The challenge of powering industrial IoT applications

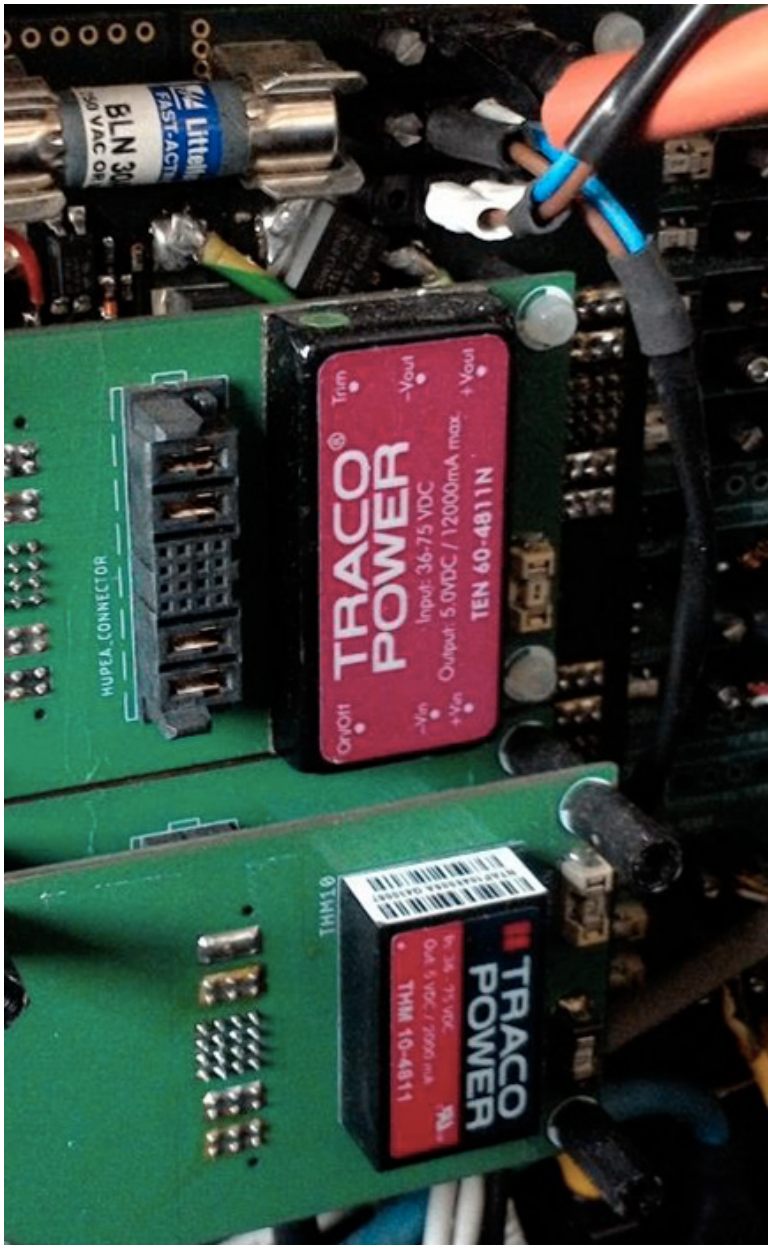
The hype around IoT devices nowadays is not surprising. IoT engineering kits and the appropriate technologies for designing IoT prototypes are widely available and affordable for creative technology enthusiasts. Consequently, there are no limits for enabling ideas and possible business models based on these technologies.

Also in the industrial environment, there has been an rapidly increasing demand for professional IoT applications. Common characteristics include the ability to distribute intelligence by connecting various sensors and actuators with decentralized control. The ability to make them smart is that these sensors and actuators can collect and communicate data and are designed to be managed with intelligence. The market for industrial IoT applications will continue to expand as more applications evolve, including (home) healthcare, infrastructure, utilities, home automation and smart homes, vehicle, mobility and more. These professional IoT trends will undoubtedly involve miniaturization, mobility, robustness, efficiency (degrees of effectiveness) and the networking of electronic devices.

In contrast to hobby IoT applications, such safety-relevant industrial IoT applications are subject to strict regulations, both, for the engineer and for the components being used. This poses a great challenge for developers of industrial IoT applications. The use of certified, reliable and long-term available electronic components is critical, as they are often used in safety and function-critical applications. The professional support of component suppliers is playing a very important role.

Requirements for powering professional IoT applications

Critical modules within professional IoT devices are without a doubt the power converters and the power supply. Miniaturization, low power consumption, size and a high efficiency are playing an increasingly important role for those products. Semiconductors are probably the components which offer the highest level of innovation. As a second key technology I'd mention the power transformation and isolation devices used in the products. Additionally, since these mostly battery-powered IoT systems spend most of their time in standby mode and only a small part is in active mode, the built-in DC/DC converters must cover a wide load range with high efficiency.

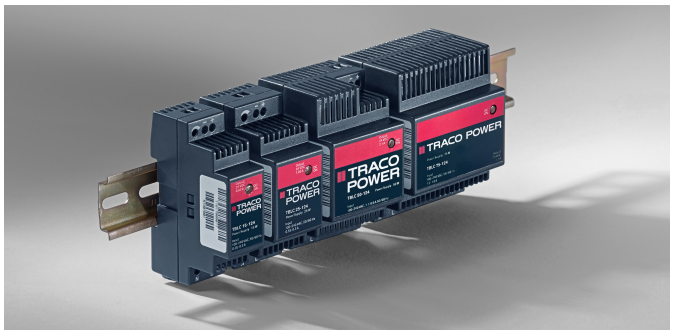


Size and efficiency matter- what else?

In order to design, certify and market such professional IoT devices, not only these technological product features matter. If these professional IoT devices want to be certified and sold, they have to be fully compliant with increasingly stringent regulations through globally harmonized standards and guidelines, which bring a big challenge to today's IoT electrical engineer. If IoT functionalities are required for critical applications such as in medical technology, the electronic components must be designed in such a way that they can be used accordingly, meeting industry specific regulations.

As an example, let us take a medical approved, wireless, battery-powered control panel with Internet access to the patient file. Wirelessly connected to this control panel is another device, which may can come into contact with the patient (e.g. a blood pressure monitoring device). One of the key safety concerns with respect to medical devices is that the patient is often electrically connected to the device. As a consequence, the power supply and the DC/DC converter of this IoT application must meet safety critical regulation such as BF compliance and 2XMOPP standards within IEC/EN 60601-1 3rd Edition.

Another good example are industrial IoT applications for "smart" homes and buildings. High efficiency & low no-load power consumption (ErP compliant), small size, high reliability and an affordable price are key elements to all these home/building IoT automation applications, and the ever-increasing compliance & standards including IEC/EN 60335-1.



Careful planning is required, with the entire supply chain

We know the use of new technologies in security-sensitive and functionally critical applications requires increased reliability, quality, service life and certifications and - last but not least - seamless traceability of electronic key components.

Manufacturers are more and more in the need to use tools that have been established and perfected in the automotive industry for years, such as failure mode analysis, Corrective actions, 8D Reports, DFMEA, PFMEA, Total Quality Management and continuous improvement).

Today Total Quality has to find its way into the earliest phase of almost every development. To achieve this, a developer today has to do more than just provide a functioning solution. Where a mobile telephone used to be a useful accompanying instrument, today we are increasingly dispensing with redundancy from other means. Cash, camera, address book, subscribers are all integrated into the smartphone. Smartphones are therefore critical life companions today. The product designer today bears much more responsibility for the quality of his development than he did 10 years ago. We all know that this trend not only continues but will continue to develop rapidly. Moreover, suppliers should regard the digital transformation in the individual components' supply channels as a highly significant development. By establishing, analyzing and processing relevant data, a fast, reliable and economic availability of the components

can contribute to increased productivity at the customer's facility

In summary: This means that in IoT applications in critical applications, for example in medical technology, building automation or mobility, not only need to be efficient, miniaturized with a ultra-low standby power consumption, they also need to be available for decades, tracable and fully compliant with the relevant standards and regulations.

Author Florian Haas, Director Marketing & PM
Date July 2019

Contact/ queries

Yves Elsasser
Traco Electronic AG
Sihlbruggstrasse 111
6340 Baar
Switzerland

Tel: +41 43 311 45 11
E-mail: ye@traco.ch
Fax: +41 43 311 45 45
Web: http://www.tracopower.com

TRACO POWER