2017 Embedded Systems Safety & Security Webinar Transcript

The following is a transcript from March 23, 2017.

Slide 1: 2017 Embedded Systems Safety & Security Survey

Stacy: Welcome and thank you for attending the Barr Group Webinar Release of our 2017 Embedded Systems Safety and Security Survey Results. My name is Stacy, and I will be your moderator for the next hour. For those of you live tweeting, you can see our Barr Group twitter handle on your screen now. Today's webinar presenter is Andrew Girson, the CEO of Barr Group.

This presentation will be approximately 40 minutes long, followed by a moderated question-and-answer session. If you have a question during the event, please type your question in the Q&A chat area located in the bottom left corner of the Webinato window. Our presenter will address the questions that appear most frequently during the Q&A session.

As we prepare to start the webinar, please make sure that all other programs on your computer and mobile device are closed for maximum efficiency of audio and video feeds.

I will now turn the presentation over to Andrew Girson, CEO of Barr Group.

Andrew Girson: Hi everyone, and welcome to the webinar on our 2017 Embedded Systems Safety and Security Survey. My name is Andrew Girson, I am the President of Barr Group, and I will be going over the results of our survey that we just recently completed.

Slide 2: About Barr Group

By way of brief introduction, Barr Group is a consulting firm that specifically focuses on the safety and security and reliability of Embedded Systems. We have a number of training courses that we do publicly and on-site all over the world, and a variety of consulting services that we offer. Anybody who is interested in that can go to our web site as noted on the screen or follow-up with me afterwards.

Slide 3: Webinar Format

Now just a brief overview of the format and outline for this webinar. First, we are going to spend a few minutes going over our methodology, explaining how we performed the survey, how we got our results. We will also provide some background demographic information on a general level regarding the respondents to survey; but the primary focus of the webinar will be the analysis of those results, and we will do an industry snapshot, provide some findings on safety, and some findings on security. Finally, we will wrap up with the announcement of the prize winners for the prizes that we gave away, and then we will finish with question-and-answer period.

Slide 4: Survey Goals

So this is our third annual market survey, and obviously our goal here is to deepen the knowledge of trends and practices in the industry, specifically for the Embedded Systems industry, and try to help us understand where we are, so that as an industry, we can potentially improve.

The survey is a deep dive on safety, reliability and security. It is a supplement to existing broad market surveys. As you may know, there is a number of media organizations and others that do broad market surveys. Ours tend to be less vendors focused, but similar demographics.

Slide 5: Survey Methodology

Now as far as the survey methodology is concerned, the survey itself was opened a little over three weeks from mid-January to early February. We want to reach obviously, a very large number of people with the embedded system's space to get as good demographics as possible. So we sent out quite a few email invitations. We use social media as well to get the word out; and we provided an opportunity and an optional prize incentive. If respondents gave us their email address, they could potentially win a prize. But that was totally optional, as the survey could be entirely independent and anonymous.

Slide 6: Worldwide Response

Okay, so now let's get to some general demographic information on the survey itself, so everybody can see where everybody was coming from in terms of respondents. We are on slide 6 now; so a total of 2,022 surveys were completed, and of those respondents, as you can see, about half of them came from North America, about a quarter of them came from Europe, 14% from Asia, and then the rest of the world was 9%. So a relatively good geographic distribution around the world.

Slide 7: Qualification of Respondents

For us it was very important that the respondents were qualified. We knew that of the 2,022 respondents, there were going to be some that didn't necessarily represent what we were looking for in terms of active professional engineers. So there were some disqualifications that we ended up having to do, in terms of the full numbers.

As you can see first, if the person did not have paid design experience, for example, if they were in college; their results were eliminated from the survey, that was 147 people. We also had 80 respondents that were not directly involved in designs. This was management, corporate management, or other management in the company. And then finally, there were 69 respondents, who were rather vague on their current project details, so we assumed that they were not really doing hardcore design. You subtract all of those people out, and you end up with 1,726 qualified active professional engineers, who were the results of our survey. That's a very good number, we are very happy with that number. With such a high number, we get good study repeatability and very low margin of error, statistically.

Slide 8: (Some) Participating Organizations

Just to give you an idea of some of the organizations that participated; there were over 1,000 companies that participated in the survey, and shown on this slide is just a subset of some of the companies, some of the larger companies that had multiple respondents participating; but over 1,000 different companies participated in terms of the results of the survey.

Slide 9: Company Sizes Represented

Okay, we are now on slide 9 and let's dive into some of the general demographics for the overall industry. As you see here and in overall, we will be basing our responses here and our analysis on the 1,726 qualified active professional engineers doing work today. This slide gives you an idea of the breakdown of the company sizes and how they are represented in the survey. From a low of one to nine employees within the total company, up to over 10,000, and this represents the number of people that filled out our survey.

On the right, you see the number of engineers within companies and you see a relatively flat distribution, certainly more of an emphasis on a smaller number of surveys. Obviously, teams are still relatively small, and we will go into more demographic and more information on that, as we go through this webinar.

Slide 10: Product Categories

The pie chart on this slide shows a distribution of respondents in terms of the type of industry or the type of market that they are in. The questions that we ask were all about what -- your specific current project. So whenever someone was answering the question, they were asking about the current project that they were working on. As you can see, going from about 12 o'clock around to the right on the pie chart, Industrial Automation at 19%, and then Consumer Electronics, Medical Devices and Automotive Systems, represent the top four industries. Notice at the bottom there, Internet of Things is at 9%. We allow the individuals to answer IoT as a market space. Even though as all of us know, IoT kind of spans all of these market spaces in one way or another. It was interesting that 9% of the respondents self-identified as being as part of the IoT space, as opposed to a more traditional space such as Medical Devices or Automotive Systems.

Slide 11: Qualified Respondent Experience

Continuing on with the general demographic information in our survey; overall, years paid experience, the average was a little under 17 years. This is slightly up from last year's survey. And you can see, that the bulk of the respondents, or at least a plurality of them, were in the earlier part of their career, of about one to nine years of experience, going up all the way to about 17% at 30 plus years.

Breaking it down by region, those of us in the U.S. are older. Those of us in Asia, are younger, as you can see on the right, with Europe being in the middle, in terms of average years of experience by region.

Slide 12: Team Sizes and Respondent Roles

So, on this slide, we will wrap up our demographic analysis of the general industry. On the left, you see the bar chart showing the size of the software team. The question as noted at the bottom is, at the peak of effort on the project, how many people were really involved in writing embedded software, for the current project that you are involved in. And you can see that the teams are small. The obvious peak there is on two to four people. So your software teams in the embedded space are still very small.

We also asked, as you can see on the bar chart on the right, what was your primary role in design? And software predominates, we all know that in this industry, software is taking on a more major role, relative to the other parts of the embedded system. But still, quite a few people, about 25% self-identify as having both a hardware and a software role in this industry, in terms of their team sizes and what they are focusing on.

Slide 13: Industry Snapshot

Okay, we are now on slide 13, and we are going to start into the general industry snapshot. This is not specifically about safety or security, but just general overall trends and information about the industry, the Embedded Systems industry in general.

Slide 14: Number of Processors

First, let's look at the number of processors; this includes microchip controllers and cores. Interesting result here, is of the overall group of 1,726, only about a third of the designs have just one processor. So designs are getting more complex, more challenging more sophisticated. 43% have two or three processors and a full 23%, almost a quarter have four or more processors. If you look at this in general, approximately two-thirds of the systems being designed today are multi-processor systems. That's an interesting result that shows the sophistication and complexity of Embedded Systems and embedded devices in general, is going up.

Slide 15: "Primary" Operating System

Next, we ask the overall group about the primary operating system for the main processor within their embedded device design. Many still use no operating system, and many obviously still use an RTOS. Linux is very popular still, and if you look at non-RTOS or Linux, you end up with about two-thirds of the numbers here. There is use of open source. Still a fair number use proprietary. Industry APIs or Windows or others are relatively low in terms of the percent of use. So we still have a large number of people, using no RTOS at all, or no operating system at all. The number using RTOS and quite a few using Linux as well.

Slide: 16: Internet Connectivity

The pie chart on this slide deals with internet connectivity over the whole group. Interestingly enough, 60% of current projects will be online. As you can see in the pie chart, we split it up between those that said it could be online all the time, as well as some -- just sometimes online. But only 40% said their device would never be online. These are important results that we are going to dive into more deeply, as we look at the security results. We all know that security issues abound on the internet and we need to be mindful of the fact that 60% of the designs that we are all working on, are going to be online, at least at some point, during their useful life.

Slide 17: Types of External Interfaces

Related to the question of the internet, we also wanted to understand the physical interfaces, the external interfaces by which these devices would connect either internally or to the outside world. And respondents here, everybody could respond with more than one, because many devices have both wired and wireless interfaces. As you can see, wired interfaces predominate, but at least half, if not more, a little bit more than half have a wireless interface as well, and bus and backplane and line-of-sight interfaces are lower. So wired and wireless interfaces are predominantly what's used in the industry today.

Slide 18: “Primary” Programming Language

The bar graphs here on this slide are about programming languages. C for years, has been the predominant programming language in our industry. No surprise here, that C at over 70% is still the primary programming language for embedded software development projects. C++ is healthy at a little over 20% and a chart on the right shows the breakdown of the other, which is in total, well less than 10%. You can see that C Sharp, Java and Assembly are still getting some play in the industry, Ada and LabView a little bit less.

Slide 19: Software Development Practices

Okay, just a few more slides on the overall demographics in our industry, and specifically related to software. Of the full group of 1,726 respondents, we asked whether they used version control, whether they do test-driven development and whether defect-tracking is implemented. Version control, very healthy, 91%. Obviously we'd like to see as much as possible here to better manage as larger teams get involved in designer projects. 36% are using some form of test-driven development these days, and 80% are tracking their defects in some formal or informal manner.

Slide 20: Software Development Practices

Here is some more info on software development practices within the Embedded Systems space. Coding standards are used by about two-thirds of the respondents. Code reviews by about two-thirds as well. Those that entered no here, was really a question of no or just maybe, they only did partial code reviews, not complete code reviews; but about two thirds do complete code reviews. And about half of the industry is doing static analysis today, overall, within the industry.

Slide 21: Coding Standards

And finally, on overall results, that pie chart from the previous slide, showed that about two-thirds of the developers were using coding standards; and so we wanted to dive into that a little. Within that, two thirds of those respondents were using a written standard and we were curious, which standard they were using. About half are using their own proprietary standard. That may have been derived from another standard.

MISRA continues to remain very popular, at about 30%. As many of you know, Barr Group has an embedded software coding standard, specifically targeted at reliability and bug prevention. But then, there is a number of other standards out there, such as a Linux Kernel standard, the CERT standard, and others that have some use in the industry as well.

Slide 22: Safety Findings

All right. Now we are going to get into the safety findings from our survey, which is obviously of great interest to us in Barr Group. The question we ask, and we are on slide 22 right now; of the 1,726 overall respondents, we asked them, what's the worst thing that could happen, if the device that you are designing were to malfunction. They can only answer with one. As you can see, from this slide and this bar chart, that the worse that could happen for certain types of devices was relatively benign, that a customer might get frustrated or annoyed, they might return a product. But what we are really interested in, is those top four bars, which deals with minor or serious injury or single or multiple death.

The point here being, the people -- the engineers that responded in one of those top four categories in the list, those are the engineers that are designing safety critical devices. Those are the devices that could kill or injure, if something went wrong, and that's a pretty big group within our survey, 28% or 475 people total are working on devices that are safety critical. And in the following slides, we are going to dive into some of those results. What are these people? What are these engineers doing, the 475, that are designing devices that are safety critical?

Slide 23: Where are the Dangerous Designs?

First, let's look at where the safety critical designs are occurring, in this subset of 475. No real surprises here; industries like medical, industrial, automotive, those are industries where the devices that are under development are often safety critical and so those are the top industries in terms of designers of safety critical devices.

One of our initial findings on the right in the pie chart, is troubling. As you know, in these industries, such as medical and automotive, there are relevant safety standards in these industries that are used or are supposed to be used by the developers of these devices.

While two thirds of those designing safety critical systems are following those safety standards, one third are either not following it or are not even sure if they are following it.

Now in a subset, where devices can kill or injure, you want to see a 100% following of relevant safety standards within the industry. So right off here, we have some concerns that not enough of the engineers and the teams within the industry, that are designing safety critical systems, are following the safety standards that are relevant for their specific industry.

Slide 24: Safety Finding #1: Insufficient Process

Here on this slide, we are looking at process. And as we see, there really is insufficient process, as it relates to safety critical devices. When it comes to software, safety is going to depend on the software being high quality, reliable. The risk of injury is significant in safety critical devices. So best practices really need to be followed, and there are a number of best practices in our industry, that apply to embedded software development; coding standards, the use of code reviews, the use of static analysis tools. Studies have shown over the years, that the use of these practices, universally, will increase the reliability, reduce defects, reduce bugs, and a system with higher reliability is generally going to be a safer system. So one would expect that these well known best practices, that are easily accomplished with a lot of experience, there is lot of tools out there. They really should be followed universally, within this group, developing safety critical devices.

We look on the pie chart on the left, in coding standards, a full one third are either not using coding standards at all, or they are not enforcing the use of their coding standards. About 40% are either doing no code reviews or only partial code reviews, and about a third are not doing static analysis. Remember, this is specifically within the subset that are doing safety critical devices, devices that could kill or injure. We need these practices to be universal within our industry, especially as it relates to safety critical devices, and the fact that they are not, is troubling.

Slide 25: Non-Use of Static Analysis vs. Risk

What you are seeing on this slide, is a deeper dive into the subset, approximately one-third that are not using static analysis tools in safety critical devices, and it's comparing the non-use of static analysis, that one third that aren't versus the risk in the device. Going from left to right, you will see that minor or serious injuries, all the way down to one or multiple deaths, the trend is generally downward. That means that more engineers are using static analysis as the seriousness of the injury that can occur in their safety critical device, increases. But it doesn't go to zero. It levels off at around 25%. That means that about 25% of those are in multiple deaths. 25% of the people developing devices that could kill multiple people, are not using static analysis. That's a rather alarming finding in this survey.

Slide 26: Test Plans

Now on this slide, we are looking at testing. Again, for the subset, the 475 of the engineers that are designing safety critical systems; obviously, testing and verification, very important for devices and software in those safety critical devices. The respondents could answer with more than one type of testing, and we certainly hope they will do multiple different types of testing. And probably, the most surprising thing here is under regression testing. Again, in safety critical devices, only 59% are doing regression testing. Remember, regression testing is very important for safety critical systems. It ensures that quality only ratchets up, because the regression test will scan for misbehaviors, including those previously found and eliminated. So as you are adding new code, new functionality, or just fixing things, you want to do regression testing to make sure that old bugs don't creep back in, and these tests will become more and more difficult to pass, as you are doing more and more testing in regression testing.

And the fact that a good 40% or two out of every five engineers, two out of every five designs are not doing regression testing, as it relates to their safety critical systems. That's something that we need to really understand as an industry and try to do better.

Slide 27: Risk Should Dictate Process

And finally just wrapping up on this first finding of insufficient process, this slide just gives a summary of where we think things are. There is an old saying that safety -- justice needs to be seen to be present, and I think that applies to safety as well. We'd like to see more focus on safety, it's obviousness, its presence in design. This should be written safety case analysis. And obviously, what we also talked about, the risk. Some devices are minor risk or minor injury, all the way up to single or multiple deaths. The greater the risk, the greater they need it. You got to understand your worst case risk and design to SIL to a safety integrity level in process. That is -- it makes sense for the risk in your project, for the risk of the user of your device. Just as an example there, MISRA requires code review at SIL2 or higher and automated static analysis, at 3 or higher. We saw in our findings, that these types of things like code review and static analysis, they are not being followed enough.

And finally, the message we really want to get across is, don't bolt safety on after the fact. Think about it early, think about it often. In your architecture, in your initial analysis, in your initial discussions with management, understand the safety in your device, make sure you are doing the proper process for that. We need to preach that as an industry, and we need to do better as an industry, in making sure that the devices that we are developing for tomorrow, especially with the explosion of IoT is -- are safer, and that that safety is conserved from the very beginning and all throughout the design process.

Slide 28: Safety Finding #2: Missing Standards

Now our second finding in safety critical devices, relates to the safety standards within industries, as we all know, industries such as automotive and medical -- there are regulatory bodies. There are agencies such as the FDA or NHTSA within the medical and automotive industries respectively, and there are specific safety standards, international standards, that can be followed.

So looking at this chart on top of the slide, Medical Devices will risk death, as will automotive devices. But automotive devices are much more likely to risk multiple deaths, in terms of the number of passengers in a vehicle or the bystanders that may be around the vehicle, when an accident occurs. So it's very important in both of these cases, but certainly in automotive as well that, the relevant safety standards within industries are followed. Nonetheless, as shown at the bottom, the medical community is generally more likely to follow a safety standard than the automotive community, and one has to wonder, why that is?

Slide 29: The Safety Landscape

Just to follow-up on this concept of safety standards in automotive and medical, and in general in terms of devices that could kill or injure. You know, there are obviously voluntary standards within these industries, ISO and IEC standards, very familiar, 26262 as well as other standards. But then there is also regulatory bodies here in the United States of America, we have the Food and Drug Administration which sets a number of rules and policies and procedures for different classes of Medical Devices, and how they can come to market and what they have to document and demonstrate in terms of safety and reliability, before those products can come to market.

There is also DO-178 very familiar to the aviation industry, the aerospace industry, and the Federal Aviation Administration here in the United States. In the automotive side, there is some oversight, but perhaps a lack of oversight, and that makes automotive perhaps a little more voluntary. The automotive industry takes safety seriously, but from an oversight perspective, I think there needs to be a look at the oversight within that industry relative to other industries, and how we can improve on quality and reliability, in terms of that oversight, of voluntary versus mandatory.

Slide 30: Where We're Headed

And finally, as it relates to safety, where are we going? I mean, I think we all understand that software, embedded software is playing a much greater role in the operation of today's and tomorrow's safety critical devices, and within, for example, automotive, software is really controlling a lot of the safety critical systems, if not all of the safety critical systems. So today's cars that are driven by human beings, still have a lot that is left to the software. And tomorrow's cars, so called autonomous vehicles are going to have software and systems and sensors taking the place of the driver, partially if not totally, in terms of autonomous vehicles and autonomous driving.

That's an exciting time, and certainly one can argue, as to the safety of human drivers who are capable of human error versus systems and software, which also may have errors, but may have lower incidents of errors and that's argument beyond the scope of this webinar; but I think the point here is, that as we get into this automated future, both in automotive and in other industries, we are going to be placing the emphasis more and more on software, embedded software. And as an industry, we need to make sure that that software is as safe and reliable as possible.

Slide 31: Security Findings

All right, now let's get to security. We are on slide 31, and we are going to dive into some of the security findings, as it relates to Embedded Systems in our survey. And for a starting point, we asked the entire group, 1,726, a very simple question; is security a requirement in the design of your project in any way? And the result was, 60% said yes and 40% said no. Now, given the experience at Barr Group that we have with security and designing secure systems and seeing some of the things in these systems, and also things that could go wrong, I'm surprised that that number is as well as it is.

I generally believe that most, if not all, embedded devices have to at least have some analysis and requirement for security. That requirement may be low, based on the type of system, and certainly there are Embedded Systems that may not connect to the internet, that may not be used in an open forum, that may be in a very controlled, tightly manipulated environment, where security is minimal, in terms of its requirement and not needed nearly as much. But as an industry, I think, as it relates to safety as well, from a security perspective, we are living in a world in which with more and more devices, we need to generally be thinking about security in just about any project that we undertake in the embedded space.

Slide 32: "Primary Security Concerns"

So from the previous slide where we asked about security being a concern or a requirement, about a thousand of the respondents, just over a thousand, said it was in one way or another. And we wanted to understand, well what were those requirements, what are those concerns? What concerns you as a developer, if you are designing a system that has security as a requirement. And so we asked that question, and you see the results here on this bar graph. The respondents could choose more than one, and you can see that there are your traditional concerns such as theft of service or denial of service, injury or death, theft of IP, product tampering, as well as a number of others. And as we said, you could choose more than one, because many devices do have multiple security concerns.

What's interesting in this slide, and I just think this speaks to the management view of security, in terms of trying to protect the company, is that the blue bars generally represent concerns that are important to the company developing the device. The orange bars represent concerns that are important to those of us out there, that are using, the users of the device. And as you can see, the blue bars generally are of greater concerns to the company's developing devices than the orange bars. So we are certainly excited to see these companies concerned about many things, as it relates to security. I think it probably would be ideal or better, if the concerns of the user, especially as it relates to costs, and more significantly, injury or death, if those were a little higher on the risk as an industry, as we move forward.

Slide 33: The Internet of Dangerous Things

Now moving over to this slide; the results here are very interesting and frankly very concerning, perhaps one of the most concerning results of the survey, and it's something we need to look closely at. So what you see on the left here, is -- the first pie chart shows the question that we ask generally of all of the respondents, is your device attached to the internet, either sometimes or all the time. And 60% of the designs have some connection to the internet.

Within that group of 60%, we asked, are you designing systems that we would call safety critical? Remember, from earlier in the webinar, those are systems that could kill or injure one or more people. And on the right, you see that there are 226 people that are designing devices, that could be killing or injuring and are on the internet, we call this the internet of dangerous things. And this slide shows us, that there are 226 of our designers that are doing that. And we want to try and understand as we go on to the next slide, what are these designers doing within the industry?

Slide 34: Security Finding #1: Low Hanging Fruit

Now let's go deeper on this so called internet of dangerous things, remembering that this is the subset, 226 engineers, designing systems that are on the internet and are safety critical. That is, systems that could kill or injure if they malfunction. We know, as an industry, that security depends at least in part, on reliability and a system that is safer and has fewer bugs or defects, is generally not only just safer and more reliable, but is also more secure. Many hackers use vulnerabilities and reliability and bugs to penetrate a system and a system that cannot be secured, is in general, not safe.

So again, within this subset, those that are on the internet, where hacking and other security concerns abound, and/or design devices that are safety critical; a full 37% are not following coding standards in some way, over 40% are not doing meaningful or detailed code reviews, and 36% are not doing static analysis. As we discussed earlier, coding standards, code review, static analysis, these are process steps that have been demonstrated to improve the reliability, the quality, the safety of systems. And the fact that those that are designing devices that are on the internet, where security risks abound, and that those devices are safety critical and are not following these well known attainable and well documented process steps. This is something that is frankly a concern and something that as an industry we need to -- we need to look at, a little more closely. We need to address this within our industry.

Slide 35: Death by Internet: An Overview

So here on this slide, the so called death by internet, the subset that have designs that are safety critical and are also on the internet, we are just providing a little bit more color for you. So you can see the breakdown; on the left, you see a pie chart that shows that industries, represented by these 226 engineers; medical, automotive, industrial, consumer, these are industries that are -- obviously, there is a number of safety critical devices in them. You see on the upper right, a little bit more on how often these devices are online, and then lower right, the type of safety criticality, in terms of whether there are injury or death or multiple death.

Slide 36: Security Finding #2: Engineers in Denial

Our second finding here in security is about denial or not even recognizing the issue of security. This is something that really surprised me, in terms of the result here. So we are again talking about the so called internet of dangerous things. Those devices that are on the internet, and that could kill or injure safety critical devices. We are looking at our 226 engineers, who responded in this way. And you may remember from a prior slide, that one of the questions we asked was, is security a concern in your product? Now, it frankly doesn't make sense to me, and it's very interesting and something that as an industry, we need to kind of look at a little more closely. 22%, about one in five -- over one in five, of those designing the device that's on the internet, where security is a major issue, and designing the device that has safety critical features, or is required to be reliable and is safety critical a full 22%, don't even have security as a requirement. I mean, I find that very concerning. In general, if you are designing the devices on the internet, forget whether it's safety critical, you should at least be considering security; but these engineers really need to focus on security, they are not thinking about it, they are in denial and these are for devices that can kill. As an injury to have, one in five, internet-based safety critical devices, not even considering security as a design requirement in any way. There is no other way to sugarcoat that, than to just discuss that as something that needs to be addressed and looked at more closely in the future.

Slide 37: Security Finding #3: No Easy Solutions

And finally, as it relates to security in terms of our findings, let's recognize that, as engineers in this industry, we have got challenges, it's tough. And I am not sitting here in judgment. We want to understand and we do understand that the role of engineers is a very positive one, and when it relates to security, there really are not easy solutions.

And this slide really reflects that. This slide is over the full 1,726 respondents. And let's face it, our industry is evolving, and our devices that we are designing today, and those devices that will be on the market tomorrow, they are very sophisticated. They are very complex, and they are only getting more so. And the amount of software in these devices is getting larger and larger as a percentage of the control of these devices.

And really on the slide, as you can see on the left, we talked about this earlier in the presentation. The systems are multi-processor now. There is multiple software code bases that are executing on different processors within these systems of simple up to very complex complexity. And a full two-thirds of the designs are more than one processor in the system. And looking over at the right, you can see that there is a lot of different types of operating systems that are used; and if you look at the bottom, you will see that there is a number of different interfaces. The point is, when it comes to security, you are only secure as your weakest link; and in these systems that are highly sophisticated and very complicated, the opportunity for weak links grows. And on the one hand, that makes our job tougher, and we all know that. On the other hand, it means we need to be more vigilant as an industry, and we really need to look closely at security, remembering that security and safety are related. There are things that you can do to make a device safer, by reducing its bugs, reducing its defects, increasing its reliability, which also have an impact on security; but then there are additional things in security such as cryptography, authentication, that are also important as it relates to security.

Slide 38: Winners of the Prize

Okay, let's wrap this up. I want to express my thanks to everybody who participated in the survey. This survey is about taking a critical look at ourselves as engineers and trying to learn. And as an engineer myself and what I love about engineers is how generally honest and brutally honest we are about our industry and the things that we can do to make it better. And so while this survey on safety and security has some alarming results, the point here is to try and make things better and try and help us as engineers have ammunition to go to our management, at the corporate level, at the technical level, and say, you know, there are things that we can do, to do better. And I hope, that if nothing else comes out of the results here, that we do that -- that as a group, as an industry, we look at these results and we utilize them to make the case, to do better; because no matter how good a job we are doing in terms of safety, reliability, and security, there is always incremental improvements.

And so with that, with those thanks, I want to just point out the prize winners that are noted here from various places around the world. Obviously, it's just a small subset, and it doesn't reflect the appreciation we have for everybody who completed the survey. So once again, thanks on that, and we are now going to move forward to the Q&A.

Slide 39: Question & Answer

All right. Let's head into the Q&A now, and I see that there are a number of questions that are popping up. I am going to try and answer the ones that are most commonly asked and obviously, we only have a few minutes left. So I won't necessarily be able to answer every question. But if you have a question, and it doesn't get answered, or you'd rather ask it privately; send us an email. You can fill out contact information on our web site. So we'd love to hear from you.

So just looking at some of these questions, let me start with -- so, one of the questions was about, getting a number of questions about -- what about this subgroup within automotive that does this or this subgroup within medical that does that? As you can well imagine, in a survey with over 1,700 qualified responses, there is a whole lot of data, and we have certainly analyzed a lot of it. But there are different ways that data could be sliced and diced, and we certainly don't claim to have analyzed every distinct possible combination of demographics in users relative to safety and security. There are many more results. We are putting together a white paper, that has even more results, and be on the lookout for that. If you have a specific question about results, let us know, and if we can answer it, we will do our best to answer it.

I was at Embedded World last week in Germany, and I met with a lot of editors within the industry, who were asking a lot of really good questions, as they prepare articles about our industry on safety and security; and we will certainly be trying to help them and anybody else who has a specific question on a specific subset within the survey.

Let me see, another question, I get this question all the time, it's a very popular question;

Q: What about comparison on prior years? Are we seeing improvement or are we seeing things get worse?

A: It still a little early. It is only the third time we have done this survey, so it's spanning the 24 month period. And so it's hard to analyze specific trends year-over-year yet, and partially that's because we are not seeing significant differences year-over-year yet. So we are seeing, on the one hand that's positive, that we are seeing consistency, that tells us that they feel even more comfortable that we have got some interesting data. But we are also not necessarily seeing a change in the trend yet, in terms of an improvement in process for safety-critical design. As we get more and more years under our belt, we will obviously be doing this survey again next year and in years to come, we will be presenting more data on safety and security, as it relates to prior years.

Same thing about geographic distributions, and that's a question we get often as well.
Q: Are European engineers more likely to be more conscious of safety than

American engineers? Are older engineers more likely to be cognizant or less cognizant than young engineers?

A: We are not seeing, at least yet, significant differences stratified across age groups or experience groups rather, and also geos; but as we do more years, and get more years under our belt in this survey, we will certainly be providing more data on that.

Let me answer this other question really quickly, here is just a general question, what about the availability of this webinar? So yes we will -- we are recording this. We will be doing a transcript and the slides and the recording of this webinar will be available on the Barr Group website, www.barrgroup.com. Give us a few days to get this transcribed, get this recording set up, and it will be available online.

I have got time for a couple more questions; so one question I am getting is:

Q: For those that responded that they weren't using processed steps like coding standards or code reviews, how can we be sure, that those aren't being used in the project, just not being used by an engineer, say who's designing hardware or designing something specific? A: So we were very careful in how we ask those questions. We ask them in a way, that would not limit it to that person. We ask it in your project overall, are you aware? Is it going on? And you notice we had -- that most of our design teams were very small. So we weren't asking, if you specifically were doing it, we asked if it was being done within your project. And generally, the small design teams, we expect that people would know, whether they were or were not being used. So that's the answer to that question of whether someone would know.

Okay, let me look. I am just looking at these questions. So one more question; I guess, probably a big question here is why?

Q: To the extent that engineers are not following safety or security standards. Why are they not?

A: And that's a question that's probably, in some respects, beyond the scope of this webinar; but certainly, we have to look as an industry at budgets and schedules and the relative importance of process, as it relates to safety and security in general. Engineers, and even their managers, for the most part, are good people. They are trying to do the right thing; but in this age of IoT and increasing technology, we are all under incredible development pressures to get the product out; to get the product out on schedule, to get the product out under budget, and we all know that these process steps have a short-term impact for a long term gain. So, doing static analysis, implementing coding standards, doing code reviews, these are all aspects of design that will extend development during the development phase of the project. And upper level management needs to understand, that the impact of these increases is generally a positive in the long term.

Sometimes it's hard to prove that early on, and there is certainly an element of, well this won't happen to me, I won't get caught or my company won't have the security breach or the security problem. And that type of mentality does exist in some companies and in some management, is an issue. And as an industry, I am hoping that the survey helps to highlight some of the issues there. But as to the why in general, I think, as an industry, we all have to think about that. Why aren't we doing this? What can we do more? How can we show that these steps to improve safety, security, reliability, are going to pay dividends in the long term. And I think as an industry, we can do that. We are dealing with a group of people and engineers who really care about the quality of the systems they are designing, and hopefully this survey, if it does nothing else, bring some awareness of some of the challenges of that.

Slide 40: Thank You for Joining Us!

And so with that, we are just about out of time, so I am going to end the Q&A session here. And finally, I want to thank everyone for joining us. I want to thank everyone who participated in the survey. It was a really large number of you, and that's great. We always like to see that, because that gives us better results. And I want to thank everybody for listening in today. Remember, the webinar here is a summary of the key findings. There is going to be a written report available, it is a free PDF. Stay tuned to our web site for that. If you register for this webinar, you will be getting an email, reminder, when the report and this transcription and recording of this webinar available. And as I said, give us a few days on that. But keep an eye out for even more details on this survey.

As I mentioned, contact us if you have a very specific security request. Certainly, the raw data is available under license, but if you have a very specific question, whether you are an editor or a manager or whatever it might be, or anybody who is interested, let us know. We will do our best to try and get you the information you need. It's part of the outreach that we try to do within this industry.

Last, I just want to mention again, that we do have a training that we do. A number of public courses that deal with safety and security. So take a look at the URL for the training calendar below, we have got some courses coming up on security and safety in the United States, and also in Germany. I met a lot of people last week at Embedded World in Nuremberg, that are interested in safety and security and so we hope to see you in Munich, in May and June; and then we of course have our traditional boot camps; software boot camp, android and security. They are coming up as well. So take a look at our training calendar. If you have any questions on that or you have an interest in doing any of our trainings on-site at your facility, we do training all over the world, and we love to engage with engineers, and working on our industry and improving as an industry in general.

Again, thank you for joining us, and I hope everybody has a great day and takes time to look at more of these webinar results and to improve in the safety and security. Good day everyone.

Stacy: This concludes our presentation. Thank you for attending and for all of your great questions. We hope you found this webinar informative, and hope to see you at future presentations. If you haven't already, be sure to sign up for Michael Barr's firmware update newsletter, at www.barrgroup.com. The contents of today's webinar will also be available on demand on the Barr Group website in the next five business days.

Thank you, and we will see you next time.

More Questions and Answers

Q: What is the good method to learn about making safe and secure products?
A: Barr Group also offers training courses for embedded systems engineers. See our complete training calendar at http://barrgroup.com/training-calendar

Q: Can't remember the questions in detail, but did any answer Matlab/simulink or similar as language? (If no, was it possible to give that answer?)
A: It was possible to answer “Other” and a couple of people answered “Matlab” and/or “Simulink”, specifically. Those rounded to 0%.

Q: What is the better code language to write code for safety critical system?

A: Ada’s a great language for that purpose, far superior to C/C++/Java. But good luck finding an Ada compiler and team of knowledgeable programmers these days.

Q: What about those developing SDKs/BSP, drivers, etc that may go into safety critical systems. I'm one of those and I never know how to respond to these surveys.
A: As consultants, we understand completely. This is why we go through a process of weeding out survey respondents that don’t appear to know enough about their specific “current project” before analyzing the answers to the safety and security questions.

Q: Software is invisible, so management will never see the mess.. At least not until it blow up…
A: Sadly, it sometimes does work that way. Hopefully not at your company.