**[HVT][WS03 Extra2] Cyber-20250509\_133101-Meeting Recording**

0:02  
Ohh, not too much time, OK, for this meeting, right.

0:07  
So Vijay we can start.

0:09  
Yeah, sure.

0:10  
Yeah, thanks.

0:11  
So Stefan, who will provide us that the cyber security related information?

0:18  
So we have Catalin Stasi, he's on workgroup for cyber security and also we have Marta Alexander.

0:35  
We does he wanted to to join.

0:48  
Yeah.

0:48  
So maybe I think, I think they were part of earlier workshop also, right?

0:53  
Yes.

0:54  
OK.

0:54  
So maybe we can directly start with this topic.

0:58  
So hi.

0:59  
So we would like to understand how you manage the cyber security requirements, any specific tool use or you do this manually.

1:10  
So if you just explain that end to end process from start to end that will be helpful and in between we will ask that the if any specific questions comes I will ask those.

1:20  
So will that help?

1:21  
Will you able to show us that process?

1:24  
Yeah, but I think that today in whole side there is no process written for the cyber security part and I'll explain to you why.

1:31  
So currently for the existing renovable projects, there is a cyber security team in we'll say in Reno company.

1:39  
And in fact they are sharing with us the requirements in the in their part.

1:44  
I don't know if you heard about the rescue package.

1:49  
So it's package they are sharing, right?

1:52  
Yeah.

1:52  
In the RFQ you have a lot of requirements for car communication, for diagnostic and we have also files which are related to the cyber security and normally in the beginning of the project, these files are shared with the supplier.

2:07  
So we have the, I think that you know the USFT leader.

2:11  
So we have a 3rd point.

2:13  
And in this SharePoint for every type of project you are storing the entire RFQ package and from the SharePoint, the supplier, it will be after that able to download the corresponding requirements for, for, for, for his project.

2:28  
And by this way we share the requirements for the moment, OK, we don't, we know that it's not really a standard way and we'll work for that.

2:37  
And the only way today to let's say, to be able to, to check if the implementation is properly done on supplier side is managed by a compliance metrics.

2:51  
So cyber security team from from Reno Group, they are creating a compliance matrix, which again you showed the supplier.

2:57  
The supplier will perform implementation testing and so on.

3:00  
And they'll feel their, the, the results in this compliance matrix.

3:03  
And all the time the SPL from Reno Group will be the window person.

3:09  
So the guy which will perform the link between the supplier and the cyber security team from Reno Group, if I should be reported by or did the supplier have doubts about the requirements they SPL will put in contact the supplier and the cyber security team in order to to arrive to clarify all the points.

3:28  
But it's by this way the managing of the cyber security.

3:34  
Yeah, So process, yeah.

3:36  
So here in this process, what I understood is Reno is currently mainly handling all the cyber security related requirements.

3:44  
So currently in HORSE, you are not developing or kind of modifying, enhancing the cyber security related requirement.

3:52  
So is that understanding correct?

3:54  
Yes, OK.

3:56  
For the feature, we intend to also to create our database in let's say maybe indoors only, maybe another tool, but the cyber security team is not yet let's say defined in the HORSE company.

4:10  
OK, So how normally like in current process, so any new function definition will be there.

4:16  
So how you communicate with Renal or so can you just provide some input on how you get that like how the communication start and then Reno provide you the required the cyber security requirements for suppliers.

4:32  
In fact, there are police technical points.

4:36  
I I know that today there are direct let's say meetings between supply and let's say responsible from Reno group.

4:43  
And by this way they also the project team from horse it's involved in the discussions.

4:48  
But they, they are, let's say, not responsible.

4:52  
They are just last they are accountable of the for the for the for the meetings for the moment.

4:59  
I saw that in the first phase of the project there is the USFT maybe which is organizing with these meetings because the cyber security requirements, they are transversal and need to be after that officialized with were shared with all the suppliers for the different type of projects because OK, the cyber security requirements, they are managed in a transversal way.

5:25  
So we're calling, we're speaking about RFQ packages.

5:30  
So now I think that they have write the tariff queued version 16 or 17 and it's clear that if a new project will start now it's mandatory to respect the latest versions of the RFQ package.

5:45  
So in RFQ package those cyber security requirement are in Excel format or it depends because if you want I can share something.

5:54  
Yeah, that will be helpful.

5:56  
You don't know.

5:58  
See I have an example for yesterday one moment option screen.

6:14  
Please, please let me know if you can see my screen.

6:16  
Yes, it's visible.

6:17  
OK, so for example, I have a mail discussion for the SEC OC light topic, which is now requested for our 7 projects.

6:26  
And for example, George, it's out of USFT, but the ECM, let's say for the power train, ECM H ECM software and so on.

6:35  
And I have seen here an example of a standard.

6:39  
So it's a PDF standard which was shared with the supplier.

6:43  
You saw that, OK, it's shared by, you know, group, but they have some more, you know, unique identifiers.

6:50  
We have a title, it's a SQL security specification.

6:53  
And here if you go down, OK, we have the content, they will start after that to present the requirements.

7:03  
OK, here's a definition.

7:04  
I think that's said the end.

7:07  
OK, some details they will, you'll have maybe some technical description of the subjects, OK, explanation of cryptographic notions.

7:17  
And somewhere I think that we need case, they present the side by security concept.

7:23  
And OK, we have also some requirements ID I think that maybe this is something which is familiar for you, you have general requirements, but you saw they are traced in this Excel file, they are not now part of our the door database, OK, So OK, that OEM that even identifier is also like OEM is added, OK and flexibility, OK.

7:51  
And the that document is complex because they are describing all the details about the new concept and so on.

7:59  
Honestly, I don't arrive to to look in details, but I just wanted to you that to have requirement unique requirements, let's say because you have every type of requirement, you have unique ID, there's description of the requirement and the flexibility and I expect, but I think that is not yet created security team.

8:18  
They will create after that also compliance metrics in order to answer the supplier the status or implementation validation for every requirement.

8:27  
And sometimes they are creating also validation plans.

8:31  
So the cyber security validation plan usually is created by the cyber team from from Reno group.

8:37  
OK, so that requirement implementation plan, right?

8:41  
Requirement validation planning validation plan.

8:44  
Yeah, sorry, yeah, I don't know.

8:48  
OK.

8:48  
I have for example, there was an example for compliance metrics.

8:55  
So this again, this compliance matrix, it's created by by the cyber security from from Reno Group.

9:04  
OK, this first part of the table up up to column left is created by by Renault.

9:09  
And after that we have supplier agreement, supplier comment.

9:13  
And then for every requirement, the supplier need to provide the feedback after that OK, if I don't know, it's not agreed, not implemented because you can put OK, not OK or not applicable in function of the status.

9:27  
There will be technical points organized between supplier and cyber security team in order to to agree on the open points, OK.

9:40  
And for every type of let's say cyber requirement in family, they will have a compliance metrics created and they need to be checked.

9:49  
But the for the moment on our side in course there are no they say no additional details what we are doing in parallel because OK, we have words on new request from the no group.

10:03  
In fact they no group requested to horse to be certified from cyber security point of view.

10:09  
And there is a no group created few weeks ago, when in fact in this or group will now will try to say to integrate the cyber security process in our software development process in fact need to be included in fact in all the processes from the group.

10:26  
So starting from, I don't know, design software and tuning, testing, production and so on from our Python software, I know that OK, we need to implement the cyber security concept of.

10:38  
So in our SDR process, we need to have also tools which are compliant with the cyber.

10:44  
We need to include also the treatment of the cyber requirements in the requirement from process management and so on.

10:53  
When looking that for the moment the tools are not yet really adapted for that.

10:58  
I think that maybe it's an open point to be taken to account also for the future.

11:03  
We say tooling platform from from words project.

11:08  
OK, got it.

11:09  
And currently since you're not managing these requirements Renoise directly providing, but since you are accountable for these requirements, so are you we are simply storing that on a SharePoint only or how is it?

11:24  
So are you linking this to the that particular function or for the moment?

11:28  
Yeah, for the moment to explain, they are stored only in the SharePoint of the project from the VSFT perimeter in which you have all the requirements and technical details of for the project.

11:43  
OK.

11:46  
I think that maybe just an open point from my side for this for the future, maybe it will be useful when you have dedicated tools for every type of project to have dedicated to array in order to store all the world the project documents.

12:05  
Because you saw now we speak about requirements and they are stored in a USFT SharePoint.

12:09  
I think that after that they are some project documents there with which are stored in dedicated project sharepoints and so on.

12:17  
But not all the time the files are together and it will be useful to have a unique storing area for all the files for for the project, doesn't matter if they are from the beginning of the project or maybe if we speak about testing records and so on for validation reports.

12:38  
OK.

12:39  
So once horse is going to take care of this cyber security requirement, so you need to completely develop these requirements.

12:50  
And now then the the requirement sharing with the supplier that horse is going to perform, right and that matrix validation like compatibility and the compliance matrix creation testing so that all parts supplier is going to perform and based on that you are just going to capture or validate those results.

13:13  
Yeah.

13:14  
And in fact maybe there is also an additional points sometimes for the cyber security implementation.

13:20  
So if we realize that for example, we need to perform a develop, I don't know a new logic in our diagnostic applicative parameter, for sure in this case, we will create a change request and we'll follow follow ECDR process.

13:35  
OK, So sometimes you have the chance to have a traceability in our internal tools.

13:40  
But in most of the cases we speak only about the traceabilities for the physical updates in our applicative software.

13:48  
But if the entire cyber security development will be made in the supplier basic software, in this case there will be no VCDR process and so on.

13:58  
Because the whole, the whole the, the traceability of the update, we consider that is just managed by managing the compliance matrix.

14:06  
And OK, got it.

14:11  
And I think that maybe Alex can correct me because we are facing similar issues also on the ETC projects.

14:18  
And I know that also with ETC supplier we are sharing requirements.

14:23  
And after that, I think that the implementation is just monitored in some compliance matrixes.

14:30  
Yeah, it's just so the the review and agreement.

14:37  
And yeah, the follow up on the implementation is done through an Excel file with comments that are, let's see, followed, completed traced by Breno and supplier, but it's through Excel file.

14:58  
OK, So getting in one question, how you make sure that this test case, sorry, requirements are validated with appropriate test cases.

15:14  
In fact, today 1:00 is stating that on our side and whole side there is no, no control on confidence.

15:19  
So all the time we are relying on the list say the the profes provided by the supplier because the north side there is no testing team or validation team in order to prove that everything it was well implemented and so on.

15:37  
So we don't have we don't have the teams and we don't have also the competencies inside words to let's say to deal the cyber security topics.

15:45  
OK.

15:45  
You mean to say all these test cases are written by supplier only and Reno team validates it?

15:53  
In fact, I think that the test case sometimes are done in by the Reno group.

15:58  
They are provided, they are creating validation plans, they are shared with the supplier and the supplier will perform the the the test and provide the result.

16:07  
OK.

16:08  
And who is doing the Tara analysis?

16:10  
Is it Reno team or supplier, I don't know.

16:16  
Yeah, because writing that we have some safety, we have a safety team phone or can you please repeat the question please?

16:26  
Sorry, it's Tara analysis is a threat analysis just like Hara for cyber security you do the threat analysis.

16:36  
So, so it's a Tara, Tara analysis.

16:39  
And if Reno is giving you requirements, hopefully they should be doing it, but don't know in your case you are passing it to supplier.

16:50  
So might be supplier, yes, I can ask that, but at least I can give the example of ATCU.

17:02  
Yeah.

17:03  
On ATCU, we are providing them the safety requirements.

17:09  
But on an expert level on our side, we need to define some use cases and is there a responsibility to to check our but I will confirm that I will ask now because we have some topic, we have some topics with them and it is on on their side.

17:36  
Yeah, OK, OK, good.

17:38  
And you just said that you are in the process of developing this process inside host.

17:45  
So are you looking or maybe have you evaluated any tool or application to handle cyber security?

17:56  
Not yet, but I just I can share with you.

18:00  
So what we have in our first action plan.

18:03  
And for example, as you can see also for the the Tara effect, we have an actually in order to create new house the the Tara files, OK, we have a team from Spain which is helping us to perform this to prepare this audit for the cyber security certification.

18:23  
They will help us to say to to create the process and to update our existing standards.

18:29  
But honestly we don't have discussed up now about also dedicated to need, but maybe to be an open points to be kept in our say monitoring list for the discussions with the tools providers.

18:49  
OK.

18:53  
Yeah, so many of the LM tools has that capability to manage Dara.

19:00  
OK.

19:00  
That can be considered not a problem but definitely yeah, we understood that you are working on it.

19:08  
May be we can note this point and we'll see if ALM tool can thoroughly do the analysis, Taara analysis and give you the result of that particular exercise.

19:22  
OK, Yeah.

19:28  
Anything else you are looking as a process or maybe any understand you are working on it and the process is not yet established, but maybe from the future perspective what exactly you are looking for means what will help you out to address the current challenges?

19:50  
Well, I think that for cyber we don't have maybe a particular less expectation.

19:56  
The main idea is to include those is to be sure that the cyber.

20:01  
It's also part of our regular process.

20:03  
So to be included in all our, let's say all standards, productivities, domains and so on.

20:10  
But we are just in the beginning of the part because so that we are just analyzing the current processing.

20:16  
You are just trying to understand in which perimeter and in which domain.

20:21  
In fact, we need to to start to update the the rules in order to to be, let's say, cyber security compliant.

20:31  
OK, Maybe in this case you'll just, we'll useful for us to to just to share with to share with us your experience on the on the cyber security part and maybe to be just use the in the future discussions with the the the tools providers.

21:06  
Yeah, definitely.

21:07  
So our final aim is to see how this cyber security, functional safety requirements are integrated with your main functional requirements.

21:16  
So that will be easy for all the groups to manage the requirements with proper test cases and give the traceability of these requirements and test cases.

21:27  
So that is the use case we have considered here.

21:31  
Yeah, opportunity as you already saw that up to now on our hey, still I say in our safety activities, this cyber security, it wasn't included.

21:43  
So I think that we need to treat maybe at the same level the safety and the cyber security part, correct, Correct.

21:54  
Yeah, Vijay, go ahead Now if you have any other questions, Yeah, I think here since that complete process is not managed of the other part, we understood maybe Sushant, do you have any specific question?

22:09  
No, we already discussed this point.

22:12  
So yeah, maybe just one addition info from my side.

22:17  
So from the current discussion from those workgroup for cyber security, we know that the main idea is that we need to create cyber security process or include the cyber security in our regular process until week 35.

22:33  
Yeah, definitely, definitely.

22:34  
Because when you are going to work with other OEMs as well.

22:39  
So you're planning to go for going the market with the other OEMs, right.

22:43  
So there generally the expectation is that you are a cyber security compliant, you are functional safety compliant, you are a SPICE compliant.

22:53  
So you have to have those process established inside host.

22:59  
And if if you use the tools, I think this tools also help you to do some kind of compliance with with this process because they are these tools are also cyber security or function safety compliant.

23:21  
Yeah.

23:21  
So that will definitely help you in establishing the process.

23:34  
Yeah, OK for me.

23:36  
Yeah.

23:39  
So anything else you would like to highlight?

23:43  
I'm on my side now.

23:46  
OK, maybe Alex, any view from your side?

23:56  
No, no.

23:58  
OK, thanks.

24:01  
Vijay, are we OK?

24:03  
Yes.

24:04  
Maybe we can conclude the session.

24:06  
Yes.

24:06  
So thanks, Alex and Caroline for your inputs.

24:12  
Thanks for your information.

24:14  
So based on this discussion, we'll try to plot the use cases for cyber security, which will be helpful for you and can be managed in the ALM tool.

24:25  
So based on that, we'll, we will evaluate the ALM tools and if any additional input is required from your side, we'll definitely come back to you through Steven, of course.

24:40  
And if you want to highlight any other point which you missed out, I believe or maybe may not be, but if you remember after this meeting that OK, this point should have been brought into the team.

24:51  
So teams meeting.

24:53  
So you can write to Stephen and he will communicate with us accordingly.

25:01  
OK.

25:04  
And Stephen, after this call, maybe once you get a chance, please upload the record.