WHITE PAPER

Integrated Sensing & Internet of Things (IoT)

Data collection driving value-based OEM design

DENNIS JENSEN
BUSINESS DEVELOPMENT MANAGER, ADVANCED PRODUCTS

FRITZ BYLE
SENIOR PROJECT MANAGER, ENGINEERING

Millions of products and systems are connected to the Internet, and access to the data generated by those products/systems is one of the most valuable assets of the 21st century. Understanding the value and risks of making OEM designs Internet-enabled is critical for success and customer security.

TLX Technologies

INTERNET OF THINGS (IoT) IS A VERY HOT TOPIC across many industries. Gartner[1] confirms that 20.8 billion connected things will be in use by 2020 with a total spent on IoT devices & services exceeding $3 trillion in 2018. Numbers like that get the attention of executives, which then drives questions to OEM design teams about what they are doing for IoT innovations. It is important for the entire design team to discuss options and develop a plan for how IoT enhancements will drive additional revenue and/or new business. Engineering is most powerful when the different disciplines work together and not in separate silos. Everyone must be on the same page to ensure that IoT initiatives are successful in contributing to the bottom line.

The real value of adding Internet connectivity to a product comes from the data and/or control that would be available to customers. Each industry will have different critical value propositions; some require high quality performance, others can't deal with unexpected outages, and still others need improved visibility over their product/system, etc. By starting with the client's critical needs, engineering teams can determine what type of data provides the most value along with the sensors that need to be deployed in the product to provide that functionality. For example, most processing companies will do almost anything to avoid unexpected downtime. They would greatly benefit from IoT enabled solenoids that can track temperature, vibration, and other data at different points in their equipment. Rather than trying to insert sensors on an aftermarket basis, they could be integrated into key components to track critical functionality, validation, and recalibration efforts. Once the information is collected by the sensors, the data can be transferred to a database and displayed on a secure website, used in Artificial Intelligence (AI) programs or other initiatives. Systems can also leverage predictive maintenance intelligence, which will help customers with preventive maintenance and improved process understanding. These are just a few examples of the value engineering teams can design into their next generations of processing products.

The real value of adding Internet connectivity to a product comes from the data and/or control that would be available to customers.

INNOVATION THROUGH INTEGRATED SENSORS

One example of integrating sensing capabilities is TLX's supervised solenoid actuators for the fire protection market. These actuators already have basic integrated supervision to let the system know if they have been installed correctly. In addition, TLX has created the event recorder which can be attached to these actuators and acts independently from them. These recorders keep a time-stamped log of past events, provide proof of installer work, and give historical data for risk mitigation. They are passive devices that provide data output only.

The event recorder senses important information, such as the temperature around the actuator, the amount of current going into the actuator coil, whether the device has been actuated or not, whether the actuation was caused by mechanical shock or not, if events occurred during live or service mode, and if the actuator has been installed properly. System owners can then view a time-stamped log of past events to learn why the system activated.

Beyond the direct benefits to clients, OEMs can also use sensing/IoT functions to improve their margins and customer service. This capability is especially valuable with warranty audits. Sensors can be strategically placed in the OEM system to track misuse or other issues. Fire suppression products can be triggered unexpectedly if components of the system are impacted. Sensors can collect data on shock and/or position to confirm when the system sustained a mechanical impact. This could save the manufacturer thousands of dollars in analysis costs, and it would also allow the fire suppression OEM to show the client that the accident was not due to a faulty product. Another option in the same market could improve ongoing support. Collected data could be displayed to a private website or app that is only used by approved/certified repair partners. This type of set-up will drive aftermarket work to approved OEM channel partners, and it will also allow the repair technicians to provide better service. Because the deployed system will use data to confirm system status, repairs could potentially be executed before the customer even knows there is an issue.

Data collection will also have a significant impact on the security industry. Locking components can be turned into smart subassemblies that communicate critical information

Locking applications can include different sensors that are protected by a cover and hidden from view.

about the use of almost any type of physical access system. This will be critical for high value enclosures or pharmaceutical storage because the electric lock can record the time/date of access. An accelerometer can be even added to detect break-in attempts, which can also be time/date stamped. A more innovative system could be used for food storage, package pick-up lockers, and drug storage. In these cases, the locking system can include a temperature sensor to track the environmental conditions inside the cabinet. When combined with IoT capabilities, the system could send out an alert if the food or medications are being stored outside of a safe range. The system could even be designed to include a reporting function to add even more value, using the information to meet requirements of the Health Food Safety Act (HACCP Plan).

Creating Internet based controls for products and systems will be exciting for some industries, but each OEM should take a very hard look at the total return on investment for this type of work. There are challenges that stem from security issues and misuse of accounts or control systems. Hackers, in particular, pose a real threat to any web-connected product or system. The damage done by hackers can be costly even though, in some cases, personal or financial information may not be at risk of exposure. The fuel industry once suffered an attack[2] that compromised tank gauges. No money was stolen, and no personal information was exposed, but in many cases the control equipment software was corrupted, requiring an expensive on-site maintenance visit. Remote-access equipment is an attractive target for hackers, so OEMs will need to weigh the risks and benefits associated with any web-connected system and then determine and implement the appropriate layers of security.

There are many ways to leverage data flow from OEM products to generate new revenue streams in addition to traditional sales. Many companies are launching subscription models where the client pays a monthly or annual fee related to the data collection and/or software availability. Customers taking advantage of these extra services experience value every day because access to data and a web

dashboard improves their operations, incentivizing them to continue the partnership (and investment). This type of business model not only drives long-term relationships and future purchases, it also provides ongoing revenue.

This paper starts with the value of data collection because without that, there usually is not an adequate return on investment to add Internet access to the equipment. Once the design and/or product teams confirm the data customers need, the next step is figuring out how to connect the product/system to the Internet. However, rather than focusing on the type of connection (wired, WiFi, cellular, etc.), the team should review how critical uninterrupted Internet access will be to the end customer. This is a very important question for the design team and product management. If Internet access or data flow is critical, the design team should investigate an appropriate backup connection. For example, the main connection could be wired, and if that fails, the system would failover to a cellular connection. Such a feature could be marketed as a "value added" option, allowing customers that need such capability to purchase it. If an uninterrupted connection is not critical, the development team can implement the customer's desired type of Internet connection along with the ability to store sensor data (locally) in the product/system if Internet access is lost for a period of time.

Many OEM products have long life cycles, so it is best to include encryption and other security protections in the initial design.

System and data security should be discussed for every OEM project, even if remote controls are not going to be part of the designed features. As mentioned earlier, there will always be hackers who want to target remote-access systems. Data is very valuable and becoming more so, especially to hackers. Consider, as an example, the retail space. Initially, companies only needed to safeguard (credit) cardholder data, but in just a few years, the industry was forced to protect personally identifiable information (PII), which is a much larger information category. Even Europe has passed legislation related to data protection. Many OEM products have long life cycles, so it is best to include encryption and other security protections in the initial design. This action avoids costly updates to deal with any stricter laws being passed in the future. Additionally, the effort can also be used to highlight how advanced the system is and the value it offers clients because it protects the customer's data from the very beginning.

IoT is more than a catchy acronym. It is the starting point for new functionality in products and an improved customer experience that comes from a collaboration of all the engineering disciplines on the team. By collecting the right data from sensors that are integrated with key components, OEMs can use dashboards, artificial intelligence, reporting/alert systems, and other functions to make their clients more effective and profitable. In return, these efforts are rewarded with additional sales from new customers along with ongoing revenue from software services. Each design team will need to do their own evaluation on the best functionality for their projects, but don't hesitate to talk to potential partners that can speed the development process and add value to the finished product.

[1] Retrieved from: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[2] Retrieved from: https://islandpumpandtank.com/environmental-contracting/some-fuel-retailers-dealing-with-hacked-inventory-monitoring-devices/