an expert, but I can try to help with that. Maybe let's have the the next meeting in two weeks.

 **John** 57:30  
Yeah, sounds good.

 **Péter Kárpati** 57:32  
Same same or Wednesday. This what would be the 6th of August.

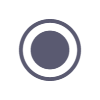
 **John** 57:43  
Just a second.  
Yes, that sounds fine.

 **Péter Kárpati** 57:49  
At 9:00 your time.

 **John** 57:52  
Yes.

 **Péter Kárpati** 57:53  
OK. I will send then the invite shortly. Thank you very much.

 **John** 57:58  
OK. Thank you, Peter. Appreciate it.

 **Péter Kárpati** stopped transcription