Machine Design

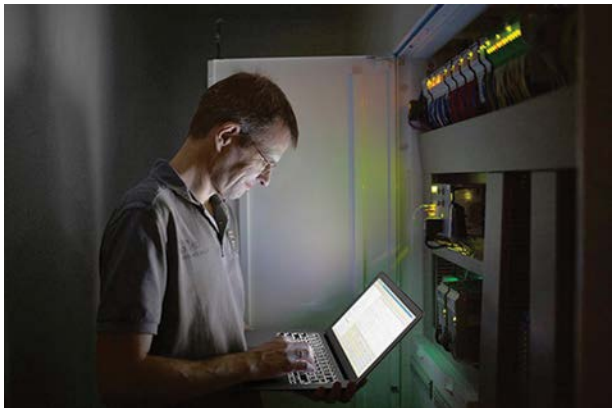
JEFF KERNS | Technology Editor

Will IoT Kill DIY?

Service agreements and certifications may prevent manufacturers from fixing their own equipment, but that could turn out to be a good thing.

Technology is changing the way we look at instrumentation and controls. To maximize profit, business plans are leaning heavily on the aftermarket, software technology, and Industrial Internet of Things (IIoT). Questions about who owns the equipment, software, and even the data become serious concerns to anyone involved. This article will show how software and IIoT are both helping and hurting industries by adding valuable features, but possibly preventing maintenance or modification to be done on the equipment.

"The rules and expectations for 'ownership' have mutated profoundly over the last couple of decades," says Jason Walker CEO of Stanley Robotics. "It seems clear that a company can claim almost anything as their product, and it's buyer beware as to whether the model being sold is what works for them. The trends seem to indicate, however, that the less open a company is, the more reluctant customers are to choose that company."



With new data services, online apps and dashboards can be accessed for remote use via computer, tablet, or phone. A data-service company might charge depending on how much access, or which features, a client wants to use.

RIGHT TO FIX

It is not news that companies are trying to get your money, but if they try to keep you from fixing your own equipment, some people have filed a grievance. As equipment becomes more advanced and connected, we are seeing third-party companies popping up offering services. Often they have dashboards, so engineers can make informed decisions on maintenance to reduce downtime. However, this same connectivity might hinder your ability to maintain the equipment independently.

The right to fix is a long ethical debate and legal battle, which saw a victory for Massachusetts' wrench turners in 2012 in Bill H.4362. This act protects motor-vehicle owners and small businesses involved in the repair of motor vehicles. The bill says that independent repair facilities will be given the same access to diagnostic equipment as the dealers of vehicles from 2002 to the present.

The bill also states that diagnostic and repair information and technical updates must be available "through the manufacturer's internet-based diagnostic and repair information system or other electronically accessible manufacturer's repair information system." Ultimately, anything a certified dealer has access to must also be accessible to an independent facility or vehicle owner. In addition, everyone must be able to access it in the same way and at fair and reasonable terms. This aspect limits the manufacturer's ability to price gouge.

The impact of this bill has been spreading nationally. "A patchwork of 50 differing state bills, each with its own interpretations and compliance parameters, doesn't make sense," says Mike Stanton, president of the Association of Global Automakers. "This agreement provides the uniform clarity our industry needs." Every car made in 2018 and after will have every code and all repair data available in a common format. This right to fix has strong backers such as AutoZone and Jiffy Lube, but the backyard mechanic and farmer don't have big independent repair corporations to fight for them.

RIGHT TO FARM

Recently, the same fight was taken up for off-road vehicles,

2 - As more automated equipment is connected over the internet, bandwidth and local processing will help ease the massive amount of data that must be handled by service providers and cloud resources

due to issues like tractor manufacturers putting software locks on sophisticated farm equipment. "Very few repairs require software; very few repairs require diagnostics," says Chuck Studer, Director of industry Relations for John Deere. Studer provided no numbers on basic maintenance and repairs that would require a farmer to have software access, but it's enough to make national headlines.

Farmers have turned to Eastern European, Russian, and Chinese hackers just so they can continue to keep their tractors running on their schedule—not when a certified mechanic is available. Hackers create their own firmware that will circumnavigate software locks put on the equipment by the manufacturer.

In a worthwhile podcast from Pri.org, farmer Kyle Schwarting said, "We can't communicate with the electronics on a tractor anymore. Let's say you're out in the field planting corn, and your tractor breaks down. In my case, the nearest dealership is 75 miles away, so for them to come out could cost me $2,000 to fix a $50 part." And sometimes those mechanics would only need to plug in a USB to the tracker, wait a few minutes, and leave to fix some problems. John Deere's Studer stated that anything requiring a certified dealer or mechanic to jump in is a rare, not common, occasion.

"If you look long enough, you can find anything you want on the internet," Schwarting continued. "If you're talking about the Russian software, if you want to buy it from them, or from China or whoever it comes from, you're gonna do whatever you can to get your tractor fixed if you have to. When a crop's worth $100,000, you just can't afford to not get it done. Most every farmer has someone that can help them out if they get into a bad spot." This has become an international business. Anyone able to hack the tractor's software is becoming in-demand. Some people now fly to Russia multiple times a year to keep their farm running.

RIGHT TO MANUFACTURE

"When thinking about whether this battle *could* bleed into manufacturing, I immediately go to the cultural differences between farming and manufacturing," says Jason Walker, CEO of Stanley Robotics. "Speaking as someone who grew up in a family full of farmers, I think of farmers as being extremely intelligent, resourceful, and independent; they are all of those things out of necessity. When it's time to harvest, plant, or spray, there's not a big window of opportunity when conditions are optimal. If a piece of equipment is impeding progress, they don't have time to wait for anyone to come and fix it."

WHERE SUBSCRIPTION AND IIOT MODELS ARE WORKING

DESPITE SOME BUMPS in the road, the subscription model is generally considered a success in the auto and farming industries. One place where subscription or leasing seems to be particularly effective is in aerospace. GE and Rolls Royce have started renting their engines by the hour rather than having the airlines purchase them. Such a system might work better in aerospace rather than vehicles, tractors, or manufacturing equipment, as it is highly regulated. Of course, road vehicles have regulations, too, but they are not nearly as strict as aviation rules, regulations, and litigious concerns.

In addition, this puts forth the idea of involving large and small companies alike. Even the small airlines are big when compared to a family-owned manufacturing plant or farm. Smaller companies are accustomed to doing their own work, while larger companies may be more lax and have the revenue to let someone else manage it as long as the ROI fits its business goals. Bigger companies, especially in the U.S., may welcome this certified, hands-off approach if it can alleviate them from having so much liability.

"The most radical departure from a traditional component purchase is the idea that customers will start paying for up time," says Marissa Tucker, product director at Parker Hannifin. "This mirrors what has happened to some extent in the ride share business. The consumer only pays for the car when they're using it, and expects it to be operational. The driver also has an agreement with the company to drive safely and not damage the vehicle, etc.

"Similarly, in industrial automation, IIoT would allow the ownership to reside with the manufacturer—where they own the product and data, but also have the responsibility to maintain operation up to the consumer's standards," continues Tucker. "IIoT is required for such a model because predictive maintenance and monitoring are crucial. If a product is about to fail, the company needs to send a replacement, or they'll be on the hook for damages. In addition, if the consumer uses the product out of spec, the company also needs to monitor this as to charge the consumer some penalty for shortening the expected life of the device."

Manufacturers may have a bigger window to "harvest," and if the IIoT delivers in its claim of predictive maintenance and a certified technician is needed, she/he should schedule a visit before something actually breaks. However, you are still putting trust in another person or company. Could this new technology be setting a trap?

In the traditional model, the customer buys the machine and owns it. New technology lets the customer choose to enable features through the OEM. From there, however, things will vary.

"These monthly models are where the real complications arise," says Marissa Tucker, product manager at Parker Hannifin. "Using both the consumer and industrial models as examples, often the customer is paying to access the data. But once it is on a company's server, the data is owned by that company. Whatever protections were specified in the user agreements is what the consumer is given. So what happens when the customer stops paying? Can they still access their prior data? It depends on the user agreement."

Often, manufacturing equipment leaves control of the machine and data to the user. Once they decide to use a feature, it can be like any other collaboration with an outside source. However, like tractors, what happens if the machine purchased has diagnostic capabilities, but the user is blocked from that feature? Now the owner of the equipment is forced to hack or pay for access to sensors and data they own. Or is that impeding on the OEM's intellectual property?

OEMs are not trying to trap anyone. Most of the time, the user has access to the data. Without the right software and analysis, though, the data is pointless. OEMs know this fact, and know that this type of analysis and software is probably not the user's core competency. If the equipment comes with an easy-to-use software subscription, it is hard to think users would opt to figure out all of this new technology on their own.

For this reason, connectivity and subscriptions in manufacturing will work. Also, if users have access to the information from the purchased sensors, it will be hard to argue about being trapped. Once manufacturers see the data analytics and benefits of the software offered by some OEMs, customers also will have no problem paying for a service or subscription fee for the added value—if it is needed.

As Stanley Robotics' Walker notes, "Manufacturing equipment tends to be more homogeneous, or at least, there are pods of homogeneity. The homogeneous nature of factories lends itself to relying on a service provider for support and repairs, because it makes more sense to have one contract, or one person, or one team to take care of an entire assembly line. I think that model, by extension, lends itself to maintaining a less-open business model. The manufacturers can have their own people, or their licensed integrators, maintain the equipment and thereby reduce or eliminate the need for a third party to request access to the data needed to service or integrate with the equipment.

"However," he continues, "while it might be true that equipment makers can maintain their models of proprietary access in manufacturing longer than in other domains, it seems obvious that a more open and collaborative approach is winning in the market."

Overall, the numbers will decide the right course of action. The main divider is that OEMs are looking at the return on sales (ROS) – the amount of profit produced per dollar of sales, while the users of this equipment are looking at the return on investment (ROI). But the mentality shouldn't be that increasing one company's ROS is reducing another company's ROI. The thought should be: How do we work together to increase both.