ceocfointerviews.com

Issue: January 26, 2015
The Most Powerful Name in Corporate News

Industrial-Grade Solutions for the Internet of Things

Chris Muench
CEO

CEOCFO: ***Mr. Muench, your site indicates C-Labs provides industrial-grade solutions for the Internet of things. How so?***
Mr. Muench: We looked at the phenomenon of the Internet of Things (IoT) from the perspective of factory automation environments. We found one interesting factor common in many factories: the traditional IoT where you connect devices to the cloud does not work in factory automation. Factory devices are not connected to the public internet so you cannot connect them directly to the cloud as with "consumer grade" IoT solutions. The IoT paradigm as currently proposed by Google and others may work for home thermostats but it does not work for industrial automation. In contrast, we use the "Internet of Things" for what it was originally intended: getting value from devices simply because they are connected to each other. You can have two devices talking to each other collectively creating new business value you cannot get with just a single device. That is our first step. You don't need a public internet connection on the factory floor to do that. We then extend this out to the enterprise and cloud with patent-pending technology that securely delivers this new business value to workers and decision-makers without exposing factory floor equipment to the public internet. That is what "industrial grade" means.

CEOCFO: ***Would you give us a concrete example of how this works so we can get a real feel for what is going on at C-Labs?***
Mr. Muench: You have a factory controller with, for example, a machine, robot, or conveyer belt. You want to have the KPIs—the key performance indicators—of the conveyer belt delivered to your headquarters in a completely different location. Let us say your factory is somewhere in Kansas and your headquarters is somewhere in Denver. How do you get the KPIs in real time? You can't put them on a disk and courier them to your Denver headquarters. You could use a VPN (virtual private network) line and dial directly into the factory, but VPNs are more and more expensive and they are very hard to set up. And VPNs burden corporate IT teams because they require significant resources to set up and then maintain all of the necessary infrastructure. If you want an easier way to do all that and still do it very securely, that is where the IoT comes into play and helps connect the conveyer and all of the factory equipment to the other facility.

CEOCFO: ***Why can't these things all be connected through the Internet?***
Mr. Muench: The main reason is the security problem. A conveyer belt or other factory device is not built with the hardened security required for the public internet. Let's say you have a conveyer belt exposed to the Internet, and a hacker comes in and speeds up the conveyer belt and all your products start to fall to the floor. Or the hacker stops the conveyer belt and your whole production line grinds to a halt. There is no security built into the conveyer belt because it was never meant to connect to the public internet. Factory controllers are very small and optimized for high-speed performance. That is at odds with what corporate IT wants, which is data security, firewalls, and antivirus protection. You will not find those on industrial devices. If you connect industrial machines directly to the public internet, you will be exposing them to a huge number of attacks. The Stuxnet worm and related incidents created the big awakening about security concerns in factory automation, and yet the solutions are still not out in the market. This is where C-Labs comes in. We help connect those devices securely through all these layers that the IT department has established, and we build a secure connection between two or more different environments within the enterprise. We do more than M2M (machine-to-machine), where one machine connects to another machine. We do true IoT, where multiple facilities all over the world connect and can consolidate information wherever you need it. Whether using a mobile device to control the factory floor,

wanting a snapshot of all the factories running worldwide, feeding a business intelligence system to crunch data for predictive maintenance, or facing any of the other scenarios at the forefront of the industry, you need a C-Labs solution that doesn't expose your equipment to the internet.

CEOCFO: ***Do people know that alternatives exist and are they actively looking for better solutions? What is the state of the marketplace?***
Mr. Muench: Customers want secure solutions, but they are not out there. Market demand for connectivity gave birth to M2M. Vendors of M2M said they would solve the connection problem by adding an M2M controller to existing factory equipment, add another M2M controller on the other side, and then have these two controllers talk directly to each other using cellular or other private networks. The problem with all these M2M boxes is that they can completely circumvent and undermine IT policies. If there is an IT policy in place to disallow direct connections to the public Internet except through the corporate firewall, the M2M boxes will just bypass the corporate network. That is happening right now in the industry as corporate IT groups push more and more of their security concerns down to the factory level. Companies are pulling M2M devices out of the factory one by one. The need is there, the demand is there, and people are looking for alternatives. That is exactly where C-Labs comes in. We provide a solution in a way that is easy to deploy yet fully compliant with enterprise IT policies.

"Whether using a mobile device to control the factory floor, wanting a snapshot of all the factories running worldwide, feeding a business intelligence system to crunch data for predictive maintenance, or facing any of the other scenarios at the forefront of the industry, you need a C-Labs solution that doesn't expose your equipment to the internet."- Chris Muench

CEOCFO: ***Who has been paying attention so far?***
Mr. Muench: Very large industrial companies, machine makers, robotics manufacturers, and OEMs in the industrial automation controller segment are engaging directly with us. One of the OEMs is in the top three and the other is in the top ten in the manufacturing space. We have other customers that are working on implementing solutions, including one in the energy segment that is working with us on an interesting solution. There are a couple of automotive companies as well. We are dealing with one big automotive company that wants to modernize a factory in Eastern Europe, and this is a new project starting in January 2015. We are very excited about this project. The interesting thing is most of our customers are currently in Germany. This wave has picked up big time in Germany through the government-sponsored Industry 4.0 initiative, of which the IoT is a fundamental part. So all the German manufacturers, customers, and OEMs are jumping on the IoT bandwagon, often without fully understanding it. This heightened interest has been quite beneficial for C-Labs.

CEOCFO: ***When a company comes to you, what goes into the process of evaluating what you need to set up for them?***
Mr. Muench: The great thing about our technology is that customers can deploy it off-the-shelf. But when customers do want help, the first thing we or our partners do is assess what devices and processes are in place and what goals the customer has in using the IoT. An IoT deployment is not just for the sake of putting IoT equipment into factory, it has to achieve a certain business goal. Is it optimizing a production line, optimizing a process, providing value chain transparency, enabling better communication, or something else? Once goals are set, we can proceed with an assessment of which devices the company should connect to the IoT network and what corporate IT policies will apply. From there, we do a proof of concept, to prove the solution will work. After that comes implementation, where we deploy the solution and transition it to the customer. The whole process can take as little as a few days or up to several months depending on the size and complexity of the customer environment.

CEOCFO: ***When a company decides that they want an assessment from you, are the workers typically on board?***
Mr. Muench: It is always best when workers, both in the factory and in IT, are involved in the process and support it. There are concerns, especially if the potential IoT project affects the performance of factory workers, which is a very delicate subject in many countries. We typically stay away from that and focus on the performance of the machines, not the workers. You can still optimize the performance of a machine by just changing cycle times and knowing what the machine does. Many companies buy a piece of equipment from an OEM, put it in the factory, and turn it on, without ever fully understanding its performance or how to improve it. Reading all these KPIs, mapping them over longer periods and finding patterns that show how to optimize the machine are all important steps in creating an IoT solution. When workers see that and see how their working environment gets more comfortable, efficient and productive, they come on board. I had a very interesting discussion with a company in Europe that came to my booth at a recent trade show. At first, they were very skeptical of our technology and said they did not need anything like it, yet after one and a half hours, they

invited me back to Germany to build a proof of concept in their factory. The biggest problem is often addressing the argument about how our solution is different from what the customer might already have. Most of the time, factory workers and managers do not understand IT policies and unwittingly bypass them. And IT workers aren't aware of the problem, or if they are, they don't know of a permanent solution, so they propose a temporary solution, which often puts systems at risk, and they just hope the hackers ignore them.

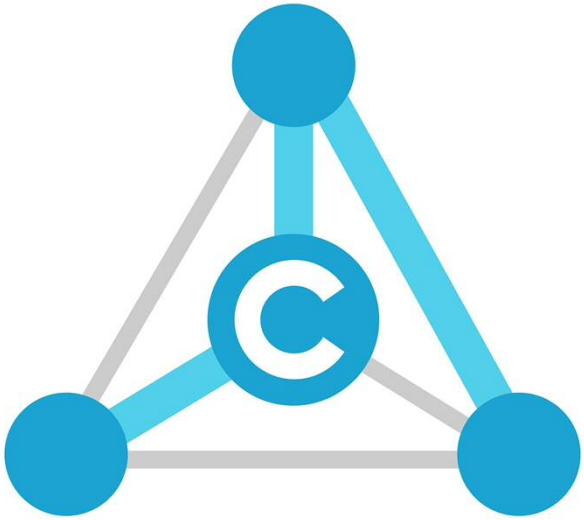
CEOCFO: ***How do you reach out to prospective customers and how do people find you?***
Mr. Muench: First, we benefit from a wide network of contacts. Many of our current advisors and employees are former employees of Siemens or other industrial automation companies. So that helps us get the word out in the industry, and we've already seen a lot of traction with OEMs, distributors, and their customers. Second, we have on-going marketing campaigns through which we present our perspective on customer challenges in industrial automation and the benefits of IoT deployments and how our products help with that. We do this via whitepapers, solution overviews, on-demand demos, as well as traditional trade show and conference events. And I'm spreading the word via my CEO Corner blog and social media channels because there is still a lot of confusion as to what the IoT really is. For example, in the consumer space you can just connect a thermostat to the cloud and be happy with it. The consumer does not really care what happens with the data. But savvy industrial customers know their data is their IP (intellectual property), which can confer competitive intelligence and provide competitive advantage. Those customers do not want to lose control over their IP. The consumer may not care if Google knows the temperature was lowered 2 degrees at 11 o'clock, but a manufacturer knows that when and how quickly a robot moved 10 centimeters to the right is intellectual property worthy of the protection that C-Labs delivers. We get lots of engagement from industrial customers who tell us they didn't know they had a problem until they saw one of our presentations or read a whitepaper or my blog post.

CEOCFO: ***What did you learn during your time at Microsoft that has been helpful in growing and developing C-Labs?***
Mr. Muench: My main experience comes from my 19 years with Siemens, where I was an architect for one of the biggest SCADA (supervisory control and data acquisition) systems in the market – SIMATIC WinCC. This gave me great insight into real-world industrial automation scenarios. At Microsoft, I came to appreciate the process of truly large-scale software development, and gained an understanding of how customer IT organizations approach new technology. Siemens really understood industrial hardware and engineering, and Microsoft really understood enterprise-grade software. At C-Labs, I am combining these experiences to guide our vision and processes to bring new software solutions to industrial automation.

CEOCFO: ***How have you changed your approach since the company started?***
Mr. Muench: The very first approach of my company was just to fix the IoT communication problem. What I found out during that task is that it's very hard to sell this underbelly of a solution; it's perceived as nothing more than plumbing. People want to see something, feel something, and understand what it can do for them. Customers are interested in the data that ends up on a factory control panel, or provides insight into machine maintenance, but not how the data actually got there. They are not that interested in that. So one of the things we added in the latest version of our product was a complete user interface layer to expose more easily what our plumbing could do. We call it the NMI, the Natural Machine Interface, focusing on Mobile Devices, Touch and other NUI (Natural User Interface) technologies. Now we have something visually rich to show and click, and to demonstrate data flowing in real time, which opens up customers' eyes to what is possible with the IoT.

CEOCFO: ***Why pay attention to C-Labs today?***
Mr. Muench: Three things make C-Labs unique. One, compared to other solutions we are extremely IT-friendly. We do not bypass IT departments; we work with them, which is very important in factory automation right now, and why CIOs love us. IT is gaining strength and responsibility due to the Stuxnet worm and other incidents where factory systems were hacked or sabotaged. Two, our technology provides a manageable and routable protocol that reaches across multiple networks without requiring that devices connect to the public internet or a carrier network. Other vendors connect factory devices to the cloud and hope for the best. We enable connectivity that protects factory equipment yet can go through corporate routers and firewalls and provides IT teams the tools they need to be happy with the solution. Three, we developed C-Labs around the IoT, so we are not like the M2M vendor doing a find-and-replace on M2M and now calling itself an IoT company. C-Labs started with the IoT in mind, we fully understand the unique IoT problems, and we build our products directly for the IoT.

Interview conducted by: Lynn Fosse, Senior Editor, CEOCFO Magazine



C-Labs

For more information visit:
www.c-labs.com

Contact:
Chris Muench
+1-425-999-3295 x101
chris.muench@c-labs.com