LS106

Contemporary Controls Interviews Eric Byres

Contemporary Controls Interviews Industrial Network Luminary Eric Byres

Eric Byres is a Professional Engineer and research manager of the Internet Engineering Lab at the British Columbia Institute of Technology (BCIT), one of North America's leading research facilities in the field of industrial cyber-security. For the past 14 years, he has specialized in data communications and controls systems in industrial environments, focusing on both Industrial Ethernet research and network security design. (Photograph by Scott McAlpine, BCIT)

Perry Marshall caught up with Eric to discuss the present and future state of Ethernet and industrial networks. Join us to hear Eric's views on Internet security, organized crime, hackers, powered Ethernet and Ethernet-enabled sensors.

Perry: How did you figure out that you were a technology man, and what were some things that got your blood pumping?

Eric: I remember one of my highlights in life. One of them was my parents giving me a little plastic digital computer. It was completely made out of plastic, and if I could ever find it again I would mount it on my desk. It was three bits long, which was the most it could calculate. It did all of its calculations mechanically.

You could program it to do very simple things with only three bits, but it was fun!

Perry: Like addition, or multiplication?

Eric: Yes! You could get it to add two plus five, and that was about it. It could multiply two by three. You could actually get it to do fairly complicated logic with only three bits, but it was quite the little plastic computer. The clock was your hand running this thing in a circle.

Perry: And now you're in communications, which is an interesting animal, because, unless you know it inside and out, it is like black magic.

Eric: Yes, it is. You do not see anything. There are no tanks to measure. Once you know it, it makes an awful lot of sense. I often describe data communications without all the right tools, is like trying to fix a car with the hood still closed and just trying to listen to the engine.

You need the tools, and you need to know how the internals work before you have a chance. Otherwise, to everybody else, it looks like black art.

Perry: Where do you see friction between the Industrial world and the I.T. world?

Eric: In the I.T. world, you can ship software and if it fails a little bit, that is okay. Your number one thing is performance, not reliability. That is what the market accepts and expects. We have an entirely different culture on the plant floor, where it is very conservative and designed to be robust.

If the patches do not work, then the I.T. department gets phone calls, and they come out and fix them. We cannot do that on the plant floor. You cannot just push patches down to all the operator stations. We need to figure out a way to be able to handle, to really test and certify and be sure of all those patches in a very short time frame.

But there are some areas in the I.T. world that actually do work differently. The Telco's, for example. They are also an environment that we can learn an awful lot from. They are also used to five-nines up time, and, "Whatever you do, do not crash that telephone switch!"

Perry: What are some things that those guys are doing that people in the industrial world really should know about?

Eric: Some of them are very similar to what we do. For instance, they actually deploy exceedingly tight change management. We do that on the plant floor, but then people will change the firewall rules.

They will go and change their workstation, or they will go and change the configuration. So, the traditional I.T. world does not have change management like we do on the plant floor. Not like the banking industry or Telco's have change management. We could learn from them how to stick to our guns.

Perry: Let's say you're "Larry Lunchbox" working on the plant floor, and you are outnumbered by all these I.T. guys. They think they are smarter than you are, and you probably do not have as much political clout as all the others. What is a typical scenario where we can reasonably slow the train down and not get run over?

Eric: I just came from a large company where they were ranting about their I.T. department.. I think we blame the I.T. department, when those guys are really just caught up in it like we are.

They are caught in a culture that they are not any happier with than we are. What we need to do is work with the I.T. department, and really educate them on how we do things, to help them to understand our world. I think they would say, 'Hey, that is a good idea. We should be doing this.' The guys in the I.T. department are no happier about this patching mess than we are.

Perry: What can they learn from us?

Eric: Things like change management and documentation management. Project planning, as well. In the electrical engineering world, we tend to have strong project planning techniques.

Sometimes these organizations have very strong project planning processes. One said that they spend 40% of their project before it gets approval in the planning stage.

They said it saves them money, even though the project may not be approved. That is not typically seen in the I.T. world.

Perry: In the I.T. world, if an office goes down or a server goes down, you go get a cup of coffee and you check your e-mail later. If the plant floor network goes down, you choke down on your last swallow of coffee and dash to fix it, while all the widgets are piling up on some machine somewhere, right?

Eric: I would not say that they finish their coffee. I mean, I have watched these guys in the I.T. department, say, here at BCIT. They are not any happier when a server goes down than we are, and they got all of these guys yelling at them. Especially if the Vice President happens to be connected to that server. So, the pressures are still there, but the methodologies are not.

If there is anything in this article, that I want to stress, it is to not blame the poor guy on the I.T. floor. If there is something to be blamed, it is just the whole culture that created it.

> *"If there is anything, in this article that I want to stress, it is not to blame the poor guy on the I.T. floor. If there is something to be blamed, it is just the whole culture that created it."*

As for us, we install a DCS or PLC system, and we expect it to have a 15-year lifetime. I put it in, run it, and it should last at least 15 years. I know that I installed Factory Link nodes back in 1988, and they are still running, and they are running on DOS. One of the things that we have to struggle with now is the rate of change that we have induced into our plants, because of the I.T. world. It does not match our rate of change.

So what do you do? That is the question. We do not want to be upgrading our operating systems every year, and yet that is what happens out there. One of the big challenges right now is that we need to create industrial operating systems. Maybe instead of Windows XP, it will be Windows Industrial. It changes less often, and it has a lot of stuff stripped out out. Ditto for Linux and ditto for anything else.

Perry: Is there a realistic possibility of having that with Windows or Linux?

Eric: It is definitely possible to do it in the Linux world, and I think that Microsoft® actually is interested in that as well. There was a meeting in Seattle back in July. There was definitely a round of discussion about creating a hardened, more stripped down version of a Windows product.

Perry: The fieldbus wars shifted into Ethernet, so everything is on TCP/IP. There are a lot of products now. There is HSE, there is Profinet, there is all the Modbus stuff, and there is Ethernet/IP; how good do you feel all of these efforts are to date? How good is the equipment that you can buy?

Eric: Bad news first: The down side is that we have created the fieldbus wars on top of Ethernet.

The good news is, that at least we can agree on what our cable is going to look like, what our data link layers are going to look like, what our switches are going to look like.

This way, Larry Lunchbox can go in and cable up this plant, and get it all in place. He can decide if he wants to go with Rockwell or Siemens or Schneider, or all three of them, and not have to pull special cables or bring in special equipment. The wiring plant can stay in tact, and that is 60% to 70% of your networking cost in any project.

There is still a long way to go, particularly in some of the products. I mean, my area of focus now is entirely on security. If I have another rant, it is that we have not started to take security seriously in this industry at all.

Perry: At all?

Eric: At all. I hear people saying, 'Why would a hacker want to attack my plant?' There are a lot of reasons.

Perry: You mean it's like they're saying 'Okay, so I am at the airport. Why would anybody want to steal my suitcase, right?'

Eric: Yes, exactly.

Perry: And your suitcase happens to have thirty million dollars worth of soup in the tank, right?

Eric: That's right. There are a lot of reasons why hackers would want to do it. Some of it is just because they could. Some of it is just because they wanted a place to run their stamp through. It is just because you have a site that they could run their pornography, and then hide behind your site, so that you get blamed.

You may be what we call a, Target of Opportunity; Easy Pickin's. Like the kids walking down the street and finding a door open. The industry, right now, is leaving all the doors open.

Then you get what we call, Targets of Choice. This means that somebody wants to get you, and there are lots of reasons why somebody might want to get a company.

For example, people can do things like cause difficulties with your environmental procedures, with your operations etc. This way they can sell all of your stocks short.

Perry: That is clever.

Eric: In the I.T. world, we started to see companies being attacked. Right now it is mostly questionable organizations. They get hacked into and blackmailed into doing something or paying something, in order to get the hackers out of their site. Some hackers came to a gambling site in Canada and completely encrypted all their servers, so that they could no longer operate their site! They were losing millions of dollars per day. In exchange for paying a sum of money, they got their site back.

"There will be at least somebody who is not happy with you. You leave yourself open to what we call, 'Hacktivism'."

When they get tired of beating up on gambling sites, they will start moving. Extortion is a potential possibility. The other possibility is most companies have somebody with a political agenda who does not like you. If you are a food company, you may have an activist with a vegetarian bent. If you are doing animal testing, you will have PETA after your case.

You can get the idea. There will be at least somebody who is not happy with you. You leave yourself open to what we call, "Hacktivism."

It is no longer just a bunch of disgruntled kids. It is starting to become an active part of organized crime. What I expect to see over the next little while is potential organized crime elements, using that hacking and using those viruses for profit to the detriments of the companies.

Perry: What are the most rudimentary things that somebody should be doing as a minimum to have a reasonable level of security, so that at least the door is not hanging open?

Eric: The very, very first thing that somebody needs to do is figure out what their security policies are. Then, figuring out how much effort you want to make from a corporate policy point of view, and then education.

You must also develop your business case for your security. What are you protecting, what is its risk? What is it going to cost you? What is it worth to protect that?

Perry: It is pretty hard to get any budget money for security until somebody figures out what it is worth, right?

Eric: Come up with a corporate policy that security is important. Then, given that, what it is worth to you? Remember 30 or 40 years ago, people were getting killed left, right and center in plants. Then the companies decided, "Safety is a priority here."

Perry: How do you define safe?

Eric: Right, how do you define safe? Same with this, how do you define security for your company? Then you can start going through standard, acceptable behavior. For example, there is all sorts of stuff around passwords, but a better example is, are people allowed to bring in laptops? Say a contractor comes in, what can he do?

Now you start to get into what I call, Standards, or Procedures. And below that, we start to get into the technology.

Perry: Once a person has gone through these steps, what technologies are going to be appropriate for most people as a first line of defense?

Eric: There are two core technologies that people absolutely have to deploy in their plant that is absolutely core to their operation, in my opinion. First of all, we absolutely need to start putting firewalls in between the business side and the process side.

The job of the firewall is not just to control the hackers, but in particular, the biggest risk that we face right now, is automated viruses. Such as Slammer and Code-Red and Nimda, all of those lovely little devils.

Perry: Are there a lot of guys out there who are checking their e-mail on a process computer, where they should not be doing any such thing?

Eric: The trouble is, with Slammer, Nimda, Code-Red and Blaster, you do not even have to have e-mail running! Those are automated worms that are taking advantage of applications and processes that we run on our machines. A good example is RPC, Remote Procedure Call. That whole component of Microsoft® Windows is absolutely core to OPC.

If you are running OPC, you could be vulnerable to exploits like Blaster that take advantage of remote procedure call. E-mail is a minor player these days.

I really do think that people have to put virus-checking software on their machine, no matter where it is on the plant floor. That is not a trivial task, because you have to work with the vendor. HMI or DCS was not intended originally to have virus software on it. Then you really need someway of pushing virus updates, the information files out to those machines on a regular basis. I just finished looking at a plant, and I found a whole bunch of virus scanners. Some of them had not been updated since 1999.

Perry: Now that we have all this data, what are we going to do with it?

Eric: Someone might say, 'Hey, we have information on the total amount of valve travel that this valve has done over the last six months. How have I tied that into my maintenance database, so that I can predict when my valves are going to fail?' Instead of just holing them out every two years or six months, I know exactly how much travel they have had.

On the paper side, I saw somebody working on the systems, not to detect sheet breaks, but to actually predict them based on the data they were getting. So, they would actually know when a sheet break on a paper machine was going to occur.

Perry: **Talk about the Ethernet switch testing that you do—what is the significance of it, and how good are some switches compared to others, really?**

Eric: I think that is a big issue for people who say, 'We do not have a consumer reports for industrial switches,' or, 'Why am I paying for an industrial switch over something that I can buy down at Radio Shack?'

There is a definitereason why you want to buy the $2000 switch, rather than the $50 switch. Now primarily, performance is not it. What we saw in our test was that performance in switches is generally a mute point.

Perry: **When you say "performance," what do you mean?**

> *"There is a definite reason why you want to buy the $2000 switch, rather than the $50 switch."*

Eric: To get your packet in and out, most switches do it pretty much the same. That is what people get caught up in, 'Is it faster? Is it fast enough? Will my switch slow my network down?' That was not the big issue. A major issue was quality of construction, particularly around power supplies. We managed to blow the stuffing out of at least one switch. It was a standard home-and-office type switch.

I do not want power switches blowing their little brains off on my plant floor. I mean, it exploded. It blew its little head off. The capacitor went "Bang!" and ripped a nice hole in the side of the casing.

Perry: **Wow!**

Eric: That was one of the issues. The quality of construction; is it tough enough? Is it well built enough for the type of environment that we expect it to survive, versus say, my desk in my office? It is very, very different. The power supply, the casing, the quality of the connectors, the quality of the circuit boards; all of those things are hugely different.

The third issue is, the feature set. On the plant floor, the ability to manage those switches; it is not one that sits on your desk, and you can watch one light; these are scattered all over our factory now. You absolutely need a secure way of being able to configure them, and manage them, and baby-sit them. The manageability of the switches, and the feature set of the switches, varies widely.

Perry: **Are you still doing ISA training?**

Eric: Lots of that. (Editor's note: Eric just received the Donald Ekland Award at the Houston ISA show, which is their award for outstanding contributions in training.)

Perry: **So, what does the typical training session consist of?**

Eric: Well, it is a lot of different training sessions. Before, it used to be one training session on networks; that was it. Now, there are training sessions on how to pick the right bus; how to pick the right fieldbuses. There are training sessions on security audit methodology.

There is much lack of understanding, especially in Ethernet, that people are just scrambling to go to these courses. They sell out every time.

Perry: **Do you think Ethernet is realistically going to go to the sensor level?**

Eric: Yes, absolutely. Right now, the economics are not there, but we see it going to the sensor level in our home now. We see people talking about the somewhat questionable internet-enabled toaster. I cannot figure out why I would want my toaster internet-enabled, but I do know why I would want my Palm Pilot internet-enabled.

I do know why I may want my telephone internet-enabled. Those are "edge" devices too. You do not think about it, but they are. Those are pretty small, lightweight devices, with not a lot of intelligence in them; at least, not necessarily a lot of intelligence in them. So, those things become in the commercial and home environment, Ethernet-enabled.

Then the price is going to get considerably driven down, so that Ethernet can afford to show up on our edge devices. I think the reason that it is not at the sensor level right now, is that it is not technology, it is economics. You still cannot justify an Internet chip in a limit switch.

Perry: **Right! Well, they get cheaper. They get down to $10, or something like that. So, it is still a little pricey, but it is moving in the right direction.**

Eric: It is moving in the right direction. I mean, toasters, telephones, etc. cannot afford that kind of hit, either. There is a lot of pressure for them to go there, and I think they will. So, I think absolutely we will see Ethernet everywhere, simply for the reason that it is going to happen in the commercial sector, and we will follow along.

Another aspect is power-to-Ethernet devices. We have howled and complained that you cannot go to the plant floor with Ethernet, because there is no way to power the devices, and we love 2-wire devices. Well, one and a half years ago, maybe two years ago, the IEEE came out with the 802.3AF standard, which basically says, "Here is how you run power over your Ethernet cable."

They did not do it for us, they did it to power those telephones. Now, I know of at least one company that has an Ethernet powered pressure transmitter. So, that product has come out. It is there and people will start to say, 'Hey, I want that.'

Perry: What are you looking at in the near future?

Eric: Over the years, we have learned how to make extremely robust, tough control systems. How often does a PLC just walk off on its own and do weird things to the IO? Almost never. We have really learned how to do a good job of making tough, robust systems. Then we went and took Ethernet and TCP/IP and put it on the side.

We never spent the time and effort to see, "Is this robust? Is this tough? Is this secure?" So my big interest right now is testing. Trying to make systems that will test PLCs and DCSs and anything else, and getting an idea, "Is this a tough box?" If somebody sends you a bad message over the network, will it roll over and play dead or will it just throw it away and keep on trucking?

> *"I think we can offer an awful lot to the I.T. world on how to certify things for security."*

What I am hoping is that in the long run, just like we do in safety, that we have fill levels in safety. Things do not get certified in the I.T. world. Now, how many years did the industrial world battle to be able to come up with a safety certification system? Well now we have it! So, I think we can offer an awful lot to the I.T. world on how to certify things for security. I do not think we need to invent our own, but I think we can help them along.

Perry: So then, if this got adopted all around, it would be like, 'This is a firewall with a security rating of 8.'

Eric: Yes, and I think it applies right down to your PLCs or DCS. This PLC has a security rating of one or two or three or whatever.

Perry: Well, that would certainly be a differentiator in a world where all the vendors are paranoid about being the commodity, right?

Eric: Yes!

Perry: It is something that is very much needed, and there are a lot of people with their screen doors unlocked, so to speak.

Perry: How do People find you?

Eric: Where they find me is at the Internet Engineering Lab at BCIT, the British Columbia Institute of Technology. I am in, what we call, the Critical Infrastructure Security Center.

(Continue on with the interview by reading about one industrial plant hack: Vitek Boden. This case is known as the Maroochy Shire Sewage Spill.)

Industrial Plant Hack: Maroochy Shire Sewage Spill

In November 2001, 49-year-old Vitek Boden was sentenced to two years in prison for using stolen wireless radio, SCADA controller and control software to release up to one million litres of sewage into the river and coastal waters of Maroochydore in Queensland, Australia. Boden, who had been a consultant on the water project, conducted the attacks in early 2000 after he was refused a full-time job with the Maroochy Shire government.

The crown case on the computer hacking offenses was that between February 9, 2000 and April 23, 2000, Boden accessed computers controlling the Maroochy Shire Council's sewerage system, altering electronic data in respect of particular sewerage pumping stations and causing malfunctions in their operations.

The evidence in the case revealed that the Council's sewerage system had about 150 stations pumping sewerage to treatment plants. Each pumping station had installed a Hunter Watertech PDS Compact 500 computer (RTU) capable of receiving instructions from a central control centre, transmitting alarm signals and other data to the central computer and providing messages to stop and start the pumps at the pumping station and the central computer by means of a private two-way radio system.

Boden, an engineer, had been employed by Hunter Watertech as its site supervisor on the SCADA installation project for about two years until resigning December 3, 1999. At about the time of his resignation, he approached the Council seeking employment. He was told to enquire again at a later date. He made another approach to the Council for employment in January 2000 and was told that he would not be employed. The sewerage system then experienced a spate of faults. Pumps were not running when they should have been, alarms were not reporting to the central computer and there was a loss of communication between the central computer and various pumping stations.

On March 16, 2000, when a malfunction occurred in the system, Mr. Yager, a Hunter Watertech investigator of the problems, communicated over the network with a bogus pump station 14, which was sending messages to corrupt the system. He was temporarily successful in altering his program to exclude the bogus messages, but then had his computer shut out of the network for a short period. The intruder was now using PDS identification number 1 to send messages.

Further problems then occurred as a result of a person gaining computer access to the system and altering data so that whatever function should have occurred at the affected pumping stations did not occur or occurred in a different way. The central computer (SCADA master) was unable to exercise proper control and, at great inconvenience and expense, technicians had to be mobilized throughout the system to correct faults at affected pumping stations. On the occasion the subject of count 45, a pumping station overflowed causing raw sewerage to escape.

On April 23, 2000, an intruder, by means of electronic messages, disabled alarms at four pumping stations using the identification of pumping station 4. The intrusions began just after 7:30 p.m. and concluded just after 9:00 p.m.

By this time, the appellant had fallen under suspicion and was under surveillance. A vehicle driven by him was located by police officers and when the vehicle was pulled over and searched, a PDS Compact 500 computer, later identified in evidence as the property of Hunter Watertech, was found in it, as was a laptop computer.

Impact: Along with 27 counts of using a restricted computer to cause detriment or damage, Boden was also convicted of one count of willfully and unlawfully causing serious environmental harm. The sewerage spill was significant, polluting over 500 metres of open drain in a residential area and flowed into a tidal canal. Cleaning up the spill and its effects took days and required the deployment of considerable resources. “Marine life died, the creek water turned black and the stench was unbearable for residents,” said Janelle Bryant, Investigations Manager for the Australian Environmental Protection Agency.