IN THE DISTRICT COURT OF OKLAHOMA COUNTY
STATE OF OKLAHOMA

Jean Bookout; Charles Schwarz, individually and as Personal Representative of the Estate of Barbara Schwarz, deceased; Richard Forrester Brandt, as Personal Representative of the Estate of Barbara Schwarz, deceased,	)	
Plaintiffs,	)	
vs.	)	Case No. CJ-2008-7969
Toyota Motor Corporation; Toyota Motor Sales, U.S.A., Inc.; Toyota Motor Engineering and Manufacturing North America, Inc.; Aisan Industry Co., Ltd.,	)	
Defendants.	)	

* * * * *

TRANSCRIPT OF AFTERNOON TRIAL PROCEEDINGS

HAD ON THE 11TH DAY OF OCTOBER, 2013

BEFORE THE HONORABLE PATRICIA G. PARRISH,

DISTRICT JUDGE

Reported by: Karen Twyford, RPR

***** THIS TRANSCRIPT HAS NOT BEEN PROOFREAD *****

APPEARANCES

For the Plaintiffs:

Mr. Benjamin E. Baker, Jr., Attorney at Law
Mr. R. Graham Esdale, Jr., Attorney at Law
Mr. J. Cole Portis, Attorney at Law
Mr. Jere Beasley, Attorney at Law
Beasley, Allen, Crow, Methvin, Portis & Miles, P.C.
218 Commerce Street
Montgomery, Alabama 36104

Mr. Larry A. Tawwater, Attorney at Law
The Tawwater Law Firm, PLLC
14001 Quail Springs Parkway
Oklahoma City, Oklahoma 73134

For the Defendants:

Mr. J. Randolph Bibb, Jr., Attorney at Law
Mr. Ryan N. Clark, Attorney at Law
Lewis, King, Krieg & Waldrop, P.C.
424 Church Street, Suite 2500
Nashville, TN 37219

Mr. James A. Jennings, Attorney at Law
Mr. J. Derrick Teague, Attorney at Law
Jennings Cook & Teague
204 N. Robinson, Suite 1000
Oklahoma City, Oklahoma 73102

(Whereupon, the following trial proceedings were had on the afternoon of the 11th day of October, 2013, to wit:)

MR. CLARK: Your Honor, I have one of them. I've got Mr. Ishii's CV. Plaintiffs have it numbered as 3104.

THE COURT: So you want to make it Plaintiffs' 3104?

MR. CLARK: We agreed to introduce it in lieu of hearing any more of his qualifications.

THE COURT: Okay. I will introduce it as Plaintiffs' Exhibit No. 3104.

MR. CLARK: I think that was probably a good agreement.

MR. BAKER: We offer 3108. That is the only one that we will offer.

MR. CLARK: Your Honor, at this point we have foundation and 403 objections to that because of the amount of testimony from Mr. Ishii that he couldn't understand things in there. I think once Mr. Kawana has testified we won't have additional objections beyond the ones that the court has already ruled on. That hasn't happened yet.

THE COURT: Is Mr. Kawana going to testify?

MR. BAKER: Your Honor, he testified to Mr. Ishii that is a Toyota document from a Toyota presentation as a corporate representative, so that sets the foundation that we need.

MR. CLARK: However, the fact that it may be a Toyota document does not take care of the 403 issue.

THE COURT: The relevancy?

MR. CLARK: This issue is that there is a variety of testimony from Mr. Ishii that he doesn't understand some of the things in there. I think we need to hear from Mr. Kawana because it goes to the jury.

THE COURT: Is Mr. Kawana going to testify?

MR. BAKER: I doubt it. You already ruled on this in motions in limine that it would be relevant.

MR. CLARK: Well, we didn't know who was going to testify at the time she ruled on the motions in limine.

THE COURT: And this is the document that he testified about was prepared by Toyota and did all the testimony at the end of his deposition?

MR. BAKER: Yes.

THE COURT: Then I will admit over your additional objection, and your other objections, Plaintiffs' Exhibit No. 3108.

(Whereupon, the jury returns to the courtroom.)

THE COURT: We're back on the record in Case No. CJ-2008-7969. Mr. Koopman, you can come back to the stand. Sir, you're still under oath. And Mr. Portis, you can continue your direct examination.

Q (By Mr. Portis) All right. When we left for lunch

-- have you ever taught after lunch before?
A I teach every week after lunch twice. It's tough.
Q All right. Well, I want us to talk about this very briefly just to get us back on point. Any safety critical system with a single point failure is unsafe; is that true?
A That is correct.
Q It is defective?
A Yes, it is defective. Specifically as a defective design.
Q And describe for us briefly how you get rid of the single point failure.
A The only way to get rid of a single point of failure is to have two pieces that check each other or take over for each other. You have to two completely independent ways of making the system. If there is any shared resource, anything shared, then it is unsafe.
Q And that's where you got into that picture back there on the jet engine, right?
A Right. On the jet engine, what was shared was the computer on one engine could turn off both fuel pumps so that was the single point of failure.
Q Now, your opinion that a single point of failure is unsafe, is that shared in the academic community?
A Absolutely.
Q Is it clear that at the time that this software was

designed on the 2005 Toyota, prior to 2005, that the single point of failure existed?

A I'm not quite sure what you mean by "existed."

Q Okay. Was it part of the system designed into the system, the 2005 system, would that have been before the car was actually manufactured?

A Yes. It was -- part of the design process was to design a system which has an inherent single point of failure. And then all cars manufactured would have that same single point of failure because it is a design defect.

Q Now, you say this and then I want to go to the next slide. And I think maybe here you say NASA agrees that the ETCS has a dangerous single point of the failure. Do you see that?

A Yes, I do.

Q That is one of your opinions, right?

A Yes. That is my opinion.

Q And on the next slide, that you have you talk about a fault tree analysis.

A Yes.

Q Why did you do that?

A What I would like to do in these few slides is to give a more detailed rigorous way of explaining what I mean by an arbitrary fault and how single points of failure work. So when you analyse a system for safety, and this

can happen during design, or this example is actually a NASA accident investigation.

One of the techniques is called a fault tree. What you do is you say, Here is a bad thing that could happen. In this example it is a spacecraft that lost a bunch of fuel, but in this case it might be unintended acceleration. And what you do is you go down and there are "or" gates and "and" gates. This is just computer terminology. What you're looking for is anything at the bottom like a bad algorithm or a corrupted data structure.

You see it only goes -- any one of these can cause a software problem. Any one of these software or hardware can cause a computer error. Any one of these can cause the bad thing. So to make a system safe, you need at lease one and gate between the top and the bottom to make sure that two different things have to go bad.

Q You said you need at least one?

A And gate.

Q And, A-N-D?

A Both have to fail. And if you don't have that, then you have a single point of failure. One thing failures, the whole thing goes bad. In this spacecraft, they actually had a software problem that wasn't mitigated and they almost lost the mission.

Q All right. What is a fault containment region?

A So a fault -- this ties into a fault containment region, and I will tie these two concepts together quickly. A fault containment region is a part of the computer, typically computer hardware, that a fault outside it can't affect inside, and a fault inside can't go out. So it is a barrier that if a bit-flips or there is a software defect, this barrier keeps all the bad stuff in so it can't corrupt something else. It keeps all the bad stuff out so it will keep working.

Q Hence, the word containment. In other words, your fault is contained in a specific region so it doesn't corrupt everything; is that right?

A Right. It is a big mote, nothing gets across mote, particularly no faults get across the mote. Good data gets across but not false.

Q And false tolerance requires having more than one fault containment region; is that fair?

A That's fair. Once a fault happens, it can do anything that it wants inside but it can't affect another one.

Q So what is the problem with the Toyota design?

A Even though they have two chips, both chips are in the same fault containment region. So a safe design would have two chips, and each one is its own fault containment region. What you do is you would have separate inputs.

Because no one has ever made a CPU that doesn't fail.

A safe design has two inputs. Each fault containment region has its own input, and then they cross check against each other. This means a fault in one can't affect the fault in another.

Q Now, we heard Mr. Ishii say that Toyota had their own standards that they follow, right?

A Yes. We heard that.

Q And when he says that, if they allow, if their standards allow there to be -- for there not to be redundant fault containment regions, would you say that is acceptable in the industry?

A I would say it is unacceptable and leads to unsafe systems.

Q Would that be contrary to MISRA?

A Yes, it would.

Q Contrary to any other standards?

A It would be contrary to every safety standard that I've ever seen. So in order to build a safety critical system, you need two fault containment regions so that if one of them messes up, it can't affect the other one. Each one has to have its own set of inputs because you can't trust the other guy to tell you the truth about the inputs.

Q Well, you notice up here you use the word critical?

A Critical. Yes.

Q Is redundancy required for noncritical systems?

A Redundancy -- well, let me clarify critical. Critical means safety critical. There is a broader concept that maybe if you have a economic loss, like a chemical processing plant blows up but no one is hurt, it is still a critical system, so you see it is used there as well.

But in a critical system, if you're critical that there is an unacceptable loss if there is a system failure you have to have two fault containment regions or you don't meet the accepted practices.

Q Now, this diagram right here, can you describe how these two computers cross check everything.

A This are several ways that can cross check. This is how the rails guys do it, this is how the chemical processing guys do it, the aviation guys do it this way. What they do is they take the inputs. The first thing they do is they say, Hey, I have got this value of an input, what did you get? And they exchange the input values. And either one of them can say, What I saw isn't what the other guy told me.

It is common in these systems if you see one input the other guy tells you something else, you kill both of them. They both take each other out, and the system does a shutdown or it reverts to another pair next to each other to resume operation.

Q Let's be specific here. Let's talk about a Toyota UA event.

A Okay.

Q If this system was in place, how does it work?

A So it would look at the accelerator pedal. If the two inputs from the accelerator pedal weren't within a very small difference of each other, because nothing is ever perfect, if they work -- I will just make up some illustrative numbers -- if one input said 15 degrees and one said 16 and one are assuming one degree is okay -- I'm not opining on that -- then they would say, Oh, mine is 15, you said 16, close enough, we're good.

And the other guy said, Mine says 16, but you told me 30. Sorry. That's not right. I'm going to shut everything down. Also with the throttle position, it also is duplicated. And if the throttle position doesn't match, it would shut everything down.

So what they do is they periodically run an internal computation and if what they think is going on doesn't match, they shut everything down.

Q What do you mean by shut everything down?

A Typically they would reset both processors, depending on the system, they would reboot and try to restart or in some systems like rail system, they shut themselves down, and a person has to come and restart them.

They can do that on rail because they have another pair next to it, and the other pair takes over.

Q Is that a safer system?

A If you shut down and require manual intervention, it is safer if the system is safe when it stops. In an airplane engine, you try to restart them. And a rail switch, you just shut them down.

Q All right. And I guess my question is: This is the way it should be designed to be safe?

A This is the only way I know of designing to be safe. Or the only alternates have three processors or four processors or more. This is the simplest way to design it to be safe.

Q Turn to the next one, please. You they the simplex fault continue systems are not safe, and that makes my brain hurt. But what do you mean by simplex fault containment systems are not safe?

A Simplex is a term of art that people use to mean there is only one as opposed to duplex. You have heard of a duplex house, that means two. Simples just means one. This is another way of saying in more technical language if you have one fault containment region where any fault inside can do whatever it wants to make the system unsafe, then that is not safe, you need two.

More specifically, let me tie this back to the

fault tree. When you have all the software in a system in one fault containment region, and that fault tree has a bunch of things going on, the and gates don't help you because it is both happening in the same CPU, so there is no way to say these are two independent things. The and gates only work if they're independent. If they're not independent, you're not safe anymore.

Q Is this the Toyota system?

A The Toyota system, we will get to some pictures, is a simplex architecture with some built-in tests, it is not duplex. And duplex is the minimum requirement to be safe.

Q What is the purpose of what you highlighted here?

A This is -- so NASA, in their report, referred to this Hammett paper to define some terminology.

Q I see that is mentioned here and it is 2001. Is that when that paper was published?

A That is my understanding.

Q You're telling us that NASA referred to the Hammett paper?

A Yes. NASA explicitly referred to this and used language out of it. So my impression is they referred to it to make sure we understood what the words meant.

Q What do these words mean?

A The aerospace guys, I do some work with some aerospace guys, and they all use these terms. They say

failure passive means that the thing shuts down and there is an assumption that it is safe.

Fail active is a malfunction. So when you fail active, it means it does the wrong thing and the presumption is that it's dangerous. So if you say this system fails active, what you are saying is it is unsafe. And the paper spells it out. In some systems, it maybe okay if you lose function an failsafe, but a malfunction can be catastrophic. And that is my experience as well. So fail active is bad.

Q And your next page continue on, right?

A Right. These are some more pieces out of the paper. And NASA references this, so I'm going to the pieces they reference. So a simplex disengagement feature, in the NASA report they said it was a simplex with disengagement. So that means a single computer. And this exactly corresponds to my understanding of the Toyota system.

So what you have is a computer with BIT. BIT is built-in self test. And that maps to the failsafes. So you have a computer, and it is computing along and something goes wrong. You can put in a bunch of countermeasures to say, Well, let me check myself here, let me check myself there, and let me check myself there. But no computer has ever been made that has a single fault containment region, can't check everything. There is

always something that can get by you.

I know when I write a paper and I proofread it, I don't care how many times I proofread it, there is still a typo in there somewhere. Nobody can check their own stuff. It is the same thing with computers. This BIT helps some because it catches a lot of the faults, but it can never catch all of them. It is just not possible.

Q You talk about this BIT cannot check all faults.

A That's right.

Q Is the standard in the industry that you must check all faults?

A The standard in the industry is all single point failures have to be accounted for. That means all faults in a single fault containment region.

Q Okay.

A And in the paper it says maybe it catches 19 out of 20, but one in 20 are left over. So that's why they have this table. So this table sort of sums it up. If you have simples with no built-in self test, well, that's easy, it does whatever it wants to with the fault. With built-in self-tests or failsafes in the Toyota system, this is their system, it will turn itself off much of the time but not all the time.

Q And this right here is the Toyota architecture?

A Figure 5 is how the Toyota architecture shows up in

this paper. Yes. I think that's a fair representation.
Q And here is what you referred to earlier. What is that?
A That is a self-checking pair. And that is this picture right here. So that's --
Q Okay.
A -- the two fault containment regions, they check each other. This is all standard terminology. People have known that for years, and this is a good paper that NASA referred to to explain it. What it says is that simplex with built-in self-test is after most failures it fails safe, but after some failures it's going to failure unsafe.
Q NASA says this?
A This is what Hammett says, and NASA uses the Hammett words to describe. The system refers to it quite explicitly.
Q Hammett says this, and NASA refers to the Hammett report.
A Here is the NASA language. It is a prime system, is a simplex system. A wimples with disengagement monitor, reference 14, and 14 and 14 is the Hammett paper.
Q So NASA -- this is NASA language?
A That is NASA language out of their report.
Q And they're saying that the system appears as a simplex system with disengagement monitor and diverse

safing, correct?
A That's correct.
Q Is that the unsafe?
A That's unsafe.
Q Is it defective?
A It's defective.
Q The simplex system, go to the next slide. You mention that the simplex system that Toyota uses -- and we talked about A/D. Remind us what that is again.
A That is analog to digital conversion, voltages into bits.
Q Tell us what you mean by this slide.
A By this slide, there is a single shared A/D converter, but the fact of the matter is that both chips together are the same fault containment region, there is no good isolation. They are not a good self-checking pair. They send data back and forth through a lot of failsafes, but it is not perfect coverage. In particular, something disturbing is the failsafes run on the same processors that are doing the computation.
Q Why is that disturbing?
A Because you've got the same thing that is doing the computations seeing if it made a mistake. Well, it if made a mistake on a computation, why on earth would you believe that it will get it right, the failsafe? Once it has made

a mistake, all bets are off.

Q Your next opinion here is that Toyota's methods to ensure safety were themselves defective; is that correct?

A That's correct.

Q What do you mean by that?

A What I mean is that you need to use a rigorous engineering process to be able to build safe systems, and their engineering process was defective.

Q You mentioned in support of this idea of MISRA, set by the MISRA automotive safety recipe. Again, that is the big, thick document?

A That is the big book. Right.

Q Okay. What do you mean by this MISRA is a recipe?

A It's -- we're going to go through that in some detail in slides, but it tells you what you need to do to be safe at great length. There is a summary I can show you that says, Well, these are the kinds of things that you need to do. It has everything that you need to know, all the accepted practices for building safety.

And I want to point out that my wording is rather precise here. I'm not saying that they had to follow MISRA itself. They had to do something that was just as good. MISRA is good. If they had done one of the other standards, I might still be happy, but they didn't do anything that meets this level. So they didn't go good

enough, as opposed to nitpicking them on individual practices.

Q Well, at the time, prior to the development of the 2005 Camry, were there even more rigorous standards than MISRA?

A There were several standards that I would consider more rigorous.

Q What do you mean by that?

A They required you to do more things. For a given level of safety, you had to do more engineering, more steps, more checks to meet that level.

Q So is it fair to say if they don't meet MISRA they didn't meet even more rigorous standards?

A If they don't meet MISRA, they don't meet any of them. I think that's fair. And in my opinion, I don't think there is any of them they would meet.

Q And I know we will not go through the entire MISRA document. Tell us what you emphasized here.

A This is a document. It has a main document that says here is a methodical way to design safety critical systems.

Then there is nine reports. And the reports are specific to things like for software integrity, and for how to do hardware. There are different aspects so if you have a team each part of the team might get one of the reports and

concentrate on that, and the main documents is overarching.
Q Mr. Ishii said in his testimony that Toyota had their own code software standards?
A He was talking about the MISRA-C standard, which is the small book.
Q Okay.
A And I don't recall him saying that they had a standard like this that they were following. He was just talking about the style.
Q And you make a good point. Based on Mr. Ishii's testimony, where -- the big thick book -- he didn't even mention any standards related -- any standards similar to MISRA standards, did he?
A I did not catch any references to anything except the C standard. I did not catch any reference to this standard.
Q And the difference between this MISRA, this big MISRA report and this smaller one here, is what?
A The smaller one is very specifically ways to use the C programming language in a way that is safe, and the bigger one is how to design an automobile with software that is safe.
Q So not only should they meet the standards -- am I correct, not only should they meet the standards is the large MISRA book,, but also the standards in the MISRA-C

book?

A Yes. In fact, we will see that on a chart in a moment.

Q All right. Tell us what this is.

A This is a list of safety standards that follow a thing called a SIL, safety integrity level, and this is sort of the main concept in the safety standards. And I have done at least some work with all of these at some time or another. A big one at the time of MISRA is IEC 61508. And I know that at least some car companies were looking at using that standard as well as MISRA back then. The newer standard, ISO 26262 was a new automotive standard.

MR. BIBB: Objection, your Honor.

THE COURT: Approach on this one.

(The following bench conference was had outside the hearing of the jury:)

MR. BIBB: I thought there was a ruling about ISO 26262. That is the one that didn't come into effect until November 2011.

THE COURT: I do remember discussing it in one of the motions in limine.

MR. BIBB: I can get into standards that were in existence at the time this car was manufactured. That is --

MR. PORTIS: I wasn't here for that one.

MR. BIBB: I think if we just move on we will be fine.

THE COURT: Okay.

MR. PORTIS: If I get it in, I will have to lay a predicate for it?

THE COURT: I think I already ruled. Right now I ruled that it was a standard --

MR. PORTIS: Unless I lay a predicate for it. And I may not be able to.

THE COURT: Right now, do not use that chart anymore.

MR. BIBB: We can go to the next slide.

MR. PORTIS: Sure.

(Within hearing of the jury:)

Q (By Mr. Portis) We'll go onto the next slide. I may come back.

A Okay.

Q Hold on a second.

(The following bench conference was had outside the hearing of the jury:)

MR. PORTIS: Judge, what I'm going to ask him about related to the ISO 26262 standard, was that information available in draft form prior to the manufacture of our vehicle.

THE COURT: Okay. Was there --

MR. CLARK: I think what the court's ruling was last week was he didn't show what knowledge Toyota had about it, not whether it was available or not, which Toyota had. I'm not sure if I can make it a --

THE COURT: I think he can at least testify that it was in a draft form at that point. Isn't that what they're saying?

MR. PORTIS: Right.

THE COURT: Are you just basically going through the different kinds of standards that were available during 2005.

MR. BIBB: This one was a draft.

MR. PORTIS: It is a draft of a standard, though, that are more rigorous.

MR. BIBB: Just because there is a draft of a law out there doesn't make it a law.

MR. BAKER: IEC 615108 existed in the '90s.

THE COURT: He already talked about that. He didn't object to that.

MR. PORTIS: ISO 26262 is just an adaptation of that standard.

THE COURT: But if it didn't exist in 2005 --

MR. BAKER: But there is going to be testimony that they were aware of it. In fact, they were on the committee for ISO 26262, Toyota was. They knew about the

draft. I've got the document to show it.

THE COURT: You have a document that Toyota knew about that?

MR. BAKER: Yes, ma'am. It is a 2005 document that shows this.

THE COURT: Does someone have my ruling about what we talked about?

MR. CLARK: I think what you go on is line 18 are where ever your comments start.

THE COURT: Okay. So yes. What I said is I need to reserve whether I will allow it in until I see it Toyota was, in fact, aware of the drafts.

MR. PORTIS: Yes.

THE COURT: So with this witness obviously it can't happen because we don't know yet. Do you have a Toyota witness that is already addressed this?

MR. BIBB: No.

THE COURT: Do you have something that you can show me it is going to come into evidence?

MR. BAKER: We have some documents that we quoted in our briefs. It is in Japanese. I'm not sure I have it here. It is a 2005 document where Toyota is talking about the ISO standard in 2005.

MR. CLARK: This is the one that I said I've never seen in English.

MR. BAKER: I don't think this is a big enough deal to stop.

MR. ESDALE: We will move on.

THE COURT: After all of that, just move on.

(Within hearing of the jury:)

Q (By Mr. Portis) Now, we were talking about standards, and there were a list of --

A If I can summarize without mentioning that one standard. The common aspect they all have is they have a thing called a safety integrity level. You can decide how critical something has to be, and then you pick practices. All of those standards have that flavor, and they all have sets of practices that are kind of similar, some are more rigorous than others. 61508 was one at that time that was more rigorous than MISRA. But if you followed MISRA, that was accepted practice as well.

Q And you say that Toyota should have adopted MISRA?

A They should have adopted MISRA, or they should have adopted something that is roughly comparable. So this is a paper from 1997 where they are talking about be compliant with a sector standard. If you're automotive, the obvious choice is MISRA. But if you want to pick another standard and make a case that it is more applicable to you, that's okay too.

Q But Toyota says they picked their own standard, they

picked their own internal standard.

A To be precise, the standard they were talking about was for code use languages. And I've not heard them talk about a standard of -- a safety standard as such. That is a much narrower statement, I believe.

Q I hadn't either, but let's assume that they did. Let's assume that it wasn't related just to the code language, but they had their own internal standard what is the problem with having internal standards?

A If you have an internal standard, it's -- the onus is upon them to demonstrate that it is as good as the public standards, which have had scrutiny from people all over the world and had buy-in that this is appropriate. The standards I've seen are not like the MISRA software standards.

The only standards I've seen from Toyota are very, very narrow coding standards.

Q All right. In this -- real briefly -- in this MISRA safety integrity level, in the MISRA itself, if they wanted to -- when did MISRA come into effect?

A That was '95.

Q '95. So in 1995, ten ears before our car was manufactured, if Toyota had wanted to build it safe according to MISRA standards, were those available for them to look at and to follow?

A Yes, they were.

Q Now, you mentioned earlier MISRA safety integrity levels. And I see over here on the side integrity level 4, 3, 2, 1, 0. What is an integrity level?

A So an integrity level is the idea that depending on how bad an outcome can be you need to pay more attention. If you're making a product that at worst is a paper cut, you don't have to spend the same engineering resources getting it right as something that can kill somebody. And this is a way to methodically say it starts with zero up to four. And these same numbers appear more or less across all the standards that's why I showed that slide.

It is a common idea that four is the highest level of integrity. And that means this is something where, very loosely speaking across all the standards. If it's cell four, what that means is if there is a defect, if it is not designed right or there is a runtime fault, that probably you will have a large, large accident in which quite a number of people die, that is an expectable outcome.

Three is more like, well, if this will misbehaves for some reason, then it's pretty reasonable to expect one or two or three or four or five people to die but not a whole plane full of people. Down at two, you can expect people to be severely injured, but you would be kind of surprise if someone died, it would be a freak event. And

down at one, fender bender. So that is a lose way of describing it. If you go to MISRA book, you will find wording to this effect.

Q So the higher the integrity level the greater the idea that it's safety critical?

A The higher the integrity level the more safety critical it is; therefore, the more rigorous you have to be to make sure you get it right.

Q And was this ETCS of Toyota, was it a safety critical system?

A It was a safety critical system, and I would put it at cell three.

Q On the next page, you mentioned Leveson. What is that about?

A So this the original software safety research paper, and she is defining safety critical systems are those that can directly or indirectly cause or allow a hazardous system state to exist. And safety critical software is software in such systems. And the ETCS is clearly a safety critical system.

Q And Toyota agrees, right?

A And Toyota agrees. Well, that deposition quote has them saying yes to that question.

Q And Mr. Kawana is a Toyota employee?

A That is my understanding. Yes.

Q I want you to go to two more slides there. This is what MISRA says is required for SIL-3 software development?

MR. BIBB: Objection. Leading.

THE COURT: Overruled.

Q (By Mr. Portis) Tell me about this document.

A This is a summary out of the big MISRA book which is a summary of part of the recipe for getting it right. And so if you have a cell three system, you have to do everything inside the yellow. For cell three, everything in this column and everything in the column two and everything in the column one.

As an example of just one item, it says a restricted subset of the standardized structured language, the small MISRA document, MISRA-C, is the restricted subset of the C programming language. So you have to follow that document as cell two, which is only going to injure people not kill people. And for cell three, you also have to follow it. It is all these other things that you have to do on top of that. That was the distinction that I was trying to make.

Q Did Toyota follow -- is there another page?

A That is the top half, then there is the bottom half. There is a bunch more things that you have to do.

Q We have testing, we have verification and validation, access for assessment. And prior to that was

specification design, languages and compilers, configuration management processes. Did Toyota follow one, two and three of all of those standards?

A My opinion is they did not. For example, the specifications are not formal. You recall Mr. Ishii was asked about whether he had formal specifications. And the answer, as I understood it, indicate a no. And the reason is the word formal means mathematical. You actually have to write the specifications out in mathematical notation to be formally specified. And that wasn't his answer, and I have certainly never seen such documents from Toyota.

The language, they did not follow MISRA-C. Configuration management, this is making sure you can go back and get whatever tools and whatever software you want whenever you want it. And Mr. Ishii also said they didn't use it.

For testing, the part of testing is coding rules, and they did not meet the coding rules, and they did not formally document deviations. So in the MISRA-C code it says if you are not going to follow the rule, every time you don't follow it, or for each class, you have to say why, and it has to be in writing.

For validation, the reviews were informal and only some modules. So you heard testimony they only looked at some things, the things they were concerned about. World

safety critical software, you have to look at everything.
Q So just to put it in context, prior to the manufacture of the -- even the vehicle involved in this case, 2005 Toyota Camry, Toyota did not follow the guidelines required of MISRA or SIL-3, correct?
A That is correct.
Q All right. Let's go to section 6.
A Okay.
Q You mention in your opinion three that Toyota safety culture is defective?
A That is correct.
Q That's a -- why do you say that?
A Let me start by defining safety culture. Safety culture is how the employees and the management treat the concept of safety. Either safety is at the top of the list always, or it's not. And we read about big catastrophes and big problems like the space shuttle Challenger and things like that, when you dig down far enough, what you find out is the safety culture was broken. And because of that, people took short cuts and people made mistakes, and there was a big loss.
Q Tell us why it is important that there must be an emphasis on safety that permeates an organization like Toyota.
A If you put things above safety, then people are

incentivised (sic) to take shortcuts, they skip process steps, they go through the motions instead of doing it for real; that's how you end up with unsafe systems. Most of the case studies come down to that people weren't taking safety seriously and sure enough that led to an unsafe system.

Even if they did try to follow a standard, if you don't take it seriously, it's not going to do you any good. If you define rules and you don't follow them, you're not going to get safety.

Q Well, let's look at Toyota. Toyota, what they were missing. Describe this particular document.

A So this is a document, it is from 2007, but my understanding is it reflects processes that were in place through 2007. They sat down and said, There is a processing place for hardware but not for software.

And this is a classic V diagram, this is how most automotive companies design software. They take a high-level specification and they refine it to details to write code. And going up the other side, they are making sure that each step got done right.

Q What is your concern with it?

A My concern is it's marked. And these are their markings. The only thing that I put in here it was this yellow highlighting.

Q The only thing you have done to this document is add --

A That yellow highlighting. These boxes were all there. And they have an X saying no knowledge at Toyota for all of these boxes. And these are the kind of module inspections, software binding inspection. So these are all the things to make sure that your engineering process was executed correctly. And this document says no knowledge at Toyota, so I find that very concerning.

Q Why is that concerning to you as a computer software engineer?

A When you are doing software safety, it is important to do checks and balances. No one person should be able to make a mistake without it being found later, because people make mistakes, right? That's what they do, so you have to have checks and balances all the way up. It says here Toyota didn't have knowledge in those areas, so they were getting software and they were getting an operating system with no assurance that it was useful for safety, and they were not checking it themselves, and they didn't have the capability to check it themselves.

The same thing, the Denso code, they didn't have the capability to check it for themselves, and they didn't have an independent certification saying that somebody outside had checked it for them.

Q You mentioned a name right now that had not been mentioned before, and that is Denso. What is their involvement with Toyota?

A Denso is the company that actually did the low-level design as a supplier to Toyota.

Q And is that common in the industry?

A That's common in the industry.

Q What is Toyota's responsibility related to the Denso work?

A In a standard, in a MISRA type setting or a safety critical type setting, their responsibility is to ensure each component they get is safe. And there are several ways you can do this. You can check it for safety yourself, although this chart suggests they didn't have that capability; you can have the supplier document and convince you that they did it, but o do that they not only produce the code, but all the audit trails and all the reports, we did a peer review, we did all our things, here is our paperwork to prove to you we actually followed the process we're supposed to follow; or as was common in 2002, I was involved in one of these, you would have an independent company come in and do the audit for you and you would believe their report.

Q Let's talk about the ETCS and whether or not Toyota took the electronic throttle control system seriously.

A Couple of the documents I've seen, the first one was a letter to a customer which said for the accident to occur -- and this is a customer complaining of the UA event -- as reported, two totally separate systems, brakes and throttle, would have to fail at exactly the same time, and this is virtually impossible. The brakes will always override the throttle.

And my understanding is to do vacuum depletion that is not always true, although other experts will testify in more depth about that.

Q What else did you have?

A The other one, this is a deposition of a Toyota employee whose job it is to take car that have had reported problems and see what happened, see if the car is defective, something wrong with it. And he was asked -- and there are several pages, but this is the heart of the matter -- again, as an engineer, do you recognize the possibility when you investigated these 10 to 50 reported events of unintended acceleration, did you acknowledge the possibility that these reported events of unintended acceleration could have been caused by a problem with the software in the vehicle? She is asking could it have been software that caused UA.

And their technician, who specializes in figuring out what happened said, No, this is not something I

recognized. In the Toyota system, we have the failsafe, so a software abnormality would not be involved with any kind of UA claim.

Q Well, in the Toyota system do they have the failsafe to stop unintended acceleration?

A They have some, but they don't have enough to catch them all. But beyond that, in a mature safety culture, you don't say, Well, we think we got it all so that is impossible. You say, in these cases, he could find nothing wrong with the car. And if you find nothing wrong, and you're ignoring software, that is a big problem from a cultural point of view. You have to take software faults seriously, even if you think you're perfect because nobody is perfect.

Q All right. Go to section 7. We heard from Mr. Ishii this Denso had done some software programing and it came in and they did some testing. Did you hear that testimony?

A I recall that yes.

Q Is testing, testing of that software, is that good?

A Doing some testing is good, but it is not even close to good enough to make sure a system is safe.

Q Why is that?

A You can never test long enough and thoroughly enough to find all the little bugs. What happens is when you test

you shake out some of the bugs that happen all the time, but you don't catch the ones that happen very infrequently. And system testing, you just can't -- nobody can buy enough vehicles and test them for long enough to catch all the rare bugs, just can't do it.

Q Now, in your next slide there, you talk about validation testing; is that right?

A That is correct.

Q And this all goes to your opinion that Toyota should have gone beyond just vehicle level testing, right?

A That's correct.

Q And you described why they should go beyond vehicle level testing, right?

A That's correct. There is more to it than that. You can't test long enough to see everything, but there is also somethings that you can't do at a vehicle level. For example, fault response. What if this bit flips? Well, there is no way testing a vehicle, unless you modify it, to flip the bit. So you don't know what is going to happen.

Q So if you cannot do enough vehicle testing, what do you do?

A You do other things. You do fault injection, which I will talk about in a second, and you also have to make sure you have a rigorous engineering approach. Testing just isn't enough. You have to have a good engineering

process on top of it.
Q Because it is impractical to test everything at the vehicle level?
A You just can't test everything.
Q Now, as part of your work, is it true that NASA described Toyota testing?
A So NASA did describe some Toyota testing. This is a point that -- I think it is on the next slide -- this is point even if you have 500 cars for 2,000 hours, you're going to see a thousand times more rare things in the --
Q Say that again.
A Even if you had 500 cars for 2,000 hours, which is a million hours, this is about how much Toyota tested I believe, that is going to see things that happen once every million hours. But if you have 15 years, the fleet will see maybe a thousand times less likely things.
Q Look at the next slide.
A So they did 35 million miles of system level testing; that is actually generous based on the NASA data. I gave them credit for all of their vehicle testing, so I rounded up
Q So you looked at all the testing that was done by NASA?
A This is NASA reporting what Toyota did. NASA did very little testing, they had limited resources. So this

is Toyota spent a lot of time driving vehicles around, which is a good thing. But if they had 400,000 Camrys year -- and the numbers go up and down, but that's in the ballpark -- and all those vehicles get driven oner hour per day, that is 145 million hours of exposure just for one year worth of Camrys.

Severe testing for 12 million hours, you will see things that happen every 12 million hours. You will not see things that happen every 20 million hours, but your fleet is going to see it.

Q According to the NASA report, what did they determine?

A And they said, No reasonable -- Toyota's vehicles are so complex that no reasonable amount of analysis or testing can prove an absence of errors. This goes back to you just have to assume any single pointed failure is going to have a problem. There is no way you're going to prove it doesn't through analysis and testing, you just assume it is there.

Q Is that why the rigorous engineering process is absolutely vital?

A It's absolutely vital because no amount of testing demonstrates it is safe. You have to do something else. And the something else is good rigorous engineering.

Q Is it true there are just going to be some bugs,

some faults that cannot be found?

A There is always going to be software bug that you can't find. There is always going to be hardware events, maybe hardware bugs that you can't find. You do rigorous engineering to make sure you have gotten as many of them as you can to a sufficient level, and then you add failsafes on top.

Failsafes are great for the couple that you didn't know about, but if you skip the step of being rigorous and then you say, Well, the failsafes will catch us, that is not good enough.

Q In this vehicle, Toyota has argued, Listen, we have gone with the car, looked at the system, we can't reproduce any of these things going on. Are bugs reproducible?

A So let's see. Some faults are harder to find.

Q Right.

A And some faults are impractical to reproduce.

Q Why is that?

A In a system -- so some of the fault injection that I showed you before where they said, All right, we flipped some bits and we produced UA, they had to specially modify the system to be able to flip those bits. There is no way to go into a Toyota system and say, I am going to flip that bit here without modifying it. You just can't do it.

And even if you could, there maybe very, very

tight timing that if the bit flip happens exactly in this time widow, it goes nuts, and everything else, no big deal. There is just so many things to try that it may be very hard to find it. Even if you find it, what people have found is it is just this thing that comes and goes. And there is no way. You can try a hundred times, a thousand times, maybe you get lucky, maybe you don't.

I have friends in the compressor business that will take a compressor that fails regularly, bring it back, and they will run it three weeks, four weeks, five weeks, and they don't see anything. If they're luckily after six weeks they see it, or maybe they don't. That's just the way it is. You crash a laptop computer, somebody says, Make it do it again. You can't do that. Sometimes you can, but a lot of times you can't.

Q Now, your next opinion is that Toyota's source code is of poor quality. And we mentioned source code earlier. If you can just refresh our memory on what source code is.

A Source code is the human readable recipe, a computer program. So it is in the C programing language for the main CPU. It is in a thing called the assembly language for the ESP-B2.

Q Have you reviewed Toyota source code?

A I have not reviewed Toyota source code.

Q Why not?

A I was asked for access, and it was denied several times.

Q The --

MR. BIBB: Your Honor, can we approach on that.

THE COURT: Yes.

(The following bench conference was had outside the hearing of the jury:)

MR. BIBB: I think that leaves a false light with this jury. He was denied access not by Toyota but by Judge Selna. He has limited the number of people, he limited it to 12 experts.

THE COURT: Why didn't someone come to me and ask me to give him access like you did with the lawyers?

MR. PORTIS: That is -- his report had already been done. That is untrue. Toyota has specifically said we don't -- we're not going to allow him to have access, and they told Judge Selna that.

MR. BIBB: We have opposed expanding the number of experts in there, and Judge Selna has agreed. We expanded the number of attorneys who have access to source code information on a case-by-case basis as needed.

MR. CLARK: There are 12 plaintiffs' experts that have source code access. They either have three or four of them in this case. So they had eight or nine other options that they could have hired, so it's really misleading the

way it is right now to the jury.

MR. PORTIS: Well, I don't know about misleading. All I'm asking him -- I asked him why -- because he gives the opinion it is of poor quality. And I will establish the foundation as to why he says that. I think the jury is entitled to know that he was denied access to the source code, period. I think they're entitled to know that. It has been requested that he have access to source code.

THE COURT: And Judge Selna didn't allow -- and Toyota objected, and Judge Selna didn't allow it, right?

MR. PORTIS: Correct.

THE COURT: Do you want me to tell the jury that, that he requested it in another litigation?

MR. BIBB: I think so.

MR. BAKER: As long as you say Toyota objected to it.

THE COURT: I say that, obviously they have heard about the multi-district litigation anyway. Do you want me to instruct the jury that he requested through the multi-district litigation, explain to them that the source code is confidential, that he requested it through the multi-district litigation, Toyota opposed it, and the judge in that did not allow him access?

MR. BIBB: I think also what he said, that the court allowed 12 plaintiffs' experts -- 12 experts.

MR. PORTIS: Not in this case. Not in this case.

MR. BIBB: The total of 12 experts to have access to the code and denied his access. You have three in this case.

MR. PORTIS: That's too far, your Honor.

MR. BIBB: They examined him about it.

(Within hearing of the jury:)

THE COURT: Ladies and gentlemen, Toyota -- what we referred to as a source code, is highly confidential. And in the multi-district litigation, Dr. Koopman, the request was made for him to see the source code. Judge -- Toyota objected to expanding the parties who -- or the people who could see the source code, and Judge Selna did not allow additional parties to see the source code. So that's -- to explain his comment about not being allowed to see the source code.

Q (By Mr. Portis) The fact that you have not see the source code and you this opinion this the Toyota source code is of poor quality, how do you square that? Let me ask it again. How do you square that?

A The way I look at it is I've done many design reviews where I don't see the source code. In fact, most of my safety reviews the source code hasn't even been written yet.

And they ask me higher-level things like, Can you find a

single point of failure that we can fix.

The ones where I do have source code I've noticed a correlation and the academic literature supports a correlation between some high-level qualities of the source code and whether it is defective or not.

So my opinions are based on the summaries done by NASA, done by Mr. Barr and his team that say, Here is some descriptions of things that the source code does that are commonly accepted as defective practices and not accepted practices. So I'm opining based on those summaries that I say, Gee, for example, it has 10,000 global variables.

Well, I know that the right answer academically is zero. And in practice, five, ten, okay, fine. 10,000, no, we're done. It is not safe, and I don't need to see all 10,000 global variables to know that that is a problem.

Q What is a global variable?

A So a global variable is -- let's go back. So a variable is a location in memory that has a number in it. And a global variable means any piece of software anywhere in the system can get to that number and read it or write it. That is considered a bad practice because it is hard to tell what is going on.

When you have hundreds of thousands of lines of software, it is really hard to tell who changed it and when they changed it, and it is well known to be very bug prone.

And that has been known since the 1970s that that's a really bad idea.

Q Was the Toyota -- was the Toyota programming, was it prone to bugs the way it was designed?

A From everything that I've from the software quality metrics, I would call that software prone to bugs.

Q Tell me your support that -- tell me about your support that the Toyota source code is of poor quality.

A To start with, there is the MISRA-C guidelines. This is the small book that we have been talking about. And it tell us you how to use the language. Here is an example: Toyota actually does not make a mistake on rule 35, but it is easiest one to explain.

So if you say A, equal, equal B, or A, equal B, they look almost the same. I've made this mistake. It is hard for me to believe that any programmer has never made this mistake. It is easy to miss. But this one says if they're the same do this, and that's okay. This one says take B and put the value in A so it corrupts the value of A, with the value of B, and it is probably not what you meant.

The compiler will say, Sure, I know how to do that, but it is dangerous. So MISRA-C says even though this is a valid line of source code, you're not allowed to do it because it is too dangerous. There is 127 rules in

the 1998 version that are all I know you can you do this, but it is not allowed, it is too dangerous. It is pointing a loaded gum at your foot. I know you're not going to pull the trigger, but don't do it.

Q Tell me about that.

A So MISRA-C, or something like it, some restricted sub-setted language, is required a MISRA cell 2 or higher. And they also say, you know some of these rules are just advisory instead of required. Most are required. Some are just good ideas. But any time you violate a rule all deviations should be documented. So you either have to have written down someplace that someone can see one of the MISRA SIL-3 things was everything has to be written down to see it. If it is not written down, it is not MISRA SIL-3.

So you have to have it written down, or a rule 35, we decided we're not going to do it and here is why. Rule 127, we decided not to do it in this one place, and there is
a line in the source code saying in this one place we decided it is okay. But if it is not written down, it did not happen.

Q Again, the MISRA-C is that a recipe to write the language properly?

A That is a recipe to use the language properly that is widely used outside of automotive.

Q Even based on listening to Mr. Ishii did they follow MISRA-C?
A They did not follow it. He said that they followed about 50 percent.
Q Right.
A Okay. And what we found was you can -- to know whether you followed it, you can actually use a piece of software that goes through and says, Hey, did you follow it or not? NASA checked 35 of the rules and found 7,134 places where they didn't follow the rules. Mr. Barr checked the 2004 version of the rules which have a few more rules than the 1998 version, but not really that different, and found 81,514 violations.
Q Are you telling the ladies and gentlemen of the jury that Toyota had this many violations of MISRA-C?
A Yes, I am. That's my understanding based on the analysis done by these sources.
Q All right. Now --
A And I should say the accepted practice is zero.
Q Zero?
A Zero. You should have no violations. If you have a violation, the way around it is you put in the source code, Hey, I'm going to violate rule 127 on the next line. Here is why it is okay, and then the warning turns itself off. So you can get to zero as long as you have documented why

particular ones are okay.

Q Why else do you say that this source code is of poor quality?

A I looked at some of the warnings. Mr. Barr provided a very detailed analysis rule by rule, not with the lines of source code but with the kinds of mistakes they're making. And so number 52 unused variables. So that's a place where you said, I'm going to store something in this location and you never use it. Okay. Declared, but not referenced. I'm going to have a subroutine, and I have a subroutine called add three things. And you say I will define it, and you never get around to it.

Uninitialized variables. Here is something where you say, here is a value I will use later, and you forget to set it to a value, so who knows what the value is. Those are all just sloppy coding practice. Those are the kind of things if teaching you programming and you make those mistakes I slap your hands because nobody should ever make those mistakes.

Q And you actually write code, don't you?

A I've written plenty of code. And if I weren't a compiler, and it tells me any one of those things, I fix it every time because that is a malfunction waiting to happen.

Q Earlier, in Mr. Ishii's testimony, there was a graph that is part of a -- there was a graph. This graph right

here. Mr. Kawana had given a presentation. Also, Exhibit 4229, which is a paper written by Mr. Kawana called the *Empirical Approach for Reliability Assurance of Vehicle Software* by Toyota Motor Corporation.

A Yes.

Q He introduces this particular graph?

A Yes.

Q Can you tell us about that.

A The meaning of this graph is based on his studies at Toyota was that these rule violations that they -- they 81,514 things that I told you about, the MISRA-C, and my understanding is that's the criteria that he used too. That for every 30 rule violations, you can expect on average three minor bugs and one major bug. If you take 81,514 warnings divided by 30, if I punch the numbers into the calculator correctly, that predicts 2,717 major bugs based on the data from this paper. Now, I will not say that is an exact count, but it is not ten.

I also scoured the academic literature. The practitioners all sort of know this intuitively, but I was able to find empirical study that found a statistical correlation between these warnings and code quality.

Q So just so I understand this, Toyota and Mr. Kawana had this idea that if you had 30 rule violations -- and in this case we had -- we're found 81,514 violations, correct?

A Yes.
Q Then you would divide that by 30 to determine how many major bugs you would have in the particular software?
A That's how I interpret the paper.
Q And that is the software in this case, right?
A That is correct.
Q Now also in that paper, if you go back to the slide that starts with Toyota didn't follow most of MISRA-C rules.
A Yes.
Q Discuss this right here.
A This is out of a slide set, but it goes with a paper, that my interpretation, when I look at this, is I look and it and said -- what these slides say to me is that Toyota required 114 rules and advisory 35 rules. This conveys to me that whoever presented this is representing that Toyota followed all the rules.
Q Is that correct?
A It's incorrect for two ways. One is Mr. Ishii said they only followed about 50 percent of the rules. But what I found was that they followed -- Mr. Barr -- excuse me -- what Mr. Barr said was they found -- followed maybe 11 percent, much smaller number.
Q If you will, we talked about global variables. I want us to talk a little bit about cyclomatic complexity.

A Okay.
Q Cyclomatic complexity.
A McCabe Cyclomatic Complexity Metric.
Q Then -- and we heard this used in opening. We heard about this idea of a spaghetti metric. What is this all about?
A Well, spaghetti is -- spaghetti code is a term that is widely used. It is not a very -- it's not a compliment when you call someone's code spaghetti code. You can think of a plate of spaghetti. If you have a big pile and plate of spaghetti and you pull on one end of a piece of spaghetti, not only does it look tangled, that's part of it, you pull on one end, you have no idea which other end is going to start moving.

So the fact that it is tangled has to do with, Well, there is some picture. This is out of National Institute of Standards and Technology Report of cyclomatic complexity. Some functions, what you do is you kind of count up the number of ways through the code. This is very loose.

MR. BIBB: Your Honor, can we approach for just a moment.

THE COURT: Yes.

(The following bench conference was had outside the hearing of the jury:)

MR. BIBB: Again, as I recall they needed to lay a foundation before they can talk about that spaghetti code. I was a little slow on the draw there, and I apologize. But they need to lay a foundation for that. I think that was the court's ruling before they can introduce spaghetti code.

THE COURT: I thought I allowed spaghetti code.

MR. BAKER: You did allow spaghetti code.

THE COURT: Toyota had used it.

MR. BAKER: Toyota had used it, and because it is a term of art within the industry. He just said it was a term of art.

THE COURT: Do you have my ruling on that?

MR. PORTIS: We can't lay a spaghetti code foundation? Are you saying that I can't lay a foundation in the spaghetti code.

MR. BIBB: Again, it is the source code.

THE COURT: Okay. So sorry. Now, what was just on the screen what did that it say again?

MR. PORTIS: It was talking about --

THE COURT: Just explaining spaghetti code in general?

MR. PORTIS: Yes, ma'am.

MR. BIBB: There has been no foundation laid that the code in this engine in this vehicle is spaghetti code.

THE COURT: I thought Toyota calls it spaghetti code.

MR. BIBB: No. No. Toyota talks about the spaghetti code generally. That was the whole part of the argument last week was that general discussions of spaghetti code don't get us to the coding of this vehicle being or not being spaghetti code.

MR. PORTIS: That's how we will get into the foundation of it.

THE COURT: Is he going to make an analogy and say this code was spaghetti code?

MR. PORTIS: Yes, ma'am.

THE COURT: What is he going to base it on since he hasn't seen the code?

MR. PORTIS: He will base it upon the material that is in the NASA report. I will ask him what he will base it on, but the material he reviewed.

THE COURT: But that he somehow will testify that he has seen enough of that to say that it is spaghetti code?

MR. PORTIS: Well, I don't know that he needs to see the code. He can rely upon other academic information to provide his opinion about it.

MR. CLARK: There is no foundation at this point.

MR. BAKER: Why don't we give the jury a break so

we can talk about this.

THE COURT: Let me ask: All he talked about right now is the concept of spaghetti code in general?

MR. PORTIS: Yes, ma'am.

THE COURT: He hasn't mentioned anything about Toyota?

MR. PORTIS: Yes, ma'am.

THE COURT: Do not mention anything about Toyota until there has been a foundation laid that he knows enough about it. He can reference where it is or is not. He can continue to talk about just generically what spaghetti code is.

MR. PORTIS: Yes, ma'am.

MR. BAKER: I guess the concern I have right now with your ruling is I understand he doesn't know if it -- the witness -- and he may have to go into an answer. That's why I think we should take a break.

(Within hearing of the jury:)

THE COURT: We will take our afternoon break at this point in time. We're in recess for 15 minutes or until 2:45.

(Whereupon, the jurors exit the courtroom.)

THE COURT: So the whole reference about the spaghetti code, what he is talking about right now is just generally what spaghetti code is.

MR. PORTIS: It is a couple of things. And I will show you this slide, which was the next slide. One spaghetti code we're going generally into it and talking about what spaghetti code is, trying to define it, so the jury would understand it. Then his support of he is coming in saying, Look, I think this is spaghetti code based upon what I've observed. This is what I've observed.

THE COURT: Have you seen this one?

MR. PORTIS: Yes, they have seen that.

THE COURT: Mr. Bibb it is page 73.

MR. PORTIS: This is what I observed. I have seen there is 10,000 global variables in this. This is spaghetti code. I talked about the global variables. I know in the industry, based upon the fact that this has 10,000 globe variables, that that means this is spaghetti code in and of itself.

MR. BIBB: Is that really proper testimony from Mr. Barr to talk about? He is the one that looked at the code.

MR. PORTIS: Barr can talk about it too.

MR. BIBB: I need to object more on hearsay of him saying that is what Mr. Barr told me. I think that goes beyond an expert relying on materials in the field, he is relying on another witness.

MR. TEAGUE: He just can't parrot another expert.

MR. PORTIS: He can rely upon academic information, period. But all that said, I do think the objectionable part to this particular is the -- in the bottom right which is a Toyota document.

MR. BAKER: We have taken that out.

MR. PORTIS: We will take that out. So we're not discussing that. But in terms of just the general information and the information that he knows about spaghetti code and the term of art, this is what he will testify and the foundation for that.

MR. CLARK: I think we probably need some more, for sure, at a minimum we need some more testimonial foundation before that slide goes up on the screen, and some testimonial foundation specific to what he knows from his work as opposed to Mr. Barr's work.

THE COURT: He can rely upon other expert's work, and he can rely on hearsay. So I will allow him to testify as to this, but I do want the reference to the Toyota document --

MR. BAKER: It's already out.

MR. CLARK: Just for the record, we're objecting to the relevance and the 403 that we made last week.

THE COURT: All objections are reserved. Yes.

(Whereupon, a short recess was had.)

THE COURT: We're back on the record. Members of

the jury are present as well as counsel and their clients. Dr. Koopman is still on the stand. You can continue your direct examination, Mr. Portis.

MR. PORTIS: Thank you, your Honor.

Q (By Mr. Portis) We were talking before we broke about this cyclomatic complexity spaghetti metric and trying to get educated exactly what it is. A spaghetti code, and you described it is generally compared to a bowl of spaghetti and picking out one end or another. Is that a term of art used in your particular field?

A Yes. It is a term of art. In my expert report, I reference several academic references that actually use that term.

Q When you say that code with structural problems is often called spaghetti code, tell me what you mean by that.

A So what I have done is I've taken the usual definition and sort of summarized them into a generic one. It is incomprehensible code, meaning a person is probably not going to understand it. If you can't understand it, that means there is probably bugs because you don't understand it.

Incomprehensible code due to unnecessary coupling, jumps, gotos, or high complexity. In this case, the coupling refers to those globe variables that we were talking about that take two pieces of software and make

them interact. And the complexity is the cyclomatic complexity metric. And jumps and gotos are other things that just cause the program to jump all over the place while it is executing.

Q So under where you have got this highlighted, very high cyclomatic numbers, would that include global variables?

A Those are just talking about control flow, so this is --

Q Describe that.

A So control flow is the path through the program. If this, do this, or else do this other thing. So this metric does not include global variables. There are two ways to look at it, and this one is just about the path of if this, do this.

Q Okay. And on the next page, you say that the Toyota electronic throttle control system has untestable spaghetti code; is that right?

A That's correct.

Q Why do you say that?

A I say it because from this NASA report, and in general practice, it is considered if you a number of more than 50, there is lots of ways through this code. As a practical matter, you can't test it, there are too many possibilities. No way to exercise them all. So a number

of 15, 20, not so bad, 15 or 20 are not so bad. Fifty is untestable, more than, say, 75, it's so bad that every time you make a change you're probably going to create a bug. And this comes from the Reliability Analysis Center, which is an Air Force run place that deals with reliability of everything. And that -- they're just summarizing what people in the industry tend to think.

Q Now, the code that Toyota wrote for the 2005 Toyota Camry, was it code that was written from the ground up, per say?

A My understanding is they built on previous code. When you do that, that is one way to get spaghetti code is by building on previous code. Instead of going back and cleaning it up, you saw those uninitialized variables, basically poor housekeeping. Instead of keeping the house clean, they built more stuff on top of it. That is my interpretation of those metrics.

Q What about the target throttle angle complexity is high? What does that mean?

A Well, in general there are 300 functions greater than 20. There are 12 functions greater than 100, which is just a staggering number. That is a complexity of more than a hundred. Anything over 50 is considered untestable, and Mr. Barr found 68 functions greater than 50.

A target throttle angle computation, which tells

you how open the throttle should be, had a complexity of 146 and 20 pages of source code. This is far too complex, far too long to be considered good code. So it's hard for me to imagine how it could be tested thoroughly, how anyone could really understand it completely.

Q When you say that it is untestable, are you talking about -- when is that testing occurring?

A During design. What you do is you take each individual software function and test it very thoroughly before you ever put it in a vehicle. A cyclomatic complexity of 146 as a practical matter it is really hard. We have seen no evidence. In a SIL-3 system, you would say, Here are all the tests that we ran, and here is how we know they are good. We haven't seen that.

It is hard to imagine how to test a function like this. It would take a Herculean effort to do it if you can do it at all.

Q Then you mentioned that the spaghetti code has a tangled or complex structure; what is that?

A That is back to the plate of spaghetti. So there are two types of things that you worry about. One is the control flow if this, else this, if this, and that is what the number is. With 67 functions above 50, just based on that number I can conclude that the ETCS code is control flow spaghetti. So control flow is the "if else."

But I can also conclude that with all those 10,000 more or less global variables, it is data flow spaghetti. In other words, the data, the global variables are pointed out from everywhere, and there is no reason for it to be that way. On both counts, I look at this code and say, I can't imagine how someone can get this safe. It is too complicated to test, it is too complicated to understand.

Q Now, your next section here, your next few sections really follow under this idea that Toyota did not follow other accepted practices. Are you referring to MISRA and other practices here?

A Back when I did the two tables with MISRA with the yellow circles, those were sort of engineering methodology. But you also have to get the technical stuff right. Just because you follow good process, if you are clueless about how the technology works, you will not get it right either. These are about how the technology works.

Q I see. So we discuss MISRA, now we're talking about technology. Can you describe specific difference between that.

A So the most of the MISRA were -- steps were -- this is software guidelines -- how do you know that you got it right? What did you do to convince yourself you got it right? These are basic things that we feature to undergrads saying when you are writing code, you have to do

it this way or it is going to be wrong.

Q We know on the software part, we know they didn't get it right. I think there were 81,000 plus defects.

A That was one aspect. We will talk about things beyond that, so even beyond that.

Q And by the way, were those 81,000 plus defects, were those ever documented by Toyota?

A Not that I know of. I'm sure that there were some defects that they were aware of, but my understanding is that the number they knew about was much, much smaller.

Q Now let's go through these quickly.

A Okay. I will just explain the high level idea. And Mr. Barr will go into details about these later, so this is a preview. There is a thing called a stack where the program keeps its temporary working variables. I think if you have a notebook and you have the top page is what I'm going to do today, then you go to the next page, eventually you run out of pages in the book. If the last two pages that you had set aside for things that can't ever be overwritten, and if you run out of pages and you don't pay attention, you might start writing on top of them.

So that is a stack overflow. If the stack grows too big, it will actually corrupt the globals that we were talking about, or operating system, and cause the system to malfunction. This is a well-known problem. If you're not

paying attention, it happens to embedded systems. I have done design reviews where they had this problem.

Q Was that an issue with Toyota?

A My understanding is that Toyota used far more of the stack then they thought they used, and Mr. Barr will have specific opinions about that.

Q Fair enough.

A Part of getting the stack right is you're not allowed to use a thing called recursion. Recursion is when a program calls itself and says, I want to add a number, how do I do that? I want to add two other numbers. How do I do that? I will add two other numbers.

Every time it calls itself, it is like sending yourself a message, and the message says, Send yourself another message. And you are not allowed to reply until you are done sending yourself a message. Well, how do you know that ever ends? Maybe it doesn't.

So if it never ends, you may also crop the global stack. So there is a thing called recursion. And the safety critical standards all say you're not allowed to use it because there is a risk that you will just keep growing the stack and overwriting your code, but Toyota uses it.

Q What you have highlighted says that recursion carries with it the danger of it exceeding available stack space which can be a serious error?

A That's right. So this MISRA-C rule number 70, and Toyota violated this rule. The other MISRA rules are the same kind of idea, if you do this, you're really taking a change; that's why you shouldn't do it.

Q Let's talk about peer reviews.

A So peer reviews are where you have someone other than the author take a look at the software. This is proofreading your term paper, you are never going to catch your own typos.

Q Why is that important?

A It is important because no one ever catches their own things. But it has been documented that you will find half or two thirds of your defects doing it this way. An IBM document that was actually invented in the mid-'70s and in the '80s they documented it. Basically everybody knows that peer reviews are a good way to find bugs; that's why it is part of a good safety critical design process.

Q Was Toyota's peer reviews adequate?

A I can't find any written evidence of peer reviews being conducted or find any defects. I know that there were informal meetings, and I know that Mr. Ishii said sometimes we take a look a the code. But if you're running safety critical system software, you always take a look at the code and you write down whether you found problems.

The reason that you write them down is that if

your peer reviews aren't working you can tell because you didn't find anything. If you are not keeping track, you don't know if they're working.

Q You also talk about concurrency and timing defects and how they affect safety; is that right?

A Right. So I'm just going to limit it just to a couple of things. There is a thing called task death. So when you're running Windows or Mac OS you have a bunch of programs running. If one of the programs dies, that is a task, and sometimes they die. And that happens in embedded systems as well.

And the accepted practice is if a task dies you are supposed to notice it and you are supposed to restart the task or restart the system. Because if that task is important, you are going to have a system that is malfunctioning.

And here is how you can detect it: A Watchdog timer is a thing that detects this. So the main CPU kicks a thing called the Watchdog; that is what people call it, they call it picking or petting. But there is a Watchdog, it is a timer that just counts to zero. If it hits zero, it resets the system.

So the software's job is every once in a while to go out and kick or pet this Watchdog and say, I'm still alive, everything is still okay. The big reason that you

use this is to find if a task died. If all the tasks all have to cooperate and you say there is ten tasks, there is 20 tasks, when you kick the watchdog, you need to make sure all 10 or 20 tasks are alive. If any one died, then you reset the system then you say something is wrong, let's start again.

Q What is your concern here?

A My concern is that Toyota didn't do this properly. To be correct and accepted, any single task death has to let the Watchdog reset the system. In Toyota, there is only a few tasks that when they die it resets the system. Most tasks, when they die, the Watchdog timer doesn't reset. So that's fundamentally not in accordance with accepted practices.

Q I want us to skip this. Go to 12.

A Okay.

Q And tell us what you're showing up here.

A So this is the last two slides. This one is talking about the NASA UA report. So this is the report that NASA looked at the Toyota things, and we know that they didn't get to see everything. But they looked at a lot of things, they spent a lot of effort.

What they concluded, it is important to be precise about what they concluded. What they said was they never said it was safe. What they said was they couldn't find a

reproduceable defect that resulted in the kind of UA they were looking for. And we know it is often hard to pin these things down, so that's what they found.

But they also said because proof that the ETCS-i caused the reported UAs was not found does not mean it could not occur. So NASA never said it couldn't happen, they just said they didn't find it.

Q What they did find was a single point of failure, correct?

A But they did find a single point of failure. As we discussed referencing the Hammett paper, when I read the NASA report, they're telling me that they found a single point of failure.

Q And your next slide.

A And these are my high-level opinions. So I think that the Toyota ETCS is defective. I think it is dangerous. It has a single point of failure. Both chips, even though there is two chips, they are in one fault containment region, which means no matter how hard you try to put in failsafes, there is always going to be a case that it can't check itself and it will have a dangerous failure.

I didn't talk about this in the slide, but there is some issues with the realtime scheduling that Mr. Barr will talk about. The Watchdog timer doesn't detected task

deaths the way it is supposed to, and that is a bread-and-butter safety thing, the first thing you look for in a safety system -- second thing.

The first thing you look for is a single point of failure. The second thing you look for is whether the Watchdog is right or not, and they got that wrong.

Toyota did not follow MISRA software guidelines or any guidelines that I can find that are comparable enough to get you safe. These things could be fixed. They have two chips. They didn't use them in the right way.

MR. PORTIS: Your Honor, other than offering exhibits, we will tender the witness.

THE COURT: Thank you. Mr. Bibb.

MR. CLARK: Thank you, your Honor.

CROSS-EXAMINATION

BY MR. BIBB:

Q Good afternoon, Professor Koopman.

A Good afternoon.

Q Is it pronounced Koopman or Copeman or Cokeman?

A Koopman.

Q Okay. We have had some debate. It is spelled K-O-O-P-M-A-N, right?

A That's correct.

Q And a lot of us in this part of the world would call that Koopman, as opposed to Koopman. If I lapse into that,

please don't take any disrespect from me on that, it is just habit, okay?

A That's fine.

Q Now, I understand that you first were engaged in studying the Toyota electronic throttle control system June the 15, 2012. Does that sound right?

A That sounds about right.

Q And you reached your opinions and produced a 96-page report finding many, if not all, of the flaws in the system that you've described to this jury in the last several hours in about 30 days; is that right?

A That sounds about right.

Q You spent a month to come up with the opinions that you've come to today; is that right?

A It was about a month of calendar time. Yes.

Q Now, I understand that you used your own methodology in coming to your conclusions that UA is caused -- unintended acceleration could be caused by Toyota's electronic throttle control system; is that correct?

A I'm not sure if that's entirely correct. It depends by what you mean by my methodology. I certainly didn't make up something out of thin air.

Q Good. Good. Because you have been very critical of Toyota's coding because you didn't feel they followed recognized methodology, for example, in MISRA; is that

right?
A That's right.
Q And in a prior deposition, were you not asked about where you came up with the methodology that you've utilized here? And the questions were:
"Do you recall this? And this methodology that you used
here on this hypothesis that UA is caused by ETCS, that's electronic throttle control system, that's your own methodology, correct, you didn't borrow that from anybody else?"
Does that sound familiar to you, that question?
A I remember something like that, but I would really like to see the --
Q Fair enough.
A -- details so I can have the context.
Q Fair enough. Let me get you a copy of that transcript. In fact, I will bring you a copy of a couple of transcripts that you have got.
(The following bench conference was had outside the hearing of the jury:)
MR. PORTIS: Your Honor, I'm fine with this. Obviously the proper way is to use a deposition when he testifies contrary to what he testified earlier, I don't think you have established. I'm fine with it this time,

but I want you to do that from now on if that's okay.

THE COURT: Okay.

(Within hearing of the jury:)

Q (By Mr. Bibb) I will give you that one too. Let's turn over to page 324, Dr. Koopman. And I want to direct your attention to lines 9 through 13. Have you found your place?

A Yes.

Q And the question very simply is, Dr. Koopman:

"Is this methodology, this work that you have shown the jury for the last several hours, this methodology here on this hypothesis that UA is caused by ETCS, that is the unintended acceleration is caused by the electronic throttle control system, that's your own methodology, correct, you didn't borrow that from anybody else?"

And what did you answer?

A I said there I didn't get this picture from anywhere else. But I believe later in the deposition I explained that it was roughly analogus to a fault tree.

Q If you go further down that page, did you not testify that:

"This is my own methodology, it is not a standard methodology I found someplace."

Do you recall telling us that?

A Can you repeat the page number and line.

Q Start, the question begins at page 324, line 23, through 325, line 2.
A So I'm testify that it was a way to articulate a scientific --
Q No. That is the question is:
"Did you answer the question this is not a methodology you adopted from somebody else?"
Is it your answer:
"This is not. This is my own methodology. It is not a standard methodology I found someplace."
Is that the testimony that you gave under oath at that time?
A I'm sorry. Can you give me the page and line number again.
Q Page 324, line 23.
A Okay.
Q Through page 325, line 2.
A That is what I testified, but it was not about the things I've been talking about today. It was something very specific to the Van Alfen case.
Q Well, it appears to be very general here. You haven't been suggesting that the software, the hardware of this system somehow makes it prone to unintended acceleration, haven't you?
A The context of this question and answer was with

regard to a particular picture that was in the Van Alfen report. I've not used that picture. I've not used anything like it in forming my opinions. This was on top and beyond everything that I said today.

Q Okay. Do you know of anyone in the automotive field that has used your methodology?

A The methodology of how I got what I'm saying today is to look at the MISRA software guidelines and look at best practices and to decide whether they were followed or not. And I think anyone who does -- analyzes software safety uses that methodology, among others.

Q How many electronic throttle control systems or hardware or software for a production motor vehicle has Dr. Koopman designed?

A For a production motor vehicle I have not designed one.

Q Zero, correct?

A That is correct.

Q And it's pretty easy to come in and criticize the work of somebody who does this for a living, isn't it, a college professor comes in, says they got it all wrong, a company that builds millions of automobiles every year; that's what you have done today, haven't you? You have done it in 33 days; isn't that right?

A I think what I presented today goes beyond what that

initial report was. The initial report was fairly limited. I certainly identified a single point of failure in the initial report. But I've had a lot of safety experience. I worked on safety critical car software.

My current research is how to make autonomous vehicles safe. So I have not actually done the -- written the code for electronic throttle control system, but that's not the same as not knowing about it.

Q And you know what the jury is doing in this case, they're trying to determine whether or who should be responsible for the crash that Ms. Bookout was involved in and Ms. Schwarz on September 20, 2007, you know that, right?

A I understand.

Q And before you got involved with lawyers representing the plaintiffs against Toyota in unintended acceleration claims, you had never investigated any kind of automobile crash before; isn't that correct?

A I had done work on safety shutdown system for automobiles, but I had not done a crash investigation.

Q You got that transcript still handy up there? I will direct your attention to page 207. And this again is talking -- I think you're right. You're talking about that you never investigated an automobile crash, but you worked on this ground vehicle, that unmanned ground vehicle that

you mentioned earlier, right?
A That's correct.
Q And the unmanned ground vehicle, by its very name, is it doesn't have a driver in it, does it?
A It at times has a driver who is outside the vehicle using a remote control. There is nobody sitting in the vehicle.
Q Nobody sitting in the car.
A There are, however, people who can get run over by it, so it is still safety critical.
Q When were you retained to work in the Bookout case?
A I don't remember an exact date. It was certainly more recently.
Q Was it within the last year?
A I didn't look that up.
Q Okay. I understand that you charge, at least on the CV that I got with your transcript $580 per hour for your expert witness services; is that right?
A That's what I charge all my expert witness clients.
Q And when -- I understand when you work and take, when you give depositions, or you testify in trial like this, your charge runs portal to portal, correct?
A That's correct.
Q And that means you charge from the moment you leave your house to the moment you get back home to your house,

correct?

A That is correct, but there is a maximum. And my experience is I usually work more hour than I'm actually charging for.

Q And you charge not only a maximum of 12 hours a day at $580 an hour, you also have a minimum charge, do you not?

A I have a minimum of one day to do those events.

Q You have a minimum charge. If you came and spent an hour of doing expert witness services, a minimum charge of eight hours per day, correct?

A That's correct. And what I found is that I have to set the whole day aside. And I'm pretty wiped out by the end, so I lose a day either way.

Q Okay. Now let's talk about the work that you've actually done for the Bookout case, okay?

A Okay.

Q When did you inspect Mrs. Bookout's vehicle?

A I've not physically seen the vehicle. What I did was I looked at pictures of the vehicle.

Q So when did you go to the location where Ms. Bookout's crash occurred outside of Eufaula, Oklahoma?

A I've not physically been there. I looked at pictures of the crash scene, and I used Google earth to virtually walk around and get an idea.

Q So you haven't seen the car, and you haven't seen the scene, fair enough?
A Not in person.
Q And you have not inspected any components from Ms. Bookout's car, have you?
A Not from her vehicle.
Q Have you reviewed the reports of either Mr. McCort or Mr. Stopschinski the accident reconstructionist in this case to get an idea of the speeds and distances involved?
A I've seen summaries of those reports, but I've not been through them in detail.
Q You read summaries of the reports?
A Yes.
Q Were they furnished to you by the plaintiffs' lawyers?
A I don't recall where I saw them.
Q When di you see them?
A I saw them when I initially got all the documents. I read through everything that was provided to me.
Q Was that several months ago, or just last week?
A It was more than last week. It was before my deposition. I don't have a date for you.
Q And your deposition in this case was the very end of July as I recall?
A Sounds about right.

Q Now, you know that the Bookout vehicle has been inspected by Mr. McCort and Mr. Stopschinski, right?
A That's my understanding.
Q And it has been inspected by Mr. Loudon and Dr. Van Schoor and Mr. Hannemann and Mr. Walker and Mr. Osterhow (phonetic) and Mr. Cheek and Mr. Livernois and Mr. Powell and Dr. Young and Dr. Catherine Corrigan. You know they all looked at the vehicle. Were you aware of those?
A Some of those names I recall. I don't recall the entire list. I know that it was inspected.
Q And you're aware that all of these engineers and scientists have looked at her car and have found nothing with either the engine or the brakes of her car that could account for this accident, aren't you?
A I'm not prepared to opine on that.
Q All right. My question is: So you don't know that they haven't found anything wrong with the engine or the brakes that can account for this accident; you just don't know?
A I just don't know.
Q But you do know that Ms. Bookout drove this car for two years and 9,600 miles and never had any problem with the engine or the brakes on this car, correct, you knew that?
A I read her deposition testimony, and that's my

understanding.

Q All right. You are not offering opinions to this jury in the several hours that you have been on the witness stand today that there was some software defect or combination of software defects that has led to an alleged unintended acceleration of Ms. Bookout's car about 6:30 in the evening on September 20, 2007, are you?

A My opinion is, as I said at my deposition, is that is the facts of this accident are consistent with my opinions. But I'm not offering a specific causation opinion.

Q I think in your deposition you were quite clear that you were not offering an opinion that -- as to whether the electronic throttle control system in Ms. Bookout's car was -- and I think in your words it was the proximate likely cause of the crash, you were not offering that opinion, correct?

A I'm not offering that opinion.

Q You have come all the way from Pittsburg, Pennsylvania, and you have spent most of the day on the stand talking about the Toyota electronic throttle control system, but you don't have an opinion as to whether it caused this crash; that's what you're telling this jury?

A I have an opinion that it is a possible cause, that it is defective and it is unsafe. But I do not have an

opinion whether it was for sure the proximate cause of the crash.

Q A likely cause is what you said the approximate likely cause of this crash, you do not have that opinion, do you?

A I do not have an opinion on that.

Q Because the question that you were asked is if you have an opinion.

"Can I ask you if you have an opinion within a reasonable degree of scientific certainty that the unsafe condition of the electronic throttle control system in the Bookout vehicle as alleged by you was the most likely cause of that mishap and crash?"

Didn't you answer that question:

"I don't have the an opinion on whether it was the approximate likely cause."

A That sounds about right, and I agree with that statement that I made.

Q All right. Now, in fact, one reason is you hadn't done the work necessary to reach that opinion, correct?

A This are two reasons. One was I wasn't asked to do that. The other one is I have not done the work necessary to reach that conclusion.

Q Likewise, you do not have -- you haven't tried to extend your analysis of the work you have done in this case

to the rigorous and formal process that would be necessary to identify the cause of this crash, correct?

A No, I've not. My understanding is that other experts will be doing that.

Q And you do not have an opinion as to whether there was some fault that caused the throttle to stick, or some fault that caused the throttle to open and then stick in Ms. Bookout's car at the time of the crash, correct?

A I don't have an opinion that that's specifically what for sure happened. I do have an opinion that the design is unsafe and defective and that could certainly happen.

Q Well, we don't -- is it more likely than not? You haven't reach that opinion, have you?

A That's correct. I've not reached an opinion of more likely than not.

Q If you were to look at an unintended acceleration incident, there are three causes that you would have to investigate, right? You need to look at -- one would be mechanical causes of the event, correct, need to look at that?

A I'm not quite sure of my role, because I'm not here to represent myself as an accident investigation expert. So I can answer based on what I know, but I don't feel comfortable opining what you would do in an accident

investigation.
Q I believe you've testified previously the one thing that you want to look at is the mechanical causes of the accident; do you recall that?
A Subject to what I just said, mechanical cause could certainly be a cause.
Q And another thing you would want to consider would be the electronic or electrical cause, correct?
A Electronic, electrical, including software, that would be something you would consider.
Q And the third factor would be to consider human causes of the crash, right?
A Human causes could also be a cause of the crash. Yes.
Q And human causes would include errors in pedal application, correct?
A My understanding is that's something you would consider. Yes.
Q In fact, you have done some reading in the field of unintended acceleration, have you not?
A I've done some reading. Yes.
Q And I think you have looked at the phenomena of pedal misapplication to some extent, have you not?
A To some extent.
Q So I believe you told us in a prior deposition that

you had an interest in unintended acceleration for several years; does that sound right?

A I would like to see the deposition and the quote, please.

Q Okay. If you can -- you have it up there. Turn over to page 256.

A Okay. I'm at that page.

Q You're at that page? If you turn and look at line 9.

A Yes. Okay. I see the --

Q See the answer on line 16:

"I read plenty on that topic."

A Yes.

Q And among other things that you read on that topic, being unintended acceleration, you've -- didn't you tell us that you reviewed several studies by NASA and NHTSA? If the you want to refer to it, it is page 254.

A I recall taking a look at those studies. Yes.

Q On page 257, didn't you tell us that you reviewed several NTSB studies on pedal misapplication or specific accidents involving unintended acceleration?

A Sorry. Page?

Q 257, line 10.

A Right. And what I said was I didn't recall specifically if they were NHTSA or NTSB, but those would be

the kind of studies that I was look at.

Q And I believe in the course of that deposition were you not asked to take a look at an NTSB study on pedal misapplication from 2009?

MR. PORTIS: Your Honor.

THE COURT: Please approach.

(The following bench conference was had outside the hearing of the jury:)

THE COURT: Mr. Bibb, you have to ask him a question first. You can't ask him what he said in his deposition. Ask him a question first. If he doesn't answer the way that he did in the deposition you can use the deposition.

MR. BIBB: I will be glad to do that.

MR. PORTIS: Secondarily, your Honor, the question about a pedal misapplication is beyond the scope of direct examination.

MR. BIBB: That is fair game.

MR. BEASLEY: He is not an accident reconstructionist. And he is not put up for that.

MR. BIBB: But he has read theses studies.

THE COURT: Did he give an opinion on this in any of these cases?

MR. PORTIS: No, ma'am. It is not in his report.

THE COURT: Did he testify at --

MR. TAWWATER: Here is what counsel is about to law this into, your Honor. If he starts going into other cases and start talking about this stuff, we will start going into other cases.

MR. BIBB: I have attempted not to use that name. You have asked me which deposition he is reading from. This is what I want to refer to it. I want to show his bias.

THE COURT: What are you reading from here?

MR. BIBB: I want to read that's something I've never really bought into it. It is the 2009 NTSB study on pedal misapplication.

THE COURT: So that's you're reading him?

MR. BIBB: That is the quote from the study. And I assume that he read that before. I didn't ask him for it. That's certainly something that he said a lot, And I frankly never bought into that. I want to show bias on this witness's part.

THE COURT: Okay. Okay.

MR. PORTIS: No objection.

(Within hearing of jury:)

Q (By Mr. Bibb) What I would like to ask you, Dr. Koopman, if you will take a look over at page 268.

MR. PORTIS: Same objection, your Honor.

THE COURT: Just ask him the question.

MR. BIBB: I just want to sort of set him up so he won't have to ask me where to look.

Q (By Mr. Bibb) You were shown --

THE COURT: Mr. Bibb, the way to do this is just ask him the questions about the study. If he doesn't and if need to use -- please approach.

MR. BIBB: Let me try again.

THE COURT: Don't just ask him questions out of the deposition.

Q (By Mr. Bibb) My question to you, you've never, Dr. Koopman, bought into the -- really never bought into pedal application as the only reason for unintended acceleration?

A Since we have been talking about this study, I remember reading this study. It was a study from fairly recently, but it was only talking about cars that were designed before electronic throttle control. There were two of the references that were early. One I said I didn't know. After the deposition, I went and looked it up, and it was an even older car.

We're talking about a study here that found that pedal misapplication was a common cause for unintended acceleration on cars that didn't have computers in the throttle control. Then what I said was I never really bought that it's the only reason for an unintended acceleration; that's what I said.

I didn't say I ignore human -- unintended acceleration from pedal misapplication. What I said was if somebody tells me for here it is always the driver who made a mistake, there is no way the software could do that, I don't believe that.

Q Do you know of a way of pressing on the brake pedal to cause the vehicle to accelerate?

A I don't know of a way that solely pressing the brake pedal causes it to accelerate. What I do know, what I've seen from analysis from other experts is there is some situations that failure to release the brake pedal can result in a scenario where the car accelerates even though your foot is on the brake. That is a fine point that I really would rather have the other experts testify about.

Q Merely just my simple scenario of just stepping on the brake pedal, do you know of any way that would cause the vehicle to accelerate?

A If stepping on the brake pedal somehow activates a software bug in the ETCS, which is monitoring the brake pedal, it could possibly do that. But I can't lay out a specific mechanism for that.

Q Did you not tell us in your deposition that none of the electronic failures that you have described has a direct effect on the hydraulic brakes? Correct?

A So this has been in a couple of depositions. I

don't know of any electronic failure that would directly affect the hydraulic brakes. But there can be indirect effects in the following way: If an electronic failure, software or hardware failure causes the throttle to open, my understanding is that the vacuum depletion reduce brake effectiveness. So I would consider that an indirect effect.

Q My question is then the converse, meanly stepping on the hydraulic brakes, does that have anything to do with causing the throttle to open?

A I'm not aware of a specific scenario that causes that.

Q The hydraulic brakes are mechanical and hydraulic in nature, are they not?

A They're mechanical and hydraulic. However, when you press on the brakes it also activates brake switches. Those brake switches do go the electronic throttle control system; that's why my answer has the carve out that there is always a possibility of something.

Q We will come back to the brakes switches and their effect on this system right up here in just a few minutes. You have not tried to reconstruct the throttle angle of Ms. Bookout's vehicle at the time she was coming down the ramp off of Highway 69 on Texana Road, have you?

A I have not.

Q And you haven't formed an opinion as to what angle of throttle is necessary to allow for the depletion of vacuum assist to the power brakes caused by pumping the brake pedal, have you?

A I have not. Other experts are looking into that.

Q Now, you've talked in -- and I would like to go back and take a look at some of these slides -- I will use mine up here -- about some of the things that you have put in your report. One of them that I would like to going to is this slide about how often the random faults happen. And are you saying down there that you have a UA event every 11.6 days?

A That's a dangerous fault. There are probably other dangerous faults other than wide-open throttle UA. But these are general numbers, so this is not specific to the Toyota ETCS, but rather industry standard numbers that when you do this will analysis I would expect a dangerous fault every 11.6 days.

But there is a slide I skipped that is very relevant to this, and it is that a dangerous fault can result in a UA, but that doesn't mean that there is a crash and somebody dies. There is a notion of a fault creates a hazard, a hazard is dangerous. That is an incident, and an incident is something could go wrong but maybe you catch a lucky break, maybe you don't. So that number is about

incidents, not about accidents.

Q And I want to make it clear to the jury: You're not saying that you have a UA event every 11.6 days because of all the stuff that you talked about today, right?

A What I'm say --

Q Yes or no on that, and please explain. You're not telling us that, are you?

A I believe I'm saying yes, but in a very constrained way. The very constrained way is that these are standard numbers. If I saw a system like this, in general someone said, Here is a system, here is the chips they have, I would say, you know, that's about the number that I would expect to see, but if you want an exact number you would have to go a lot more detail.

I'm not saying that is the exact number. The point is, and it says at the bottom, the point isn't the number. It says the numbers are not approximate. The point is you can expect it to happen. It is not once every hundred years, it is on a regular basis. That is the point of this slide.

Q Let's say this 2005 Camry -- and I would assume and it has now been on the road now for eight years, you would expect to see more and more of these incidents occurring from this 2005 Camry, wouldn't you?

A I would expect to see a lot of incidents happening

based on this. The thing that I have not accounted for is tha the failsafes are going to be somewhat effective and reduce the collapse of the incident down to an, Okay, it is no problem, and I haven't put a factor in. That is saying I guess it is more appropriate to say I would expect the failsafes to be exercised that often. To the degree they're not effective, you will get things that will punch all the way through to an accident.

Q We will talk about those failsafes, because we did kind of skip over that in your slide show. Do you know Professor Paul Fischbeck at Carnegie Mellon?

A I've heard his name. I have not met him personally.

Q He is like in their statistics department, right?

A That's my understanding.

Q Have you seen his analysis where he went back and counted to see the number of complaints about UA and its correlation to the publicity?

A I've not read that work. I understand it exists.

Q And you would agree with me that after the publicity about Toyota UA died down in the spring of 2010, the number of complaints went back to where they were before the publicity?

A Well, I'm nat a statistics person.

Q Well, you have given us statistics here though.

A As an ordinary person, I would have to point out

that in making that argument we're talking about the number of reports complaints, not the number of times that it actually happens.

MR. PORTIS: Again, this is beyond.

MR. BIBB: Think it is impeachment of his statistics that he put up there.

THE COURT: Overruled.

MR. PORTIS: So we are going to get into each side's statistics now?

THE COURT: Overruled.

MR. BIBB: I have two slides.

Q (By Mr. Bibb) What happened to the incidents? Have they stopped? I'm sure you will agree with me Toyota hasn't found and fixed the problem, have they?

A So this isn't my data, this is the first time I've seen it. But I would say as a nonexpert in statistics to me it is just as plausible that without the publicity they stopped bothering to report it. I know plenty of times my computer crashed and I don't call it in.

Q He just counted the number of claims that came in and sort of timing. In other words, when they were reported versus when they occurred. The lighter purple or blue is when they were reported, and the darker purple is when the incident occurred. Do you understand the chart?

A I understand. But my numbers are not about this.

My numbers are about something dangerous happened. If you press the brakes and it immediately goes away, and it doesn't happen again. You say, I'm not going to waste hours of my life calling this in and reporting it. So these numbers are not comparable to the numbers I was showing.

Q Here is another one, Dr. Fischbeck. This was a presentation he gave to the National Highway Traffic Safety Administration. Again, here we are counting back months from the date of the news coverage, and then afterwards.

Let's go on. Now, I would like to talk to you a little bit about the NASA report. You referred to it a lot in your slide show.

A Right. My slide show referred to the main NASA report and also to appendix A on software.

Q And I will just use some of the pages that you actually cited in your NASA report. Here it is. First of all you have the line here that NASA says the Toyota electronic throttle control system has a dangerous single point of failure. That sentence never appears in the NASA report, does it?

A It does not appear in those words. They use words that to me as an expert in software, that's what they were intending to communicate.

Q That's what you say it says, that's not what NASA

says?

A They do not use those exact words.

Q And then you use this quotation here from -- and you have it cited on pages 65 and 67 to suggest that it's a -- to say that it is a simplex system, don't disagree, they use that term. But maybe what we ought to do is look at the language that appears right around the quotes that you have there.

And this is -- let's go to the next page. Can you make the top paragraph there bigger. This is from page 66, and you have got the quote here about the sub CPU and its path to disengage power to the H-bridge controlling the throttle motor should a fault occur architecturally. I think you even read this to the jury:

"Architecturally the system appears as a simplex system with disengagement monitor and diverse safety."

Is that right?

A That's what it says.

Q The next sentence, though, goes on to say:

"Without power, the throttle cannot be driven, and dual springs return the value to a near-idle position as required by FMVSS 126, 6 1/2 degrees from fully closed." So there is a mechanical backup to close the spring that closes the throttle, two springs to close the throttle if there is some failure to the throttle motor.

Once power is cut off to the throttle motor, it doesn't stick there, it closes, correct?

A If the failure of the ETCS results in the power to throttle motor being cut that's what happens, but that's not necessarily how it is going to fail.

Q And you know that there are failsafes to cut power to the throttle motor, right?

A There are failsafes corresponding to the built-in tests that I explained, and they will sometime cut power to the throttle motor, but it is not guaranteed to happen every time.

Q Every time -- now, you know, because we will talk about it in a minute with about Mr. Barr's taking or removing some lines of software code and some testing that was done that you cite in your first report on this that took out the failsafes. And you know from the testing done, though, that every time the brake was applied in those tests the throttle motor power was cut and the throttle returned to the closed position, correct? And we will talk about that a little bit more. You know about that?

A There were a bunch of pieces to that, but I think what we're getting to on that is there were many tests that were run. And if you did something like kill a task -- I talked about task -- they killed a task and said, Look, you

have unintended acceleration. And if eventually get around to pressing the brake, with one exception I will get to, it will then save the engine. But sometimes that happened seconds and seconds and minutes later.

If you waited all day to press the brake, it was going to wait all day before it shut down. So the driver had to resolve the UA by pressing the brake. There is also, one of the slides that we skipped, talked about testimony from Mr. Arora that there is a case where if your foot is already on the brake and one of these tasks dies, if you don't let all the way up on the brake, if you keep your foot on the brake, having your foot on the brake will not resolve UA, the UA will continue. In that case, you have to remove your foot all the way from the brake to get the car to stop.

Q Now, in all the tests that were run by Mr. Loudon that you referred to in your report and Mr. Barr, the throttle closed every time within a blink of an eye, didn't it, when the brake was applied?

A That's correct. But the context is the UA occurred, the system was experiencing the UA for however arbitrary long time. When you eventually got around on those tests to pressing the brake then the failsafes kicked in.

Q This goes on and talks -- if we can go back a page to the colorful diagram because it talks about this

diagram. The next couple of sentences. And it shows various ways that it is going to cut off. This is the overall architecture for disengagement, diverse safety, what you were talking about, right?

A Sure. This is how NASA detected the failsafes.

Q And you had failsafes when there was a disagreement between the monitor and main CPU and the brake was applied power was cut to the throttle motor, throttle motor closed. If there were further problems, you always had the brakes which would stop the vehicle, shift to neutral, ignition off. This almost looks like your fault tree there, doesn't it?

A This certainly does look kind of like a fault tree. I would point out that the --

Q There is not a question about what you want to point out?

THE COURT: You can bring it up on redirect.

MR. PORTIS: What exhibit is that?

MR. BIBB: That is page 65 from the NESC, the NASA engineering report.

Q (By Mr. Bibb) Now, if we can go back one more page Mr. Doyle. This is the system failsafe architecture that you lifted the quote that you have your slide from?

A Looks about right. The font is pretty small from here.

Q We will blow that up here. The NASA, the National Aeronautics and Space Administration, you see them at the top there, but they have the shaded box. And they would periodically include findings during the course of a report, didn't they?

A Yes. This is a summary box of findings.

Q Right. And the finding in this section of the report is that:

"Safety features are designed into the Toyota Motor Corporation electronic throttle control system to guard against large throttle opening, unintended acceleration from single and some double electronic throttle control system failures. Multiple independent safety features include detecting failures and initiating safe mode such as limp home modes and fuel-cut strategies."

That was the finding that NASA made; isn't that correct?

A That is one of their findings.

Q All right. You didn't show that to the jury as part of your PowerPoint. Did you?

A No, I did not.

Q Now, let me just touch for s moment on fault containment regions. You talked about fault containment regions. All you have done there is to point to a location

where things are in the same area. Correct?
A Area is a little loose. In the same chip.
Q Do you call them region?
A Well, region is the term of art. But, for example, the A/D converter is all in the same portion of the same chip, for example.
Q But you did not look to see what Toyota has done to mitigate faults in that area or in a region, have you?
A I looked at the FMAA, which we saw. I looked at many of the failsafes. But the fact of the matter is it doesn't matter what you do to mitigate it except by putting in a second independent fault containment region. There is no magic that makes a single fault containment region safe. The only way to fix it is a second one.
Q Have you examined the electronic throttle control systems of any other vehicles sold in the 2005 model year to see if they have separate fault containment areas for the analog to digital converter?
A I have not looked at other 2005 model year vehicles.
Q All right. So you don't know if anybody has the system that you say everybody has got to have, do you?
A I don't know of specific examples in that particular model year.
Q The answer is I don't know, right? I don't know if anybody has this separate analog to digital convertor,

fault containment, whatever you want to call it?
A I don't know for myself, but I know if they were following MISRA standards it would require them to have that.
Q Now, you talked about the analog-to-digital converter for a long time, called it a single point failure; is that correct?
A That is an example of a single point failure in the Toyota ETCS.
Q Okay. Have you done any testing of vehicle components or systems to see what effect Toyota's failsafes and system guards would have on an analog-to-digital converter failure?
A I've not myself done testing. Other experts have done testing. But I have relied on the academic literature that says that architecture pattern, building it that way can be expected to result in UA.
Q But, again, the question simply to you was have you done any testing and the answer was no, correct?
A Not myself.
Q All right. Now, you're not, again, not telling the jury, though, that more likely than not an analog-to-digital converter failure caused Ms. Bookout's crash at 6:30 p.m. on September 20, 2007, are you?
A I'm not saying that.

Q And, in fact, you have not found any -- you're not telling this jury of any other single point of failure that in your opinion more likely or not caused Ms. Bookout's crash in September of 2007, are you?
A No.
Q And have you heard of a mitigation strategy that Toyota has called the Toyota system guard?
A I've heard of the three system guards.
Q A system guard one, system guard two, and system guard three, are they not?
A Yes.
Q You don't know how those system guards work, do you?
A I've read up on them in general. It is looking for mismatches between pedal and throttle.
Q You haven't personally tested any of the system guard mitigation strategies, have you?
A I've not tested them.
Q And you have never suggested that Toyota's system guards are defective, have you?
A I've not suggested that they're defective in terms of doing what they're supposed to do. But I have suggested they're defective in the fact that they're not a complete safety system.
Q Have you testified that I don't believe I ever said the control system guards were detective?

A Can we have the reference, please.
Q Page 366.
A This is still the Van Alfen?
Q Yes. And I'm not asking you about the Watchdogs or the monitor actuator safety architecture. All I want to know about is the system guards?
A What I said was I don't believe I ever said that the system guards were defective. When I said that it is in a very narrow sense. What I mean is the system guard is designed to implement certain failsafe functions. But I don't have any belief they failed to do what they're supposed to do.

But what I also said today was that doesn't make them complete failsafes, they still leave holes. There is a difference between saying they are not defective and saying the ETCS is safe. I can say both things at the same time, it is still consistent.

Q In any testing of the Toyota electronic throttle control system that you're aware of, have the failsafes ever failed to kick in when the brakes are applied or released?
A I don't know of specific testing that if you cycle the brake switches from on to off or from off to on, I don't know of any testing that failed to engage a failsafe under those conditions.

Q You talked about the MISRA coding guidelines an awful lot today. You can't trace any alleged violation by Toyota of any MISRA guideline as the most likely cause of Ms. Bookout's crash in September of 2007, can you?

A I can't go to a specific rule violation and say that's what caused the crash.

Q Any rule violation, you can't say that?

A This is no rule violation that I can find that caused the crash. But I should say that doesn't mean I tried and didn't find one. I just haven't done that work.

Q And you were here for Mr. Ishii's videotaped testimony today, were you not?

A Yes.

Q And you heard him say that at the time only five automobile manufacturers were compliant with MISRA coding standards. Do you remember that?

A I remember him saying that.

Q Okay. Now, you talked -- you mentioned earlier today that in talking about coding that people make mistakes. Do you remember making that statement?

A Sure.

Q People make mistakes?

A Sure.

Q You said you miss things when you're proofreading. Do you remember that?

A Happens to me all the time.
Q You say that is the reason you want peer reviews. Do you recall that?
A That is a motivation for peer reviews. Absolutely.
Q And you know that -- he is still here -- Mr. Michael Barr is one of the plaintiffs' experts in this case, do you not?
A Yes.
Q And you know, and I think you referred to Mr. Barr, as the plaintiffs' software witness in this case; is that right?
A He is a software witness. I consider myself one as well.
Q Right. And Mr. Barr, perhaps the jury knows this, he does have access to the Toyota source code; does he not?
A Yes, he does.
Q And you know that initially Mr. Barr removed about 20 percent of the software code before he did his review of the source code, correct?
A This is all secondhand from reading depositions and so on. I know there was an incident of that nature.
Q Let me ask a different way. You understand that he removed about 20 percent of the software code, correct?
A I understand that he was put in a difficult situation and that he did some analysis that did not

include some of the source code.

Q And you understand that that included -- the lines of code that were removed were lines of code that were relevant to some of the safety measures in the Toyota system, correct?

A I recall that being discussed, but I didn't dig in to make sure of that for myself.

Q And you issued an earlier rebuttal report in which you stated in paragraph 95 of that report that Mr. Barr's monitor CPU report, that monitor CPU, that sub CPU that we saw the slide on, maybe help refresh the jury's recollection. I think we have a picture of it here in one of your slides.

That that monitor CPU that I think is identified as sub CPU up there, he identified as another lack of independence in the throttle motor failsafe arrangement because he reported that the monitor and the main CPU did not independently cut power to the throttle motor, and the main CPU or the throttle motor forming another single point of failure. Do you remember that?

A I would like to see the reference that comes from.

Q Okay. Let me get you the report. May I approach?

THE COURT: Yes.

Q (By Mr. Bibb) I made it easy I flagged it and highlighted it for you.

A Thank you.
Q Since I stumbled through reading it, read that back to me tp make sure I got it right.
A This is from the Van Alfen report, which is not the report that I used in this case. And paragraph 95 in my report said:

"Mr. Barr's CPU report identified another lack of independence in the throttle motor failsafe arrangement.

He reports that the monitor and main CPUs do not independently cut power to the throttle motor, forming another single point of failure."

And I refer to Barr monitor CPU report in the Van Alfen case, page 20.

Q All right. And after you wrote that -- what was that dated?
A This is was September 17, 2012.
Q Just a year ago after you wrote that you learned that the monitor CPU can independently cut power to the throttle motor setting the vehicle at a 6.5 degrees failsafe; isn't that correct?
A I don't remember the specific numbers you're referring to. What I learned was that this paragraph was based on a report. And the opinion I was basing it on turned out to be incorrect.

Q It turned out -- and you relied on Mr. Barr a number of times through this PowerPoint show, haven't you?
A Yes. And I've gone through fastidiously in the report for St. John, which is the basis for this, to make sure that none of my reliances on that one small part of all Mr. Barr's work that turned out to be revised.
Q So you know that that conclusion in that report is wrong, right?
A Which conclusion. Which report, sir?
Q Paragraph 95 that you read to the jury is wrong?
A That paragraph 95 is incorrect because it was based on an incorrect opinion. But it does not affect, as far as I know. Any of the other opinions in any of my other reports.
Q Well, you say you don't rely on that, but you do rely on a report that you prepared for St. John?
A That's correct.
Q And I show you your report from St. John. And I want to direct your attention to -- why don't you read that to yourself and tell me, Dr. Koopman, whether you were relying on that work for your work in that report, the earlier work for your report in that case.
A That's what I said here. I'm reading part of it:
"I've endeavored to only refer to opinions of other experts which I believe also applied to the St. John

vehicle or likely be reiterated."

The reason that I did that was I was preparing this report while Mr. Barr and his associates were preparing their reports. So I didn't have the new reports to refer to, so I used their old reports. But I said:

"Which -- only which I believe also apply."

It was clear in my mind that that one paragraph didn't apply. It turned out that that wasn't true, so I'm not relying one that part of that one report.

Q And, in fact, Dr. Koopman, you know that that mistake by Mr. Barr has been proven not to occur in Toyota vehicles equipped with the failsafes, correct, which is all Toyota vehicles with electronic throttle control?

A I recall that being the result, but I don't remember exactly where I saw it or how I saw that.

Q Okay. And you know that every time the brake pedal was pressed the vehicle went into failsafe, correct?

A With the exception of the quote from Mr. Arora's deposition which I refer to which requires the brake pedal being released.

Q But the testing that was done by Mr. Loudon, who is also an expert in this case using Mr. Barr's work, found that every time that on that chassis dynamometer the brake pedal was depressed, the vehicle went into failsafe, correct?

A As I was going to complete my sentence, yes, the testing showed that.

Q I apologize for cutting you off there.

MR. BIBB: One moment, your Honor.

Q (By Mr. Bibb) Is the monitor CPU source code important?

A I would say that if you wanted to prove the system was safe, first you would have to make sure everything else was safe and then you would have to look at the monitor source code. So I consider it important because if there is a software defect in the source code that makes the system unsafe then that's it, it is unsafe.

If you don't have the monitor CPU source code, you don't know whether that potential source of hazards has been eliminated.

Q Okay.

MR. BIBB: One moment, your Honor. I believe, Mr. Koopman, you can probably catch your plane.

Thank you so much, Dr. Koopman, I appreciate your coming. No further questions. Your witness.

THE COURT: Redirect.

MR. PORTIS: Yes, ma'am.

REDIRECT EXAMINATION

BY MR. PORTIS:

Q Dr. Koopman, I want to clear up something about your

role in this case for the jury. Your role in this case was to evaluate software and the hardware on this particular Toyota Camry, correct?

A That's correct.

Q Your role, and ultimately what you determined, am I right, is what?

A I determined that it's unsafe and defective.

Q You understand that other experts will testify about causation; am I right?

A That's my understanding. Yes.

Q You understand that Mr. McCort already testified in this case and provided his accident reconstruction and provided causation opinions in terms of the throttle being open, the emergency brake being pulled, and that is not your role, right?

A That is my understanding on both counts.

Q And you understand Mr. Barr will also talk about causation issues, correct?

A Yes. That is my understanding.

Q So that's just not your role, but I think did -- but I think what you did testify about is that your opinions are consistent with the facts as you know them in this case; is that right?

A That is correct.

Q Can you describe that, please.

A So what my testimony says is that it's defective, it's unsafe. And unsafe in this context means can reasonably be expected to produce unintended acceleration due to one of these faults happening. And from reading the deposition of Ms. Bookout and reading about the accident, there is nothing that I saw in there that precludes software or hardware defect from having caused this accident.

Q Do UA event occur in Toyota Camry vehicles?

A I think it is pretty clear that UA events occur. Yes.

Q What is the Van Alfen case about?

A The Van Alfen case was about.

MR. BIBB: Objection, your Honor. I didn't go into any of the facts of those cases. They brought up the name of the case.

(The following bench conference was had outside the hearing of the jury:)

MR. BIBB: I didn't bring up the facts of that case. They interjected the names. I was trying to be so careful about saying a prior report, as we previously discussed we would handle that. And they interjected this. I don't think they get to open the doors themselves.

THE COURT: Didn't you question him about some of his result in the Van Alfen? Shouldn't he be able the tell

them? Which report were you critiquing him on for having replied on that Barr issue?

MR. BIBB: It is in the Van Alfen case. But I began by referring to it until they asked what case, deposition is it from, then he interjected the name of the case.

THE COURT: Weren't you asking him specifically about his findings in this case?

MR. BIBB: I was. In all three cases he relies on all this work for his opinions in this case.

THE COURT: I will allow just very limited on the facts.

(Within hearing of the jury:)

Q (By Mr. Portis) What are the facts as you know them in the Van Alfen case?

A It has been a while, but as I recall Mr. Van Alfen and three passengers were driving on a highway, and they got off on an exit ramp, and they were unable to stop the vehicle despite applying brakes. Witnesses actually saw brake lights. And there were unfortunately two fatalities. So coming off an off-ramp on an interstate highway and then they crashed into an embankment at the end of the off-ramp

Q What do you understand the facts to be in the St. John case?

A In the St. John case, it was -- it was more of an

issue of she was at a stop sign, and she released her foot from the brake, and it took off through the schoolyard and ultimately hit a brick -- went through chain-link fence, hit a tree, and crashed into a brick pillar.

Q Now, we talked -- he showed some -- I can't remember his name here, cohort at Carnegie Mellon who does statistics?

A Fischbeck, I believe.

Q Thank you. What are statistics?

A You're out of my area.

Q Okay. I won't ask.

A Has to do with numbers.

Q Let me give you a number. During -- Mr. Lentz is the president of Toyota Motor Sales. He testified that there was a 400 percent increase in Camry unintended acceleration events during the introduction of the electronic throttle control system. Would that number surprise you based on what you observed?

A Based on what I've seen, that would be no surprise at all.

Q Now, the NASA report, I want to talk about that because he showed a few things about the NASA report. Is it without question that NASA found a single point of failure in the Toyota system?

A This is no question in my mind that they found and

reported upon a single point failure in the Toyota ETCS.
Q And any system that has a single point of failure what is the problem with it?
A Problem is it is unsafe.
Q Now, he asked you some questions, and he says that in their systems that sometimes -- he used the word sometimes -- the power is cut. Did you have any difficulty with the word "sometimes" in relation to a critical safety system?
A Sometimes doesn't cut it. If you're exposed for hundreds of millions of miles saying, Well, it is only every 10 million miles, that is not good enough. You to have extraordinarily high scientific notation once in -- so for airplanes, for cars too, they use numbers like once in every billion hours it is okay for something bad to happen, once in every billion, with a B hours. That depends if that is sometimes or not. Most people's idea of sometimes is a lot more frequent than that.
Q Then he asked you some questions about testing that was by a Toyota expert and by Mr. Barr. Did I understand correctly in tests run by Toyota experts and tests run by Mr. Barr that UA events occurred during those tests?
A That's my interpretation of the test results. Yes.
Q I want to show you page 65. He showed it to you and you wanted to point out something, and I wanted to give you

the opportunity to do that. This is -- tell me what you wanted to point out, sir.

A So what I wanted to point out was that these failsafes are in the same fault containment region as the software that is presumably making the system unsafe. So, yes, they have failsafes, and there are these counter measures pressing the brake. This is all after the UA happened and you're trying to prevent it from getting worse, from being an accident. You want to bring the vehicle to a stop.

But what is happening is all these and gates -- you see these ands -- all three things have to be a problem, but they're all being controlled by the same place. From a fault-tree point of view, it is not a proper fault tree, because it is one place that can make all the and gate things go bad; that's what I wanted to point out.

Q Thank you. I guess after the vigorous cross-examination are any of your opinions on pages 1, 2, 3 that you provided testimony on today, have they changed in any way?

A I would not change my opinions one bit.

MR. PORTIS: Thank you, your Honor.

THE COURT: Dr. Koopman, you may step down, sir. do we have a witness we can do in 45 minutes?

MR. BAKER: Pretty close.

THE COURT: Members of the jury, do you want to stick around for 45 minutes?

(All jurors respond in the affirmative.)

THE COURT: What witness are we calling?

MR. BAKER: Keiichi Osawa, K-E-I-I-C-H-I O-S-A-W-A.

MR. TAWWATER: Now that the jury knows it is a video do they want to reconsider?

THE COURT: No, too late.

(Whereupon, an off-the-record discussion was had.)

THE COURT: Ladies and gentlemen, it is 4:20. We're going to break for the day. And, again, I want to emphasize to you: Do not do anything at all over the weekend to do any research on this case. You have heard the names of other cases mentioned today. You're to do absolutely nothing. Should there be any news reports, any newspaper reports -- I know my office has received some phone calls about this case. Do not read anything whatsoever about this case or any other case that may involve these issues.

With that said, I wish you a good weekend. And we will see you Monday morning at 9:00. All rise while the jury exits.

(Whereupon, the jury exits the courtroom.)

THE COURT: We're back on the record.

MR. TEAGUE: Your Honor, I want to renew our motion that was previously filed to exclude the testimony of Dr. Koopman. He testified while ago that his role in this case was to evaluate the software and provide an opinion that it was unsafe and defective. His safety analysis is an unsound unreliability methodology. In fact, his methodology is his own method, as he testified to, which is the same thing he is critical of Toyota for.

With respect to this case, he has not inspected the Bookout vehicle, he has not been to the scene. He has not inspected the actual software which is at issue which he wants to opine on as being unsafe and defective. He has done no testing. He admits that the mitigation safe guards that are built within the Toyota software have worked every single time and have defaulted to a failsafe when tested.

He admitted that he could not say that it was more probably true than not that any defect in the software was related to this accident. Moreover, any opinions that he's providing were based on testing of Barr, which he acknowledged the testing was wrong. This is exactly the type of testimony that should be excluded. He came in here today and he said, It's unsafe and it is defective because I said so, and he doesn't have the foundation to provide that opinion.

THE COURT: Okay. Do you want to say anything

other than adopt what you had in your motions in limine?

MR. BAKER: I just adopt what we put in our motions in limine and oral argument that we already had on the motions, your Honor.

THE COURT: I will overrule your objection. And we need to talk about exhibits.

MR. BAKER: We would offer MISRA-C 3106.

MR. BIBB: Only for identification. It is a learned treatise.

THE COURT: What is 3106? What is it.

MR. BAKER: MISRA-C guideline.

THE COURT: Oh.

MR. BIBB: They're certainly not a statute or a standard or anything more than guidelines which have got to be treated as a learned treatise, I believe.

MR. PORTIS: They are standard.

MR. BIBB: Not adopted by any governmental agency that I'm aware of.

MR. PORTIS: They're not a treatise.

MR. BIBB: And the uncontroverted testimony is that only five manufacturers even follow them.

MR. PORTIS: Well, that is true. But that's --

MR. BIBB: And they're not required to follow those guidelines, your Honor. It is just a learned treatise.

THE COURT: Remind me: Is learned treatise not an exception to the hearsay rule?

MR. BIBB: That's why I said you can mark it for ID but it doesn't go to the jury.

THE COURT: Let me ask: Are we going to do all documents that the experts have relied upon and send them to the jury, or is there an independent basis other than he relied upon this?

MR. PORTIS: For instance -- well, maybe it does. But I think it goes back for a different purpose. This is -- there are documents that, SAE papers they were asking Mr. McCort about that are part of a -- that are part of some sort of papers that are generated.

MR. BIBB: I take that back. It is a little different than the federal. If admitted they may be read into evidence, but may not be received as exhibits.

THE COURT: Where are you reading?

MR. BIBB: Learned treatise exception, which one it is 2803.18. It says they can be shown to the witness and cross-examination, relied upon the witness in direct examination. But thin it goes on to say if admitted they're not to be received as exhibits.

MR. PORTIS: This is referring to --

MR. BIBB: Learned treatises.

THE COURT: Treatises, periodicals or pamphlets.

MR. PORTIS: I don't think it is a learned treatises, I think is this issue. I think this is a standard and guideline that he's talked about. Learned treatise would be something from SAE.

MR. BIBB: I don't think this is any different. This is from whatever the Motor Industry Software Association --

MR. PORTIS: It is in evidence. The question is whether it goes back to the jury or not, and we would say it does, they say it doesn't. I don't think it is a learned treatise, but they think it is. I'm not real sure if that is defined or not and would leave it to up to the court's discretion on that.

THE COURT: Let me come back to that. I will reserve that. What else do we have?

MR. PORTIS: We have Exhibit 4229, which is a paper by Mr. Kawasawi (phonetic) which is normally a learned treatise but it is from a Toyota employee.

MR. BIBB: I think it is probably an admission, frankly, Judge.

THE COURT: 4229 will be admit.

MR. PORTIS: This is Exhibit 5696. Really what I was going -- this, again, is another Toyota document, part of overall group. I don't mind just pulling out the one document, or we can get the whole document.

MR. BIBB: I want the whole document in.

THE COURT: What number, 5669, and the whole thing is coming in. Court will admit Plaintiffs' Exhibit No. 5696.

MR. PORTIS: This is Exhibit 5682A.

MR. BIBB: This is probably is a learned treatise.

THE COURT: 5682A.

MR. PORTIS: I'm fine if we just don't put that back.

THE COURT: Do you want to withdraw it.

MR. PORTIS: Just that it's an exhibit but not sent back to the jury.

THE COURT: Do you want me to mark it as a court exhibit?

MR. BIBB: I think so.

THE COURT: I will tell you, I normally don't have a request to put the learned treatises in as court's exhibits. I'm happy to do it if you think you need it for appeal.

MR. BIBB: I think we probably have to have that for report for the record. Sorry, your Honor.

THE COURT: That's fine. So I will mark both as Court's 4. I don't know that the court's exhibits -- so I'm marking this entire document.

MR. ESDALE: That's appropriate.

MR. PORTIS: This is again -- I don't know what you're doing with CVs.

THE COURT: Marking those as exhibits.

MR. PORTIS: That is Exhibit 5648.

THE COURT: Is there an objection to his CV, Mr. Bibb?

MR. BIBB: I think we treat it the same way we did Mr. McCort marked as an exhibit but it doesn't go to the jury.

THE COURT: Okay. I didn't know that. Because you specifically wanted somebody's CV.

MR. ESDALE: I thought it was you that said they didn't go back.

THE COURT: No.

MR. BIBB: What is the court's general practice on that?

THE COURT: The general practice is that the CVs go back because generally my attorneys will waive going through all of the background because the CVs are there.

MR. BIBB: That is fine. I certainly think they need to be there for the record on appeal.

MR. PORTIS: That is a learned treatise.

THE COURT: Wait just a minute. Court is also admitting Plaintiffs' 5648, which is the CV of Mr. Koopman. And then this is another learned treatise?

MR. PORTIS: Yes, ma'am, 5670.

THE COURT: So the court is marking Plaintiffs' Exhibit No. 5670. But the court is marking it as Court's Exhibit 5, the learned treatise that is styled design -- or titled *Design by Extrapolation and Evaluation of Fault Tolerant Avionics*. And that's number 5.

Just for the record, number 4 the court marked as a court's exhibit is a document from the National Highway Traffic Safety Administration on the reported Toyota Motor Corporation unintended acceleration investigation as well as the appendix A software.

MR. PORTIS: The Exhibit 5649 is the MISRA guidelines.

THE COURT: And I assume they will be the same objection.

MR. BIBB: Same objection.

THE COURT: Okay.

MR. PORTIS: Then we have two more. Exhibit 5693.

MR. BIBB: No objection.

THE COURT: Court will admit Plaintiffs' Exhibit No. 5693.

MR. BIBB: And they have 5692. Our objection is to its translation because I think it is one of their translations.

MR. PORTIS: It is a certified translation, your

Honor.

THE COURT: The court will admit -- is this one of the e-mails?

MR. PORTIS: It is something he talked about that was part of his presentation that he relied upon.

THE COURT: And it has the certified translation?

MR. PORTIS: Yes, ma'am.

THE COURT: The court will admit Plaintiffs' Exhibit No. 5692.

MR. BIBB: I have 260.1 is the video that was showed the other day. And I understand we already have a ruling on that. To lay some more foundations for its admission.

THE COURT: This is the Cooper study video that they played.

MR. BIBB: It was 260.1 that differentiated from the written report. I also note it is 5755 on the plaintiffs' exhibit list, but we can use ours.

THE COURT: This is one that I am reserving to see if we will admit it.

MR. ESDALE: While we're on the subject, your Honor, if I can, this is -- the Koopman study, I don't believe anyone would argue would be considered if not a learned treatise a reliable authority. It was relied upon by the experts, and this is part of the Cooper study. And

as a result, it -- we should be treated just like the learned treatises and reliable authorities, it should not got to the jury for that very reason. Again, it is part of the Cooper study.

THE COURT: Okay. So you're basically making the same argument that he is making on these MISRA reports they should all be treated as --

MR. ESDALE: Reliability authority.

MR. BIBB: I would like to do research on that because I think it should come in, separate and apart. It is the background for -- there is no statement. I don't think it fits as a learned treatise there. It is a video that, frankly, the plaintiffs' counsel paid the research to be done? And it may come in as a representative admission.

THE COURT: Let me ask would these all be hearsay if it wasn't the fact that an expert was relying on them?

MR. CLARK: There is no statement. The rule defines the statement as an oral assertion; it certainly is not that.

THE COURT: Is it a learned treatise? It is certainly a statement.

MR. CLARK: No, it's not a statement. Because conduct is only a statement where the conduct is intended by a person as an assertion. That is 2801(A)(1)(C.) And I don't think there it is any argument that anybody can make

with a straight face that the conduct on that video was intended by the declarants as an assertion.

MR. BAKER: That's why you want a foundation laid.

MR. PORTIS: I would say this: The problem is completeness. Because the testimony in the case is there were hundreds of these tests run, and there was one, there was one where there was a pedal misapplication out of the hundreds and hundreds of tests run.

THE COURT: Do we have the entire test?

MR. PORTIS: I don't. If we're going to submit then let's put them all on a DVD.

THE COURT: So your objection is learned treatise and it is not complete.

MR. PORTIS: That's correct.

THE COURT: All right. I will note the objections.

I'm not ruling on anything today.

(Whereupon, court stood in recess until October 14, 2013.)

STATE OF OKLAHOMA)
)
COUNTY OF OKLAHOMA)

C-E-R-T-I-F-I-C-A-T-E

I, Karen Twyford, Certified Shorthand Reporter, in and for the County of Oklahoma, State of Oklahoma, do hereby certify that the foregoing transcript is a true, correct, and complete transcript of my stenographic notes.

I further certify that I am not related to any of the parties herein, nor am I interested in any way in the outcome of these proceedings.

WITNESS my Hand this _____ day of _____, 2013.

_____
KAREN TWYFORD
CERTIFIED SHORTHAND REPORTER
CERTIFICATE NO. 01780