INDUSTRIAL INTERNET OF THINGS

--- Point of View: Are US Manufacturers Ready for the IIoT?

Inflection points and major technological disruptions occur that change the face of industry and society. Many acknowledge the breakthroughs at the turn of the century hearkening the age of the Industrial Revolution. Several decades later, advances made by Edward Deming in Bell Laboratories and others in organizational and operational practices brought attention to process quality leading to today's Six Sigma and Lean programs. For the most part, the automation and manufacturing world (OT) has existed with attention given to process and practices confined to the plant floor, where machines such as actuators, controllers, monitors and motors speak "OT" languages and protocols to perform business processes with performance measured in micro and milliseconds. Machine failure can result in costly operational shut downs costing millions.

But "the times are a changin'" and there is a new mathematical model best in class manufacturing and industrial players must adopt. It's the adoption of technologies and platforms supporting The Industrial Internet of Things (IIoT). Adoption of IIoT is much more than simple interconnection of machines – if it were that easy we would all be done and having a beer now.

The OT world and the IT world are different – in the most basic terms in the areas of technologies, protocols, base technologies, priorities and cultures.

According to over 350 manufacturing executives asked in 2014, almost half of the respondents did not know what the term "Internet of Things" meant, much less how the IoT would impact their business or industry. Most agreed that 30% of the IoT developments will be seen in manufacturing, or within the Industrial Internet of Things (IIoT). Mostly all manufacturing executives expect profits derived and anticipate making significantly larger investments in IIoT within the next 5 years. The capture and conversion of raw data from an estimated 25 Billion "smart devices" on the automated plant floor by the year 2020 presents a challenging, and potentially impactful task ahead.

OT plant floor assets are rich in data, and this data is often orphaned – living in smokestacks and resident on particular machines. Collection of data is at the device level, and made often on an ad hoc basic resulting in reactive decision making ability. In fact, less than 14% of US

manufacturers have tied machines together allowing for the collection, interpretation and analysis of this raw data that has the potential to be converted to real time, actionable information.

Manufacturing assets typically "speak" industrial protocol languages such as ModBus, and "networks" in the IT sense of the word are disparate. Approximately 60% of the assets utilize some form of ModBus communication, 30% utilize Ethernet and 20% utilize wireless. Manufacturers can now "leap frog" from older technologies to wireless with incremental and greater return on investment. Use of standard protocols such as a common industrial protocol and use of common transmission protocols such as Industrial Ethernet allow for a scalable, cost effective and interoperable bridge forward – bridging the path from the OT to the IT cloud.

A common "interconnect" is the gateway. Much like the Voice over IP (VoIP) gateways tested in the late 1990s converting circuit time division mux signals to their data counterparts, the "gateway" in the IIoT allows for the interconnection of industrial protocol data to the "IP cloud". A host of gateways are readily available today. So once we prepare the plant floor with a common transmission link, connect and collect data from the machines, package and convert the data at a gateway, then we're in the cloud and that's it. It's simple. Well, not exactly.

Collection of data from a potentially exponentially large number of smart devices is daunting. For a security expert, a "smart" device is also an "exploitable" device, allowing for hackers to access networks through the weakest link and backdoor into your mission critical operations. In fact, according to the World Economic Forum Study conducted in 2014, over 80% of global manufacturing executives believe that their networks will be subject to hacking and/or compromise. Security is and will be a consistent issue in IIoT adoption rates and the bad guys aren't going to go away anytime soon. So, security must be addressed from initial policy through network design, monitoring and throughout the process. Many companies have a BYOD (bring your own device) policy, allowing for a myriad of devices to access core networks without a clearly defined rules based access control (RBAC) policy or administration. So the IIoT adoption will stall and only be fully implemented through the enterprise if and when security issues are consistently addressed and regularly re-assessed. The best intruder to a manufacturers' network is internal, or better, a focused team of hired consultants paid to conduct ongoing intrusion testing. Fortunately, platforms and security professionals exist to address security issues today.

perspective: Ready for IIoT

A large majority of US manufacturing executives indicate they "don't know where to start" in establishing what projects to initiate and fund, and which projects take priority over others. Recalling our experience in working with global clients considering implementing "voice over IP" and replacing "old telephone core networks" with networks supported by the Internet, we faced a similar set of questions and problems. Most Internet experts agree that use of the Internet core to support a myriad of broadband communication types (voice, data, video, etc.) represented Internet 3 – an explosive period of time and technical evolution. So we can use our knowledge and experience and apply lessons learned during that Internet inflection point to the current Internet 4 (IIoT).

Working with Bell Labs researchers, several years ago we designed an economic model to demonstrate under what set of circumstances would we deploy large-scale VoIP networks as greenfield, replacement, or enhancement. The merging of the "circuit switched telephone network" world and the "Internet world" was converging, and in many respects analogies can be made to the merging of the OT and the IT into today's IIoT. In all cases, the goal was the same, and the question was the same. When will we deploy technology, where and how so that we achieve the greatest return on investment (ROI)? Once the modeling was completed, resources, tasks and priorities were better understood and deployed. The same modeling should be done with respect to the IIoT adoption, where projects are defined and priorities set based on the highest ROI combined with the strategic goal achieved. Basically, technology deployment should either make a manufacturer money (new product launch), save them money (conversion of reactive decision making based on raw data to predictive decisions based on actionable information), or reduce risk (avoid costly operational failures). Therefore a critical relationship exists between application and adoption of technology and the economic drivers of that same decision. Of course, with proper data, financial experts can model the data to determine ROI and project priority.

A comprehensive analysis of OT process over a full business cycle assists the manufacturer collect, analyze and interpret the raw data required as input to the analysis. Layering onto this data stream, and working with tenured OT and IT professionals who can make investment decisions for technology investment including calculated ROI is necessary to identify the priority of projects selected.

The OT and IT working groups are culturally very different, both within and outside of the manufacturers' landscape. Cross functional, nimble teams with executive team support

throughout the engagement from project start to deployment are critical to deployment and success.

The protocols, platforms, and software are ready for IIoT deployments now. It's now up to the people to collaborate across functions and cultures to make the IIoT a reality.