March 2015

PSD EUROPE

Empowering Global Innovation

Special Report: Internet of Things (pg 31)

PSD EUROPE
Empowering Global Innovation

WWW.POWERSYSTEMSDESIGN.COM

Visit us online for exclusive content; Industry News, Products, Reviews, and full PSD archives and back issues

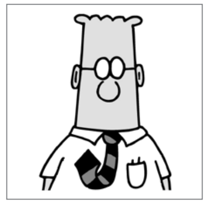
COVER STORY

TECHNICAL FEATURES

SPECIAL REPORT:
INTERNET OF THINGS

COVER STORY
Driving the Internet of Things (pg 12)

Highlighted Products News, Industry News and more web-only content, to:
www.powersystemsdesign.com



PSD EUROPE
Empowering Global Innovation

Power Systems Corporation
146 Charles Street
Annapolis, MD 21401 USA
Tel: +410.295.0177
Fax: +510.217.3608
www.powersystemsdesign.com

Editorial Director
Alix Paultre, Editorial Director,
Power Systems Design
alixp@powersystemsdesign.com

Contributing Editors
Liu Hong, Editor-in-Chief,
Power Systems Design China
powersdc@126.com

Dr. Ray Ridley, Ridley Engineering
RRidley@ridleyengineerng.com

Publishing Director
Jim Graham
jim.graham@powersystemsdesign.com

Publisher
Julia Stocks
Julia.stocks@powersystemsdesign.com

Production Manager
Chris Corneal
chris.corneal@powersystemsdesign.com

Circulation Management
Sarah Corneal
sarah.corneal@powersystemsdesign.com

Sale's Team
Marcus Plantenberg, DACH-Region
m.plantenberg@pms-plantenberg.de

Sydele Starr, North America
Sydele@powersystemsdesign.com

Registration of copyright: January 2004
ISSN number: 1613-6365

Free Magazine Subscriptions, go to:
www.powersystemsdesign.com

Volume 12, Issue 2

The IoT: revenge of Thin Client?

Once in a while we see echoes of things past in new technology development, in this case, the Internet of Things (IoT) has shifted an old methodology to its zenith of maturity. In both hardware and software, managing the IoT requires us to think of devices as clients again, an echo of things past from the beginnings of the computer age.

Big boxes

Once upon a time, computers were huge complex machines that not only cost a lot of money, they also needed a crew of people and their own special environment to function in. A smart person recognized that since a computer, even the valve-driven behemoths of yesteryear, think way faster than people can. This enabled a company to buy one computer and put it in the basement for everyone (with access privileges) to use from their office, or a common room. Each user's position was simply a dumb terminal, a "Thin Client" because it had no processing power on its own.

As computing progressed, power moved to the desktop (and eventually the hand), enabling companies to retire the basement mainframe and replace it with a communications, memory storage, site-hosting server. This was not thin client, as the processing power used in the software by the device was contained within it, with the server's role being only data transfer and offsite data storage.

With the advent of the Internet of Things and the creation of cloud-dependent devices, we see a slight return to the old management paradigm of Thin Client. There is still plenty of processing power and memory in the user's device, but now an offsite server, linked to the device by the cloud, now does some of the heavy lifting. For example, a handheld device can now use offsite processing power for a task like real-time language translation.

The complete picture is of course far more complex, with data, memory, processing, timekeeping, and a plethora of other functionality, much of which has not been invented yet. The IoT is now a community, not a server-client relationship but more and more a weave of devices, functions, and roles. These roles will be determined more by haptics considerations and product/service convenience to the user more than by technological capabilities.

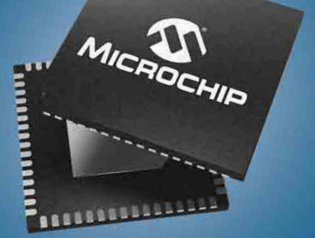
Is the server dead?

As we migrate forward, the massive computing power in our devices will be harnessed to create huge intelligent mesh networks, sharing the processing needs among them. One day there will be a a massive computing entity, a "Mesh" supporting other devices when you aren't using it.

This does not mean that the fixed site server farm is dead, far from it. The need for secure storage and redundant management and oversight, plus the need for additional functionality that may not be supported by the Mesh, demands some kind of secure facilities in the future. Not to mention that this migration could take decades, not because the tech cannot achieve it, but because the legacy systems and infrastructures would take that long to replace. However, I may be pessimistic on the time scale.

Best Regards,

Alix Paultre
Editorial Director, Power Systems Design
alixp@powersystemsdesign.com



Electric Imp connectivity platform reduces NYC building energy usage up to 15%

According to the New York City government, buildings within its five boroughs are the single largest source of greenhouse gas emissions. New York-based clean energy company Bonded Energy Solutions concluded that the biggest compliance challenge that building managers faced involved how much energy their properties were actually using.

To solve these challenges, Bonded Energy Solutions built online monitoring systems using the Electric Imp connectivity platform as a simple and inexpensive way to remotely check, accurately measure, easily consolidate and alter energy usage in real time. Electric Imp-enabled sensors were placed on energy sources, such as gas and water meters, radiators and boilers, to collect room and heating device temperature and usage activity data, which was then sent to Bonded Energy Solutions' back-end cloud database for interpretation, management and storage.

Electric Imp's connectivity platform streamlined the entire process by enabling connectivity to previously unconnected devices, centralizing data gathering, and allowing system management and a single method of communication between disparate equipment and sensor mechanisms. Once in place, energy could then be checked at any time day or night and redistributed more efficiently throughout the entire building.

Making a useful networked device is a challenge facing industrial and commercial product manufacturers. Businesses that tried venturing into Internet connectivity usually ended up reinventing the wheel at great cost, resulting in products that were expensive, fragile and often communicated to nothing more than a smartphone app.
What was needed was to take the best implementations of hardware, firmware and cloud service, consolidate them into a powerful Internet of Things platform, and let them be applied to any device in the world. Electric Imp, founded in 2012, is the result.

For manufacturers seeking to bring their products and services online, Electric Imp provides a complete end-to-end solution that makes it simple to connect nearly any device to the Internet quickly, securely and seamlessly. The

Electric Imp connectivity platform features fully integrated hardware, software, OS, APIs, cloud servers, and security making it possible to effectively empower devices with greater intelligence, utility and flexibility.

Now, rather than spending time and resources to design, integrate and maintain a connectivity infrastructure, businesses such as Bonded Energy Solutions can instead focus on their core expertise of building the best products possible, adding greater value and differentiation and significantly reducing time to market.

An initial trail upgraded the energy infrastucture of six residential buildings, resulting in a reduction of usage by at least 15%. A more comprehensive trial program will be monitored by the New York State Energy Research and Development Authority (NYSERDA).

www.electricimp.com

Is Germany into IoT?

By: Thomas Hahnel, Lucy Turpin Communications

Although we Germans are the current soccer world champions, our IoT adoption rating is less than world class. Even Telekom CEO, Timothy Höttges, declared in October 2014: "We've lost the first half time of digitalization." In football, losing the first half is not tragic. But you have to figure out how much time is left and catch up quickly.

As elsewhere, several German industries are already adopting IoT. And you can meet people who already talk about the Internet of Everything. Our high-tech organizations, analysts and research institutes predict billions of networked devices for Germany. And because no other country is as dependent on exporting its tech goods as Germany, keeping abreast of trends is essential. So what is the real status of IoT in German industry?

IoT in Germany revolves mainly around on "Industry 4.0", on production technology and Smart Factory topics. BitKom, the German high-tech association, forecasts an annual growth of 1.7 percent for key industrial sectors – driven just by the contributions of Industry 4.0 solutions. Economically, this sounds very promising.

Pessimists liken German companies with the IBM of the 1980s. That was when IBM failed to recognize the potential of the upcoming software industry. Those were the days when IBM simply outsourced an operating system from a little company called Microsoft. The fact is, Germany is not a producer of core IoT technologies. True, we do a lot of embedded software programming. We have many companies designing hardware systems, boards, etc. But most of our business models are based on foreign technology that has been developed elsewhere.

While in Germany institutions are still tied up in discussing industry standards, in the US it seems that MTConnect has already become a standard for data exchange between vendor production facilities. Yes, IoT funding is always going to be higher in the US than in Europe. And there is more red tape in Europe, especially in Germany, multiplying the hurdles to implementing new technologies and businesses. So it's no wonder that the CES didn't highlight any German IoT gadgets.

The exception was, of course, our automotive industry: the Mercedes Daimler CEO presented a super self-driving car, and Audi's was remotely controlled by an agent-style smartwatch. The Internet has become integrated into German cars and there are a lot of IoT business ideas for the future. But here, too, the primary technologies are not "Made in Germany".

Germany has the world's strongest automotive industry. And machine construction, electrical engineering, aerospace and med-tech are state-of-the-art. However, the second half of the match has started, and we have more than just one goal to win. I hope it will result in soccer-like preeminence – you must have noticed that over the last few years, the Germans managed to develop a world-class soccer match system...

www.lucyturpin.de

Dynamics of Medical Electronics Applications

By: Kevin Parmenter, contributor

The medical electronics market is in flux due to a multitude of pressures and forces from a range of sources. Ultimately this is impacting those designing and certifying of medical electronics equipment in the market. It also impacts who they partner with for the power supply and how well they are positioned to deal with the rapid pace of change.

Historically, the requirements for medical electronics were in UL/AAMI 60601, and revisions for this standard has been around for quite some time. What has not changed is the need in the medical electronics market for reliability and adherence to standards and regulatory requirements above all else.

So when standards change, the design of power supplies and equipment may need to change as well. We are now operating on the 60601-1-3 3Rd edition presently, and now they are talking about the 4th edition/revision coming out behind it. Lets review what is accelerating the pace of these changes:

1. As global population ages and life expectancies become longer, 32% of the population is expected to be 60 or over by 2050. This demographic is taking advantage of technology and will continue to need access to advanced medical equipment as the demand for devices and technology grows.

2. The emerging BRIC countries (Brazil, Russia, India and China) combined with the growth in traditional markets means that more will want to have access to medical device technology. If you want to do business there you have to meet the local standards. This increases the number of regulations needing to be met. Systems powered from the mains supplies in these countries carry requirements for even greater surge, sag and transient immunity requirements than before.

3. China's healthcare market is growing at a fast pace, with indigenous companies creating equipment for the local marketplace. This means that competitive companies need to again meet the local regulatory needs such as CCC.

4. The FDA510 controversy essentially the approval process itself and has resulted in approximately 60 changes to the 510k policy since 2010 getting medical equipment approved is ultimately more complex than it was a few years ago. And ISO13485, specifying manufacturing quality, which is being requested, and will likely soon be required.

5. Mergers and acquisitions – in 2014 the merger and acquisitions in the medical industry was 40 % higher than in 2013 and higher than ever. It is forecasted that 2015 will grow even more.

6. "Medicalized" consumer devices also need to meet safety standards, and we will see the combination of consumer products and medical devices as a growth area needing certain regulatory issues to be met in the home healthcare environment

---

Noninvasive measuring of loop gains

By: Dr. Ray Ridley, President, Ridley Engineering

It is always desirable to simplify the measurement process of power supplies, and characterize them without overly invasive testing. This can work for loop gains with limited success, and shows the pitfalls of trying to measure loops noninvasively.

Power supply output impedance measurements

For decades now, engineers have followed Middlebrook's techniques for breaking and measuring feedback loop gains while keeping the feedback intact for regulation. However, in some cases, chip designers no longer make loop feedback points available, or board layouts prevent proper direct measurement. Or, you may just have a black box power supply with no access to interior nodes of the circuit.

It is well known (again from Middlebrook) that you can get the loop gain indirectly by looking at the output impedance of the power supply. **Figure 1** shows the conceptual idea behind measuring output impedance. If you can measure both open- and closed-loop impedances, the loop gain can be calculated, even if it is not directly accessible. The quantities are related by the following equation:

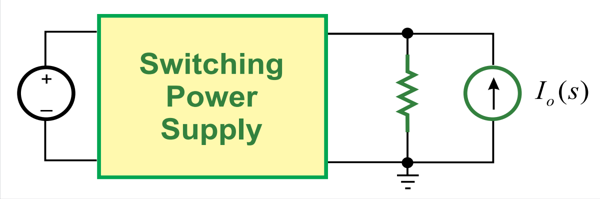


Figure 1: Output impedance is measured by driving a current into the output terminals of a power supply

$$Z_o^{cl}(s) = \frac{Z_o^{ol}(s)}{1+T(s)}$$

Note that two measurements are always needed, and it is not possible to get any meaningful loop stability information from just a single impedance measurement. In order to calculate the loop gain from the above equation, we need accurate measurements of both the closed and open-loop output impedances. As we will see later, this can present problems in the measurement techniques used. These two measurements are shown in **Figure 2** for an example switching power supply.

Figure 3 shows how this output impedance measurement is implemented practically using a frequency response analyzer. No special injection fixtures are needed [2], and as will be shown later, it is important to have flexibility on where measurements are made if you want to get good results.

Figure 4 shows multiple test points

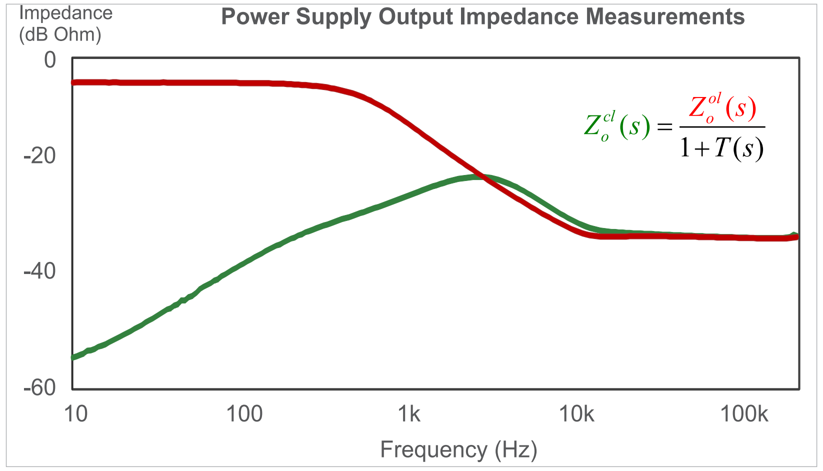


Figure 2: Open-loop and closed-loop output impedance of a power supply.

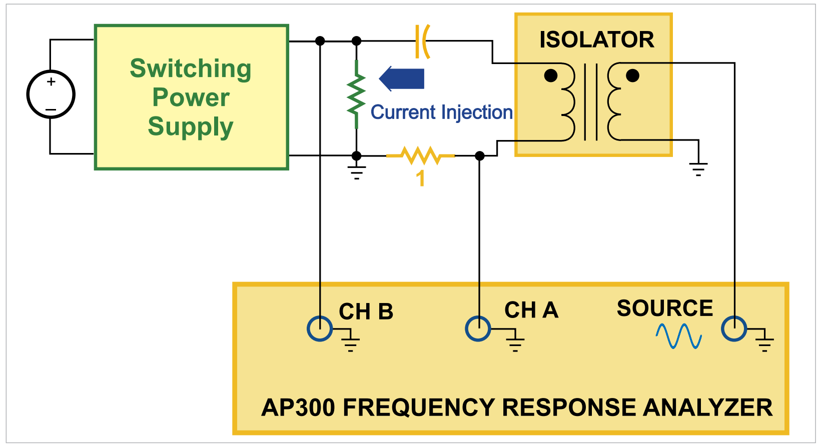


Figure 3: Practical Test Setup for Injecting Current and Measuring Impedance.

where the output impedance can be measured. As power levels go up, it becomes crucial where you inject current, and where the test signal are measured if you want to get reliable results.

The isolated current source is injected into the test pins indicated by the blue arrows. For best results, it is important not to make the measurements at these same pins, and a four-wire Kelvin connection is preferred to extract proper results.

The three arrows, red, yellow and blue, show points on the output voltage where impedance measurements can be made. (These are all the same node of the circuit, the output voltage, but they are separated from each other by parasitic impedances, which become very significant for high power supplies.) Once the impedances are measured, the loop gain of the circuit can be calculated from:

$$T(s) = \frac{Z_o^{ol}(s)}{Z_o^{cl}(s)} - 1$$

Figure 5 shows the measured loop results for a switching converter. There are two loop gains shown in **Figure 5**: the first is the loop calculated from impedance measurements, shown in gold. The second is a direct loop measurement made by breaking the loop in the conventional way. Note that the phase curve shows the phase margin for each of the loop gains.

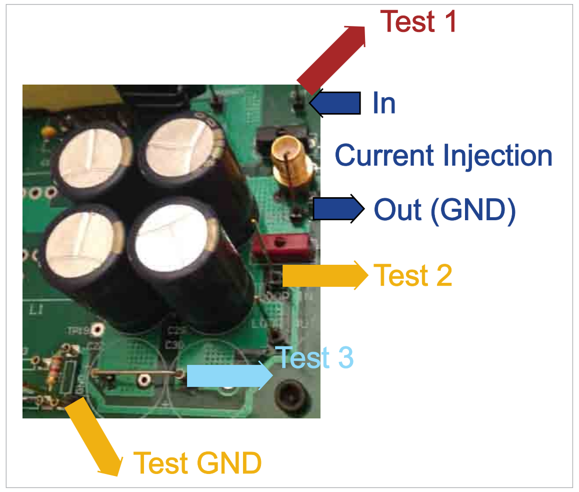


Figure 4: Different Test Points for the Output Voltage.

The results look very good from these measurements. The measurement point for the output impedance was taken from the point on the board where the feedback loop samples the output voltage, and this gives the best results. However, the estimated loop gain is very sensitive to the exact measurement location, as is shown in **Figure 6**.

There are very different loop results obtained when the test point for the output voltage is moved, even a seemingly insignificant amount. The red loop gain curve, which corresponds to the red test point in **Figure 4**, picks up the impedance of the test pin through which the injected current is driven. This is a relatively high impedance compared to the expected output impedance of the power supply, and the result is a very degraded estimate of the gain of the loop.

The blue loop gain and phase curves are even more interesting. Even though the gain is closer to the gold curve (and hence the true loop gain measurement), the starting phase is 180 degrees away from the other estimates of the loop phase. This is caused by a test point just before the output of the power supply and the closed-loop output impedance at that point is actually negative. (Engineers who use remote sensing may be well aware of this kind of result.)

Open loop measurement issues

There is a complication in measuring the open-loop output impedance, especially if you are trying to look at a point of load supply where you don't have control over the input voltage. The best measurement of open-loop output impedance is made when the input line is too low for regulation, and the error amplifier of the feedback loop is railed high. However, it may be impossible to generate this condition when testing a finished power supply. Instead, you may have to measure the impedance of the unpowered system. Unfortunately, that will usually disconnect the inductor from the load, resulting in a higher than expected low-frequency impedance.

If you have to test this way, it will result in a large error in calculated loop gain, as shown by the red curve of **Figure 6**. This observation will vary whether the converter uses current-mode or voltage mode control. If you are testing a black box supply, you will have no idea what the controller is doing, and hence no way to get the proper open-loop impedance. There are no guarantees of the accuracy of the loop gain in such a case.

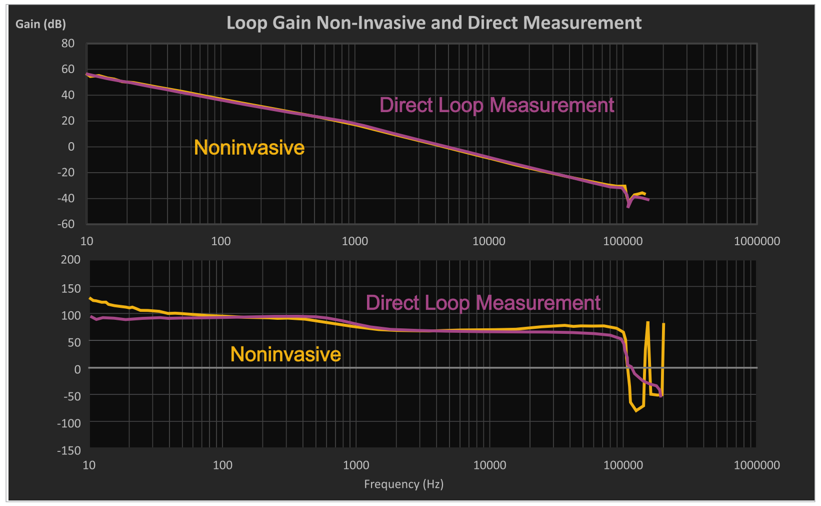


Figure 5: Direct Loop Gain and Phase Margin Measurement Compared with Noninvasive Measurement

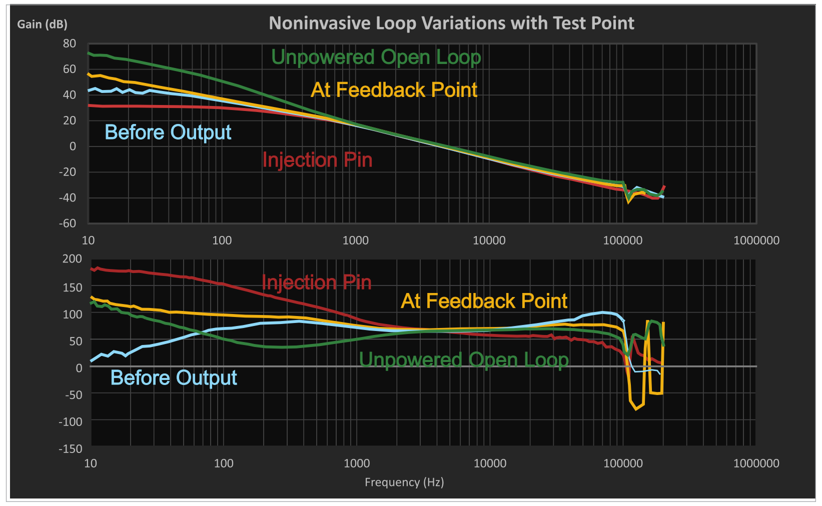


Figure 6: Different Loop Gain and Phase Margin Results Depending on Impedance Measurement Point

Noninvasive measurements

Predicting loop gain from output impedance requires two measurements, one for the open-loop, and one for the closed-loop impedance. The predictions of loop gain that result are very sensitive to the measurement location of the output impedance. It is important to be able to move the test probe detecting the output voltage to the proper feedback point if you want to get reliable results that agree with the true loop measurement. Unfortunately, this proper test point is not always accessible.

Problems also arise in measuring the open-loop output impedance. Ideally this is done with the converter delivering output power, but without regulation active, either with low line input or by breaking the feedback path. If these approaches aren't possible, then unpowered measurements must be made, resulting in large loop gain errors.

Noninvasive measurements can be useful as a last resort. However, they should not be relied on to guarantee the loop gain accurately, or to optimize control loops during power supply development.

www.ridleyengineering.com

Driving the Internet of Things

Powering the myriad of devices that comprise the IoT properly is critical

By: Dave Freeman, Texas Instruments

Figure 1: View of the Internet of Things

The Internet of Things (IoT) has been the topic conferences, articles, and blogs. Much of this has focused on the standards for communication and security of the information and devices. Just as important is powering the myriad of devices that comprise the IoT. It is worthwhile to first describe what makes up the IoT. The idea behind the IoT is that everything worth talking or listening to is connected for communications.

In many cases, the connected item can be an existing device that recently acquired communication capability, or new products created to enrich the information environment. Most often these devices are connected wirelessly. This connectivity sets the bar for the power developer. Wireless communication provides a high degree of flexibility that should not be restricted by any needs for any special power connectivity.

Figure 1 shows one view of the IoT. As the picture illustrates, everything can be connected. We also see that a subset of this concept is the wireless cloud. The wireless cloud provides connectivity for users and their devices. It also points to an important part of power consumption. A white paper published by the Center for Energy-Efficient Telecommunication, CEET, in April, 2013, predicted that the wireless cloud will consume 43 TWh this year (2015)[1]. Of that power, wireless networks will use 90%.

In 2012, the wireless cloud only consumed 9.2 TWh, so this is a very large increase in energy. It is expected to grow as more devices and traffic become part of the IoT infrastructure. This becomes the challenge for power supply designers. At some point in the future, expansion of the IoT will be limited by the energy it consumes. So let's get down to some of the tasks the power supply designer needs to address.

As **Figure 1** shows there are small devices or wireless sensors that monitor the environment, appliances that need to communicate their status, wearable electronics, security systems, automobiles, and industrial equipment, as well as wireless networking equipment mentioned earlier. So there are many devices and associated infrastructure that are integrated to form the IoT. The description of the IoT leave many people thinking of the IoT as being made primarily of wireless sensors that communicate important information – so we will start there.

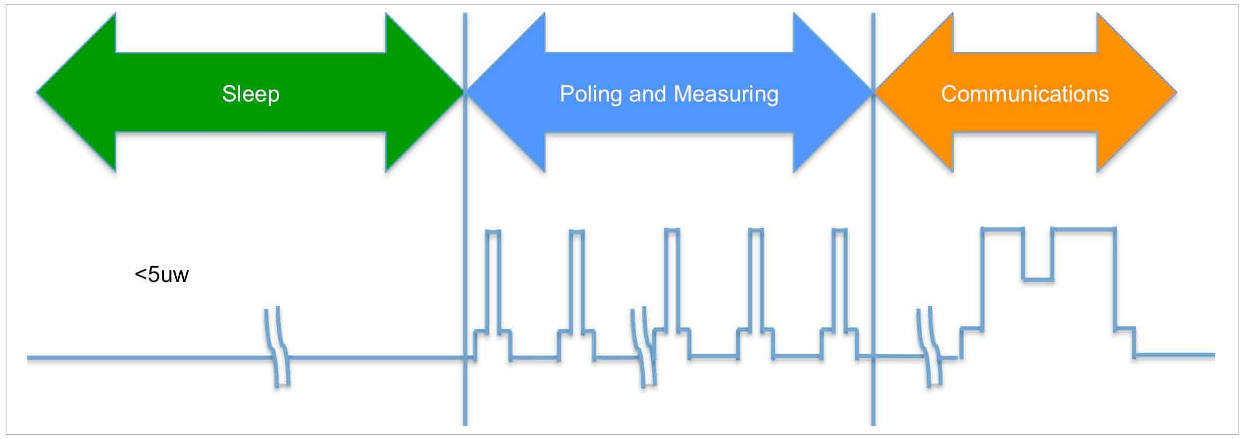


Figure 2: Wireless sensor power profile

Wireless sensors

Wireless sensors are often placed in environments that are difficult or expensive to access. This drives the energy supply to be something that either lasts for a very long time, more than 10 years, or can be supplied from the environment in a dependable fashion. So power management must be very frugal with energy consumption it uses to manage the energy. Wireless sensors also have a very high peak-to-average power ratio, in some cases greater than 100.

Figure 2 shows an example of various power modes for a wireless sensor. In this example, the sensor sleeps most of the time but may wake up on communication to take a measurement, which also serves to let the system know the sensor is available. At a much longer interval the sensor may provide much more information to the system. This transmission may require much more energy, so there is a dependency on the available stored energy. The power management solution must be able to supply the needed peak power while consuming very little of the average energy. Any of these systems where the environmental energy is low, the power management solution must collect the energy until there is sufficient energy for the required utility.

Figure 3 shows an implementation example of such a system[2]. In this example, maximum power point tracking (MPPT) is implemented based on the ratio of the MPPT voltage to the open circuit voltage of the photovoltaic source. This MPPT implementation minimizes the energy consumed while performing the MPPT function. This example also integrates the energy storage function. Since the life time of the energy storage element is very important, care must be taken not to over-discharge or charge this element. In this example, levels are set for the minimum and maximum storage voltages.

In order to inform the system about the stored energy level, the designer can configure externally the voltage level where this notification, VBAT_OK can be given. A buck regulator is also integrated into the solution to power the system load. This entire system has a typical quiescent current of only 500 nA resulting as high efficiency, even at low current. For example, at 500 mV input and 100 uA charging current, the boost converter efficiency is greater than 70 percent.

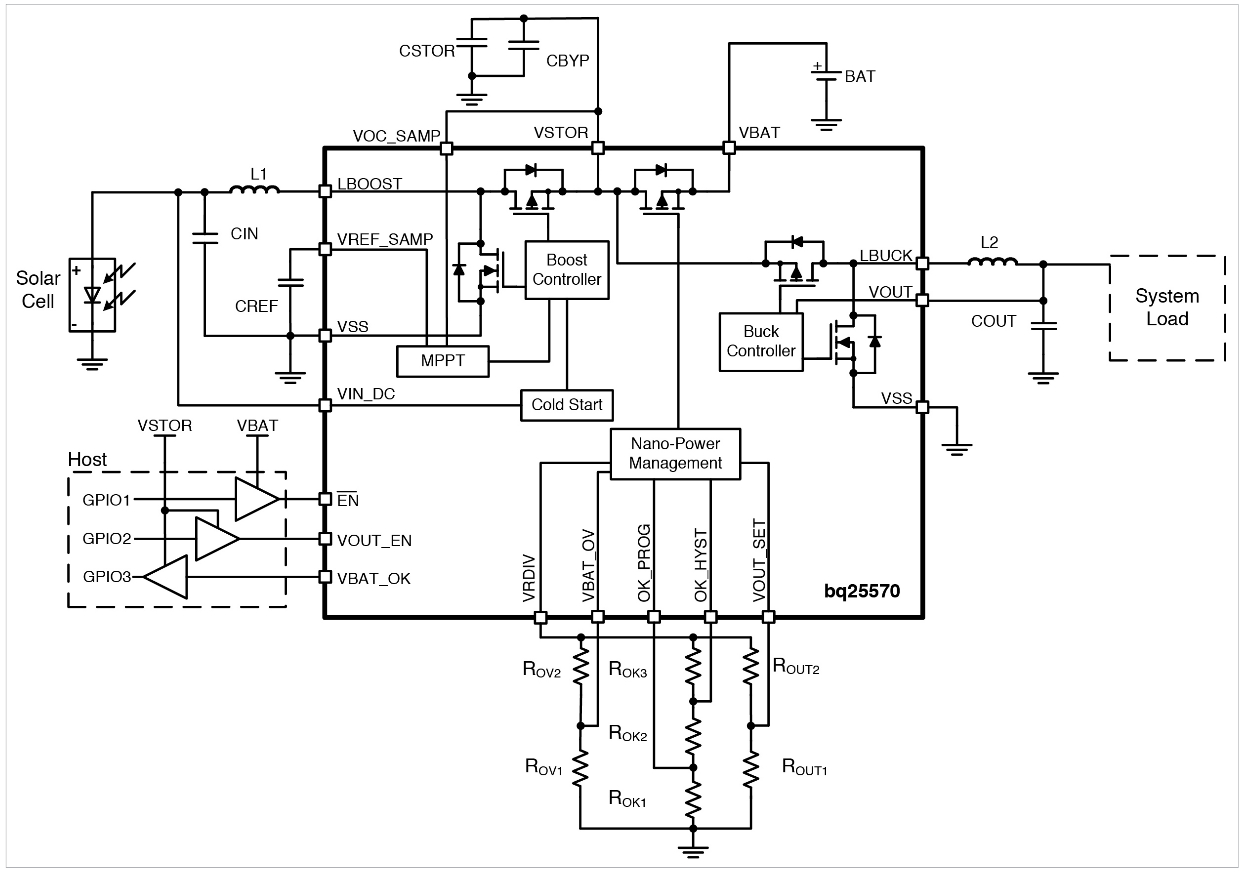


Figure 3: Energy management for a wireless sensor

Smart appliances

Another category of things that form the IoT is appliances. Many times we do not consider how such personal devices are part of the IoT, but it is through the IoT that we can exchange information with our clothes washers, refrigerators, and the like. Traditionally, these devices did not have much to say. You simply plugged them into the grid, set some information, and they did their job. In the example of the clothes washer, it might chime when the cycle is complete, but that was about it. However, today's connected appliances can give you information that does not depend on you hearing a chime. How does this affect the power designer?

These appliances are going from only on when they have a task to perform to being always on, or at least some functions must be always on. These functions must be powered efficiently as they are always on and ready to exchange information. It is this new requirement that adds to the task of the power designer where traditionally they only needed to concern themselves with providing power to perform the task of the appliance.

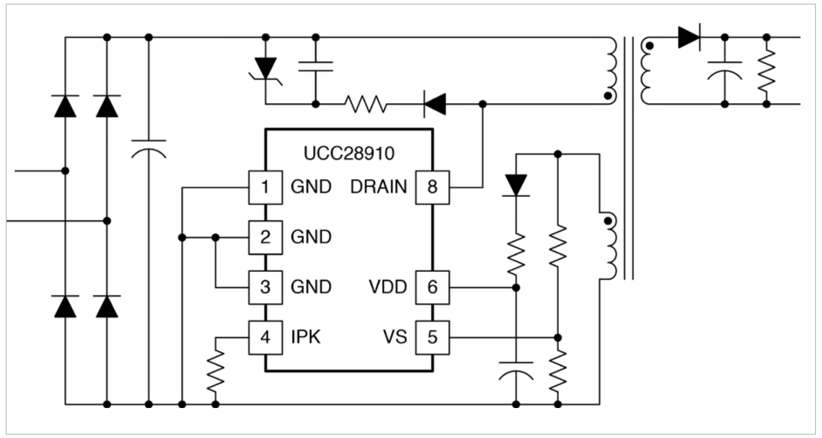


Figure 4: Low power AC/DC for appliance connectivity

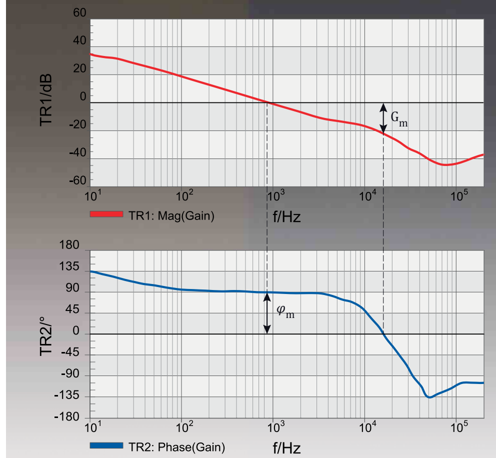
Since these devices require higher power to complete their task, they are tied to the grid in most cases. Therefore, energy harvesting is not required. However, since they are always on, quiescent power and efficiency is important for the new connectivity function. Many times these connectivity functions are performed wirelessly and communicate with a local network. This sets the power level requirements to below 10W. This low-power level is typically satisfied by a AC/DC fly-back solution. There are many integrated fly-back solutions to choose from, but this particular application has its own requirements. **Figure 4** shows an example of such a power solution to satisfy the need for connecting to the IoT.

There are several key features in the **Figure 4** fly-back example. First is that it has very low standby power, less than 30 mW. This is important because connectivity must always we ready, even if the appliance is idle. Another aspect is low electromagnetic interference (EMI) as this device most often will be powering a wireless communication circuit. In this example, the controller uses valley switching and frequency dithering to help with EMI reduction.

Another aspect is size of the power solution. The size itself is typically not the issue, but it is how the size affects the final cost. Although the IoT is an exciting technology and having your washer tell you that your clothes are ready for the drier, or the refrigerator tell you that someone left the door open via a message sent to your cell phone are desirable, the consumer does not want to pay any more than necessary. So the solution needs to minimize the cost of the power solution. One way this can be accomplished is by reducing the size. Size reduction is accomplished by operating at a higher frequency, in this case 115 kHz.

Wireless network

Let's move to what is becoming the big concern for the IoT. As mentioned at the start, it is the wireless network that is the primary energy hog. There is plenty of power design development work in play to help solve this problem. Everything from envelope tracking to digital RF power amplifiers are being researched and developed for the base station, which is certainly more than can be covered here. As many base stations are powered from the grid, there is an opportunity to make that front-end power factor control (PFC) supply more efficient. One such approach is shown in **Figure 5**. This is the power stage



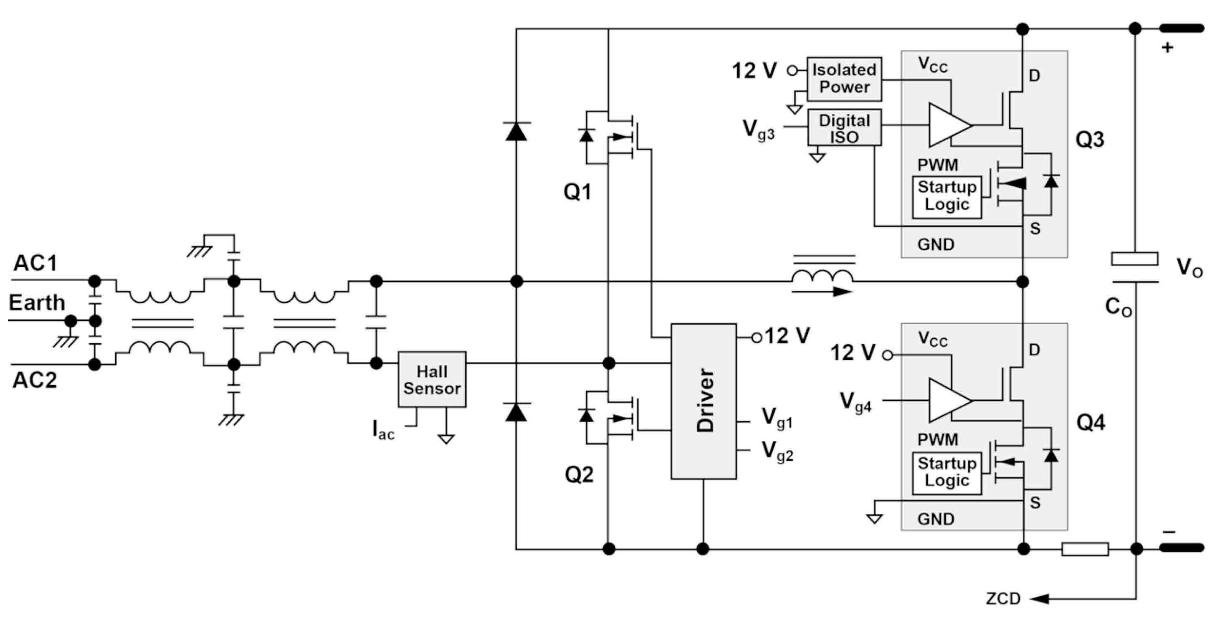


Figure 5: Totem-pole bridgeless PFC

of bridgeless PFC. By removing the diode bridge, the system can be made more efficient. There are many different bridgeless PFC topologies, but we will focus on continuous conduction-mode (CCM) totem-pole version.

The benefits from this topology are reduced component count and removing bridge losses. We can further improve efficiency by taking advantage of Gallium Nitride, GaN, switching devices. These devices, Q3 and Q4, offer lower gate losses allowing higher frequency operation. The other parasitic losses like Coss are also lower. Additionally, there is no intrinsic body diode, so there is minimum reverse recovery loss. Q1 and Q2 are switched at the line frequency and they can be silicon MOSFETs while providing additional loss reduction over diodes alone. There have been several published papers that go into detail about this topology as it will benefit the overall efficiency of high-power grid connected system.

Looking forward

The IoT provides many new challenges for power designers with only a few mentioned here. Adoption and coverage of the IoT depends heavily on reducing the energy demands from harvesting environment energy, to minimizing home energy, and reducing the total network energy requirements. As we develop new technologies for energy harvesting, we must remember that reducing the energy needs will still be important to fuel growth. The lower the energy needs, the more likely it can be supplied from the environment.

Reducing the energy need from the grid is also important. Thinking about each individual grid-powered application may disguise the impact that a few tenths of a percent of efficiency has. It is the total that draws the attention of governments. It's not the one washer or the one base station, but the millions that create the energy need. Luckily power designers have new technology to address these challenges. In some cases it will be process technologies that enable high-voltage components to be integrated with low-voltage control. In other cases it can be the WBG devices that improve high-voltage conversion by allowing low loss at higher switching speeds. Times are definitely getting more exciting for the power designer.

www.ti.com

Using Lord Kelvin's sensing method

The Kelvin Method lives on in the in the latest ultra-precise current-shunt monitors & current-sense amplifiers

By: Srudeep Patil, Maxim Integrated

Ultra-precision, high-side current sensing is crucial in applications where one must measure the current entering or leaving a battery. Today many digital multimeters feature four-lead Kelvin sensing to eliminate the series resistance of the multimeter leads and give an accurate voltage drop across a given resistor.

Similarly, a current-shunt monitor (CSM) or current-sense amplifier (CSA) measures voltage drop across a shunt resistor based on the current flown into or out of the battery. This is how you determine the amount of current drawn by the load from a battery in real-world applications. Systems today use low power and require a very accurate measure of charge left in the battery. To quantify remaining charge, every µA drawn from the battery by the load or pumped into the battery by a charger needs to be accounted for. Thus, ultra-precise sensing of voltage drop across the shunt is critical.

Let's look at measuring voltage drop across a shunt resistor with very high precision. An ultra-high-precision CSM measures the voltage drop across the shunt resistor with typical connections, and then compares this value with the CSM accuracy specification in its datasheet. There are ways to improve the measurement accuracy using that same CSM.

These measurements are enhanced utilizing the proven Kelvin sensing methods with a four-terminal sense resistor. Test results also show that one should be careful with the board layout. Once the layout practices listed in this article are followed, we can capitalize on Kelvin sensing and sense the microvolt level drop across the sense resistor with ultra-high precision.

The Kelvin Bridge

Before we talk about ultra-precision CSMs/CSAs, let's start with a look back in time to an impressive scientist and Avant-garde engineer, Lord Kelvin (see **Figure 1**). Lord Kelvin's pioneering effort is the basis of many electronic principles that we take for granted in our daily life, such as knowing when our cell phone needs charging.

Figure 1: A portrait of Lord Kelvin (1824-1907) by Sir Hubert von Herkomer (1849-1914)

Kelvin's work in measuring very low resistances is still used in modern integrated circuits (ICs). In fact, when you accurately measure battery capacity by applying early Kelvin principles and additional math, preventing overcharging or discharging extends battery life.

Early instruments such as the Kelvin bridge (see **Figure 2**) are amazingly accurate by today's standards. Note the block diagram in the center of **Figure 2**. On the left is a battery and below are four leads. The outer leads

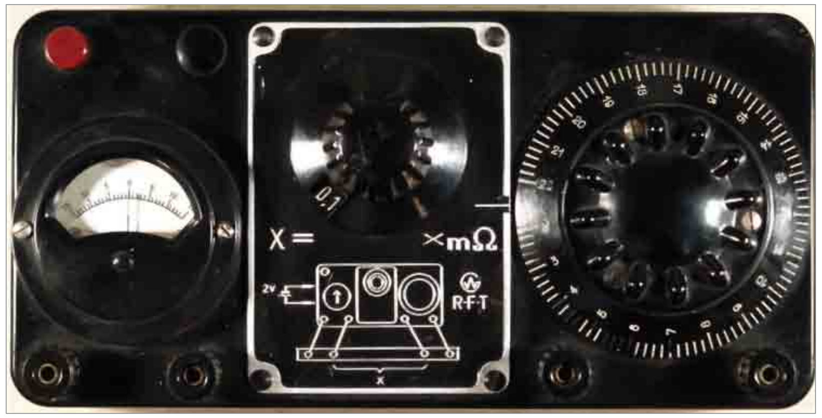


Figure 2: An early Kelvin bridge for making accurate resistance measurements of very low-ohm resistors

supply current through resistor X, while the inner leads isolate the measuring circuit. It is easier to see the Kelvin sensing principle in **Figure 3**.

By separating the main current path from the measurement path, Kelvin improves measurement accuracy. In **Figure 3**, the main current to be measured flows from the battery on the top left through the ammeter (A), and the voltage drops across resistor "X" (the gray bar at the bottom) between leads 2 and 3. Virtually no current flows through the voltmeter circuit (V and leads 2 and 3) due to very high-input impedance and, hence, the voltmeter makes a highly accurate measurement. The current is the same at all parts of the main circuit comprised of the ammeter, battery resistor, and leads 1 through 4. However, the leads 1 and 4 contribute series resistance that, in turn, contributes to a finite amount of voltage drop along the leads. Although very small voltage drops, nonetheless, they reduce accuracy.

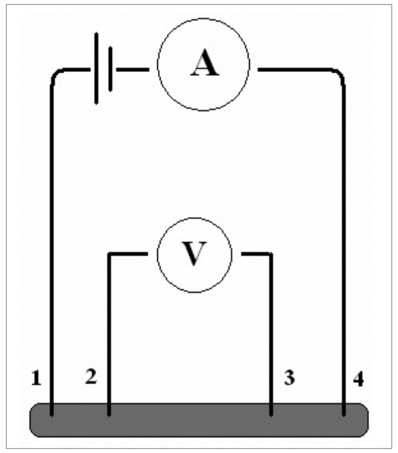


Figure 3: A block diagram showing the Kelvin sensing method.

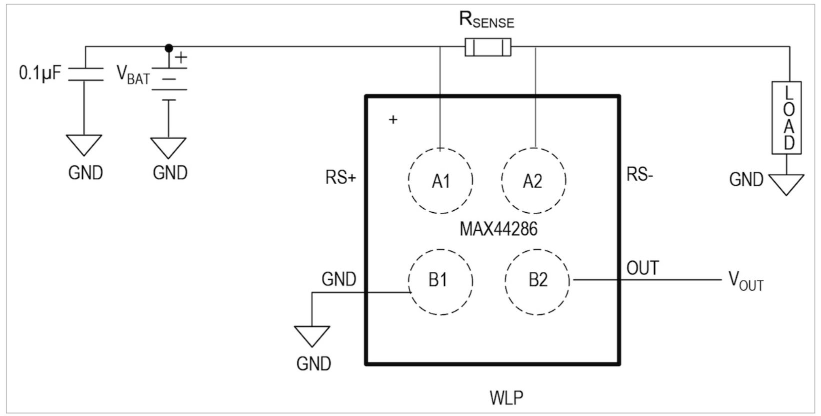


Figure 4: Typical connections to measure drop across a sense resistor. The example device serving as the shunt monitor is the MAX44286 CSA

By separating the main current path from the measurement path, Kelvin's sensing improves the accuracy of measurements. Of course, knowing any two of the three parameters—voltage, current, and resistance—we can calculate the third parameter.

Typical connections on a current-shunt monitor

Figure 4 shows connections around a CSM used for monitoring current from the battery into the load. We might think at the outset that there is nothing wrong with **Figure 4**. However, this design will not yield the ±0.23% gain error specified for this CSA. The design problems actually result from shortcomings in the board layout and poor schematic placement.

When we examine the schematic placement in **Figure 4** and make some adjustments, we can preserve the shunt monitor's DC accuracy parameters like gain accuracy and input-offset voltage. The example shunt monitor shown here is the MAX44286 available in a 4-bump wafer-level package (WLP) with 0.78mm x 0.78mm x 0.35mm dimensions. These findings and recommendations will apply similarly to any precision CSA. Although our analysis here is done with the MAX44286, the results are true and should hold good for any high-precision CSMs.

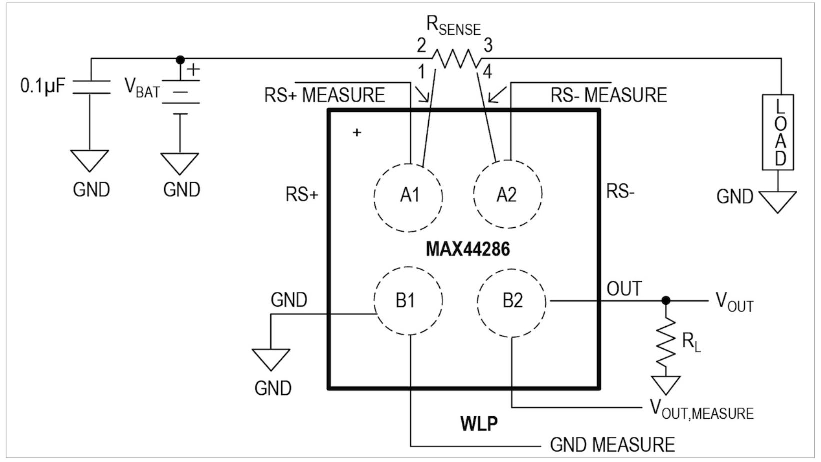


Figure 5: Circuit shows Kelvin connections on both inputs, output, and ground bump. Once again the MAX44286 is the example CSA acting as the shunt monitor

We begin the analysis of Figure 4 with a well-known axiom:

$$V_{OUT} = \text{Gain} \times V_{DIFF}$$

Where:

- V_{OUT} is the amplifier's output on bump B2 in volts.
- V_{DIFF} is input differential sense voltage in millivolts due to the current flow through shunt resistor RSENSE placed across the inputs.
- Gain is inherent to the amplifier based on the gain option chosen (for example, 25V/V, 50V/V, 100V/V, 200V/V).

Gain accuracy or gain error is a critical parameter in precision applications where highly accurate sensing is needed on µV-to-mV level drops across a sense resistor. Therefore:

Gain Error (GE) = [(GainMEAS – Gain IDEAL) × 100]/GainIDEAL

Where:

- Gain error is the percentage deviation between the observed differential gain and the ideal differential gain expected of the CSM.
- GainMEAS is the gain achieved in V/V.
- GainIDEAL is the gain that the device is rated to provide in V/V.

Below are the results for the MAX44286 on bench tests for the setup in Figure 4. To read the most accurate measurement of voltage drop, we calculate gain error by a two-point differential voltage covering both extremes of the full-scale differential sense range. Our test conditions were VBAT =5.5V with GIDEAL = 50V/V version at room temperature.

Specifically:

- V_{DIFF} = 60mV, 4mV as two points
- V_{OUT} with respect to GND = 2.99264V, 0.1992298V, respectively
- GMEAS = VOUT/VDIFF

So, calculating gain error per Equation 2 yields:

Gain Error (GE) = -0.23713148%

Now this result is not what we expect from this CSM, as its maximum gain error spec is ±0.23%.

Another important specification in these ultra-precision sense amplifiers is input offset voltage, given by:

$$V_{OS} = (V_{OUT} - V_{DIFF} \times G_{MEAS})/G_{MEAS}$$

Where:

V_{OS} is the CSM's input-offset voltage specified in microvolts due to mismatch in the input pair. From Equation 3 and our test results, we achieve:

V_{OS} = -5.93281µV

Gain Accuracy and input V_{OS} of CSA improve with a Kelvin sensing layout

There is a way to achieve gain error that is always less than ±0.2%, and better input-offset voltage. Examine **Figure 5** and notice that there are a few more traces than in **Figure 4.**

Traces from the sense-resistor terminals to the amplifier inputs carry input bias current. Supply current to the amplifier is part of the input bias current drawn through the RS+ pin because there is no dedicated supply voltage pin on the MAX44286. Otherwise, the input bias current flows through the RS+ and RS- pins and the supply current flows through the V_{CC} pin, if there is a dedicated supply pin. Also, this current through the RS+ bump increases as the input differential voltage increases.

Trace impedance will create a drop due to this current flow through the trace. The result will be extra gain error if the input sense voltage is calculated across the sense resistor, since we did not account for loss along the trace. These extra traces at the input bumps, RS+ MEASURE and RS- MEASURE, will have no effect on the input sense voltage when it is measured across them.

Note also that the extra GND MEASURE trace is isolated from the currents flowing to the board's ground and is solely used as a ground reference for accurate output voltage measurement. Another trace coming from the OUT bump, V_{OUT},MEASURE, is isolated from the actual output trace carrying the load current when the load resistor sources or sinks current out of the amplifier. This isolation lets us accurately measure the output voltage at the OUT bump with respect to the GND MEASURE trace. From all this we can calculate the gain error and input VOS of the CSA very precisely.

If you notice, there is a four-terminal resistor used in **Figure 5**. The 4-lead Kelvin configuration enables current to be applied through two opposite terminals; a sensing voltage is measured across the other two terminals. This design eliminates the resistance and temperature coefficient of the terminals for a more accurate current measurement. Also, traces from the sense-resistor terminals are taken directly underneath the pads of the resistor, thus preventing any additional trace impedance on the sense resistor.

The results below were achieved on the bench with the setup shown on **Figure 5**.Gain error is calculated similarly where a two-point differential voltage covering both extremes is applied to the shunt monitor and the output voltages recorded. Our test conditions were the same as earlier, V_{BAT} =5.5V with GIDEAL = 50V/V for the CSA at room temperature. Therefore, V_{DIFF} = 60mV, 4mV as two extremes.

Now V_{DIFF} is the input differential voltage measured between RS+ MEASURE and RS- MEASURE. Also the V_{OUT},MEASURE values, with respect to the GND MEASURE for 60mV and 4mV input sense voltages applied, are 3.013034V and 0.2141941V respectively.

Thus:
$G_{MEAS} = V_{OUT}/V_{DIFF}$

So, calculating gain error from Equation 2 yields:
Gain error = -0.08518056%
Substituting V_{OUT},MEASURE calculated with respect to GND MEASURE and substituting yields:
VOS = 3.54415μV
We can clearly see that there is an appreciable change in the gain error and input VOS. Thus, preserving the ultra-precise measurements of a CSA depends on the layout and component placement on the test fixture. If we use the sensing traces to measure as shown in Figure 5, measurements are very accurate. In ultra-precision applications, sense voltages on the order of microvolt are very important for sensing current on the order of microamps. Clearly, each trace must be laid out with great care.

Traces from each sense-resistor terminal to the respective input bumps need to be symmetrical in shape and length. Having a 2-terminal sense resistor will also provide good gain accuracy readings within a maximum of ±0.23% over temperature. For more accurate results over temperature, use 4-terminal sense resistor.

Thus, we complement Lord Kelvin's sensing principles by preserving the DC accuracy of an ultra-precision CSA. Precision measurements not only depend on the good design and layout of the CSA itself, but on the board layout as well.

www.maximintegrated.com

Enterprise labeling: an industry imperative (Part I)

The ever-increasing volume of duplicated label and redundant master data begs the question of information effectiveness

By: Joe Longo, Loftware

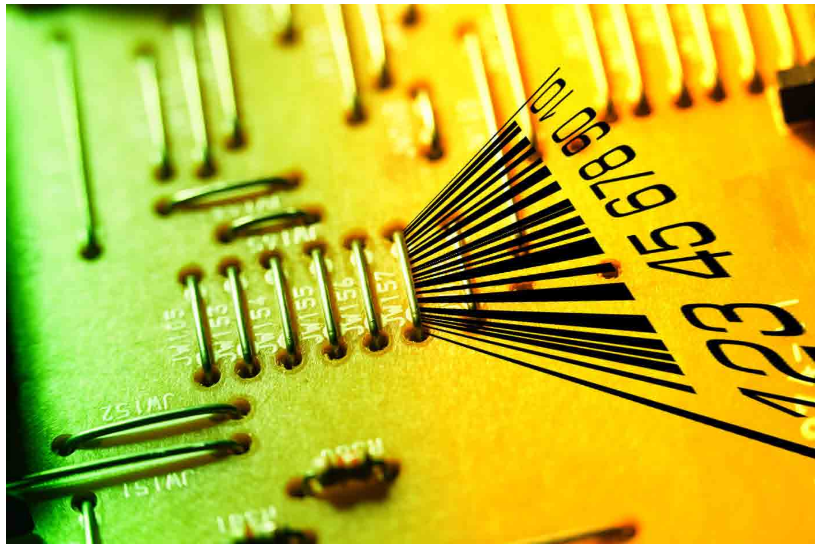


Figure 1: Proper product labeling and data standards can lead to supply chain transparency

The electronics industry today is characterized by an ever-sprawling set of global supply chains, causing an increase in disparate labeling systems spread across the enterprise with an ever increasing volume of duplicated label and redundant master data. This begs the question: how effective is labeling in the electronics industry today? Can labeling be more optimized for large corporations with thousands of printers around the world?

The challenges facing organizations dealing with global supply chains include the need to accomplish the following:

- Increase supply chain transparency for speedy product development
- Centralize and consolidate label printing from one location to thousands of remote printers worldwide
- Integrate labeling with business applications
- Reduce the number of label templates with automation
- Rapidly change labels as customer, geographical and regulatory requirements evolve
- Build "configure to order" solutions in high volumes
- Attain higher yields through fewer defects in labels
- Defend against higher costs by safeguarding against counterfeiting
- Reduce manufacturing costs and sustain or improve margins

That's more easily said than done. Why? Because among other things, and most obviously, the success of a collaborative and coordinated global supply chain depends upon operating reliably across borders, over distances, in many languages—and all must be in sync with different time zones in compliance with a variety of different local, regional, and national regulatory requirements.

This discussion is targeted toward electronics industry supply chain and logistics professionals tasked with optimizing their company's partnerships to get more done, in more places, in less time, for the achievement of greater profitability and market share. It speaks to the many components that contribute to partnership optimization and solutions at hand through product labeling and data standards that can lead to supply chain transparency (see **Figure 1**).

The basic concept is simple: if all stakeholders in the supply chain can speak the same language, figuratively speaking, then raw materials and finished products can come and go faster, more reliably, with less waste, and with fewer errors. All this can occur at lower costs for higher margin outcomes, increased customer responsiveness, and strong competitive advantage.

There's no such thing as "Business as Usual" in the electronics industry

Because the electronics industry continues to innovate, the task of meeting the new objective of supply chain transparency and integration is not merely a matter of engaging in the same, business-as-usual approach to raw materials sourcing, manufacturing, assembly, and shipment processes for a simplistic adaptation to a new supply chain model.

For example, the adaptation has to happen in parallel with new trends in unit-level traceability by involving increasingly smaller components that defy conventional labeling processes. Adaptation has to occur while demands increase for faster line changeovers, faster component and assembly verification, and inspection. It all has to happen at a time when many electronics manufacturers are looking to emerging countries with fertile opportunities for low cost manufacturing potential through new or acquired facilities.

Against this backdrop, data and product marketing standards initiatives in the electronic industry cannot expect to gain traction until ongoing trends and developments can be supported. Better-known issues with a long-standing history of adding complexity to the industry need to be solved. In other words, the electronics industry doesn't just need something different, or something new, unless the solution takes away the burden of current processes and simultaneously delivers the opportunity to leverage the industry to the next level.

Common practices with uncommonly burdensome, costly, risky, and wasteful limitations

If the common systems for product labeling were working flawlessly, there would be no demand for change. But even just a cursory review of all that electronics manufacturers must accomplish in labeling generates a profile of an approach that is unsustainable. Consider, for example, what manufacturers need to do simply to comply with their customers' labeling requirements as the industry continues to grow and expand product lines.

Customer labeling requirements often dictate the exact type and placement to be used on the product, box, carton, and pallet. It is not unusual for a major customer to demand exact specifications for label size, data titles, data field identifiers, as well as a dozen or more exacting guidelines for barcode symbologies. For example, one leading electronics buyer provides this guidance: "Barcodes should be within a character density range of 3.7 to 6.9 characters per inch, with a minimum element ration of 2.5:1 to 3.0:1…preferred." And every major customer's labeling directives can be different.

Customers today also want the manufacturers to exhibit faster, more reliable, more secure turnaround for the use of new label designs that evolve as products change. This comes at a time when products are changing faster than ever. The industry is already coping with possibly the largest number of serial numbers and labeling configurations of any industry in the world.

Failure to meet customer labeling requirements, especially across multiple customers with differing standards, leads to shipping errors, higher freight costs, returns, repackaging expenses, late penalties, compliance issues—and worse—customer dissatisfaction. For an industry already undergoing increased pressure on prices and margins, these outcomes negatively exacerbate corporate growth and profitability objectives.

Satisfying customers while taking unsatisfactory delivery of unidentifiable materials

The above example is about outgoing finished product. But electronics manufacturers have a labeling challenge with incoming raw materials—and an opportunity. At the same time, the electronics manufacturer's business sustainability depends on meeting customer labeling guidelines.

In many cases, the manufacturer is taking delivery of raw materials or components with labels that bear no compatibility or consistency with their labeling system. This means it takes time to determine what exactly has been delivered and from which provider. It means these materials or components have to be re-labeled or over-labeled with product label substitutes aligned with the manufacturer's system. This takes time, and contributes to added expense.

The contemporary objective is to have raw materials providers label their products in ways that are consistent and compatible with the manufacturer's operations and labeling methodology. Unfortunately, "homegrown" patchwork systems and solutions that are not enterprise-driven, and do not provide integration capabilities with secure access to a provider of raw materials or components, cannot easily meet this objective, if at all.

Why efficient enterprise labeling is the solution

Once considered a mere tactical necessity, contemporary electronics industry product labeling solutions can have major strategic implications. There are at least eight major negative corporate outcomes that can result from product labeling errors and inefficiencies. Averting these issues is no longer a matter of fixing one label at a time or refitting one product facility at a time with silo or purpose-driven systems. Labeling has become a core component of a manufacturer's strategic mission to create a smoothly operating global supply chain. The solution cannot be found in a patchwork of more systems, but in less and fewer disparities and incompatibilities. For a truly successful outcome, labeling must be integrated with core enterprise applications and data. To find out more about these major challenges and regulations impacting the Electronics Industry, stay tuned for Part II of this article, "Reliance on Compliance: Evolving Electronics Industry Standards."

www.loftware.com

Advanced passenger aircraft drive component innovation

Many aircraft improvements will drive increased use of electrical technologies

By: Julian Thomas, TT Electronics Power & Hybrid

Civil aircraft that are quieter and more economical promise to deliver benefits for everyone; benefits apparent to operators, travellers, and communities on the ground, as well as the environment. Technological advancement holds the key to progress, manifested in collaborative initiatives such as Europe's Clean Sky joint undertaking. Improvements being considered include not only new materials and aerodynamics, but also changes that will drive increased use of electrical technologies in the aircraft of the future.

Fly-by-wire

Some of today's most modern aircraft are already implementing advances such as the "bleedless" architecture that replaces traditional engine-driven pneumatic systems like wing ice protection and cabin air conditioning with more lightweight and efficient electrically driven alternatives. In addition to improving fuel economy, this architecture also helps reduce noise and drag to weight ratio (see **Figure 1**).

Figure 1: "Bleedless" architecture replaces traditional engine-driven pneumatic systems

The trend towards electrification places extra demands on the design of the aircraft's electrical architecture and systems. More electrical power is required, which demands a new approach to the entire electrical design. One example can be seen in the use of multiple remote power distribution units, which help minimize the overall weight of the electrical infrastructure.

New electrical subsystems must be designed to operate safely and reliably in the harsh aircraft environment. As well as wide ranging extremes of temperature – from as low as -60°C to over 200°C and rising to over 300°C in the future as equipment is located closer to the engines – other hazards include high levels of vibration and a risk from lightning strike.

Silicon Carbide to the rescue

Fast-acting Solid-State Power Controllers (SSPCs) improve protection against surges caused by ESD events such as lighting strike, by replacing slower-acting mechanical circuit breakers. SSPCs have response times in the order of nanoseconds, compared to the typical 100μs actuation time of a conventional circuit breaker, and are now feasible for aircraft applications thanks to new silicon carbide (SiC) technology.

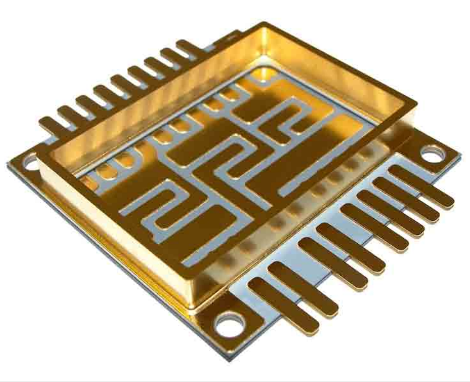


Figure 2: TT Electronics has a number of active SiC development programs focusing on high-reliability assembly and including packaging for ±270V SSPCs

SiC devices in ratings high enough to divert short, high-energy transients away from sensitive electronic circuitry are significantly smaller than conventional silicon devices, and subsequently enable SSPCs to become smaller and lighter than mechanical circuit breakers. TT Electronics has a number of active SiC development programs focusing on high-reliability assembly and including packaging for ±270V SSPCs, and is also working with SiC device manufacturers using the latest fabrication technologies to drive improvements in thermal characteristics and thus increase system performance and reliability (see **Figure 2**).

Where electronic modules are deployed in the harshest environments, such as within close proximity to the engine, extremely high peak temperatures can promote unwanted chemical interactions between materials used in the assembly or with gases in the immediate environment, in addition to melting conventional solder-based interconnects and exacerbating known issues such as differential thermal expansion. Solving these challenges can require extensive research in order to identify combinations of materials that will coexist benignly, and develop suitable assembly processes. TT Electronics, for example, has developed robust processes for silver sintering as a replacement for conventional solder-based die attach.

Reliability is key

In general, greater reliability is the over-riding target of today's advanced design projects, as typical commercial aircraft become increasingly dependent on electrical systems to perform important functions. Even where systems are not directly exposed to extremely high temperatures, improving thermal characteristics helps to enhance reliability. TT Electronics and its partners are pushing forward in a number of other areas to deliver the improvements needed.

TT Electronics has developed a process to enhance power-module reliability by helping maintain co-planarity and robustness of the interface between the baseplate and substrate where ensuring correct alignment has always been a challenge. Innovation by our engineering teams now allows this technique to be used in aerospace applications, achieving high quality, high production yield and extending life. Increasing the energy efficiency of high-power modules, through advanced device and circuit design, also helps improve thermal performance and hence reliability, by minimizing internal power losses and dissipation.

With increasing electrification, the importance of in-house environmental testing, such as accelerated life tests and environmental stress tests, is growing. The data gathered provides vital process validation and information that can be used to direct future research and thereby help to reduce time to market.

The drive for more efficient and environmentally friendly aircraft is opening exciting new frontiers in the design of high-reliability electronic devices and systems for aerospace applications. Current progress suggests everyone can look forward to safer, quieter and more economical air travel.

www.ttelectronics.com

Conquering harsh environments

Low power, precision, high-temperature components address extreme applications

By: Jeff Watson and Maithil Pachchigar, Analog Devices

When we think of harsh environments, there is no doubt that one of the most challenging applications on this planet is downhole drilling. Oil field service companies are pushing the limits of technology to design precision equipment that must survive extreme pressure, shock, and vibration, while at the same time have a long battery life and fit in very small form factors.

Perhaps the biggest challenge for electronics used in this environment is the extreme temperature. These high temperatures are a function of depth; while on average the geothermal gradient is about 25°C/km, in some regions it can be higher. Due to increasing global energy demands, there is motivation to drill and develop these hotter wells where it has not been feasible to do so before. Unfortunately, cooling the electronics in this environment is not an option.

Because of this, the industry is calling for precision instrumentation that must operate reliably above 200°C. Indeed, the importance of reliability is underscored by the high cost of a failure. An electronics assembly on a drill string operating miles underground can take more than a day to retrieve and replace—and the rate for operating a complex deepwater offshore rig can be more than $500k per day.

In addition to oil and gas exploration, there are other emerging applications for high temperature electronics. The aviation industry has a growing movement toward the “more electric aircraft.” Part of this initiative seeks to replace traditional centralized engine controllers with distributed control systems, which places the engine controls closer to the engine, greatly reducing the complexity of the interconnections and saving hundreds of pounds of aircraft weight.

Another aspect of the initiative is to replace hydraulic systems with power electronics and electronic controls to improve reliability and reduce maintenance costs. The control electronics ideally need to be very close to the actuators, which again produce a high ambient temperature environment. Similar to avionics jet engines, control systems and instrumentation are required for heavy industrial gas turbines used for power generation.

High temperature rated ICs

In the past, high temperature electronics designers were forced to use components above their rated specification due to the unavailability of high temperature ICs. While some standard temperature ICs may have limited functionality above specification, it is an arduous and risky endeavor and there is no guarantee of reliability or performance.

For example, engineers must identify potential candidates, completely test and characterize performance over temperature, and qualify the reliability of the part over a long period of time. Performance and lifetime of the part are often substantially derated and could vary substantially between manufacturing lots. This is a challenging, expensive, and time consuming process that designers would prefer to avoid. Additionally, target design temperatures are transitioning to 175°C and higher advanced packaging is necessary to enable reliability even for short durations of time.

Fortunately, advances in recent years have led to high temperature rated ICs being available off the shelf. Products in the Analog Devices high temperature portfolio use specialized process technology, circuit design, and packaging along with a comprehensive characterization, qualification, and production test program to enable reliable performance at high temperature with guaranteed data sheet specifications.

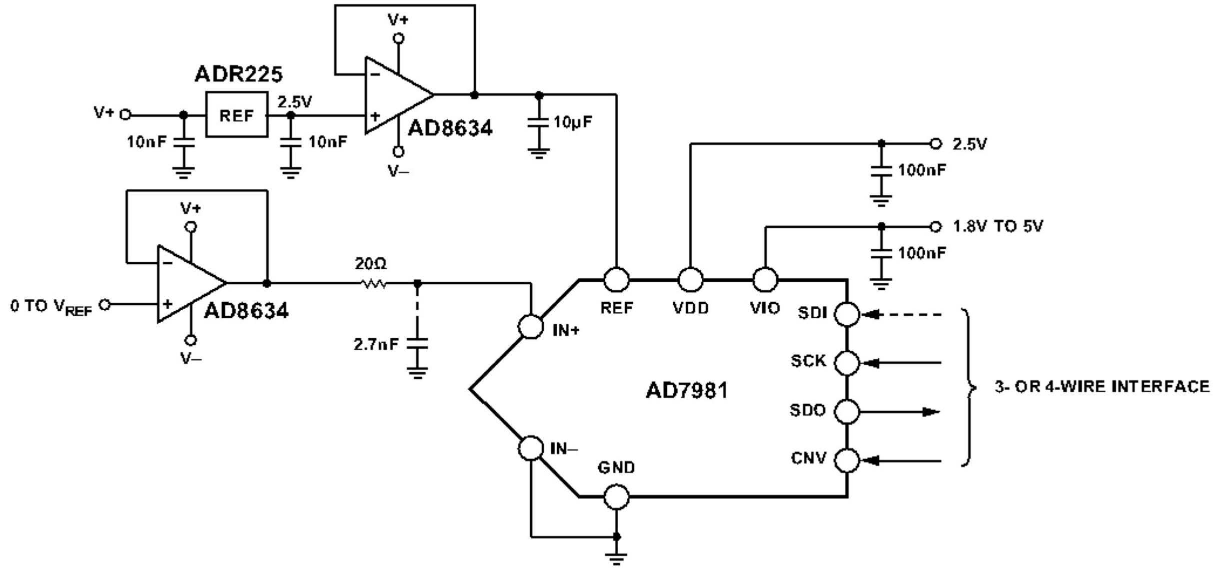


Figure 1: AD7981 Application Signal Chain

High temperature signal chain

While we have presented some varying end applications for high temperature electronics, from oil exploration to avionics to heavy industrial fields, there are several common requirements in their signal chains. The majority of these systems require precision data acquisition from multiple sensors or require high throughput rates. Furthermore, many of these applications have stringent power budgets because they are running from batteries or cannot tolerate additional temperature increases from the self heating of the electronics. Therefore, a low power data acquisition signal chain is required, consisting of sensors, precision analog components, and a high throughput ADC.

Even though there are now commercially available HT rated ICs, there is still a limited selection of circuit building blocks today. In particular, there are no commercially available precision ADCs that are low power, have a sample rate higher than 100 kSPS, and are rated for operation above 200°C. This is a major pain point for circuit designers who need to acquire and process wider bandwidth signals or want to multiplex channels. To meet this need, ADI has recently released the AD7981 ADC, capable of samples rates up to 600 kSPS with 16-bit resolution while maintaining low power and a very small footprint. It is available today in a 10-lead MSOP package rated for 175°C, with a 210°C rated ceramic flatpack, and known good die versions are to follow soon. As a case study we will examine in further detail the features of this ADC that enable its breakthrough performance and reliability at extreme temperatures.

AD7981 high temperature ADC

The AD7981 is a 16-bit, low power, single-supply ADC that uses a successive approximation architecture (SAR) capable of sampling up to 600 kSPS. It is based on ADI’s proven SAR core that has been designed into a high volume of industrial and instrumentation systems. The architecture is based on ADI’s proprietary charge redistribution capacitive DAC technology. The CMOS fabrication process enables excellent performance at elevated temperature partly due to the matching and tracking of these capacitors over temperature. In addition, optimizations were made to the acquisition circuit to improve precision at high temperature.

The AD7981’s typical application signal chain is shown in **Figure**

1, where the high temperature qualified rail-to-rail output, precision, low power, dual amplifier AD8634 is used for driving the input of the AD7981 and as a reference buffer in conjunction with the high temperature qualified, low temperature drift ADR225 2.5 V reference. The AD7981 requires two supplies: an analog and digital core supply (VDD), and a digital input/output interface supply (VIO) for a direct interface with any logic between 1.8 V and 5 V. The VIO and VDD pins can be tied together to reduce the number of supplies needed.

The AD7981 achieves excellent ac and dc performance with typical ±0.7 LSB INL, –102 dB THD, and 91 dB SNR, enabling a high dynamic range with better accuracy and precision even at a high temperature of 175°C. The AD7981 typical INL vs. code plot is shown in **Figure 2**.

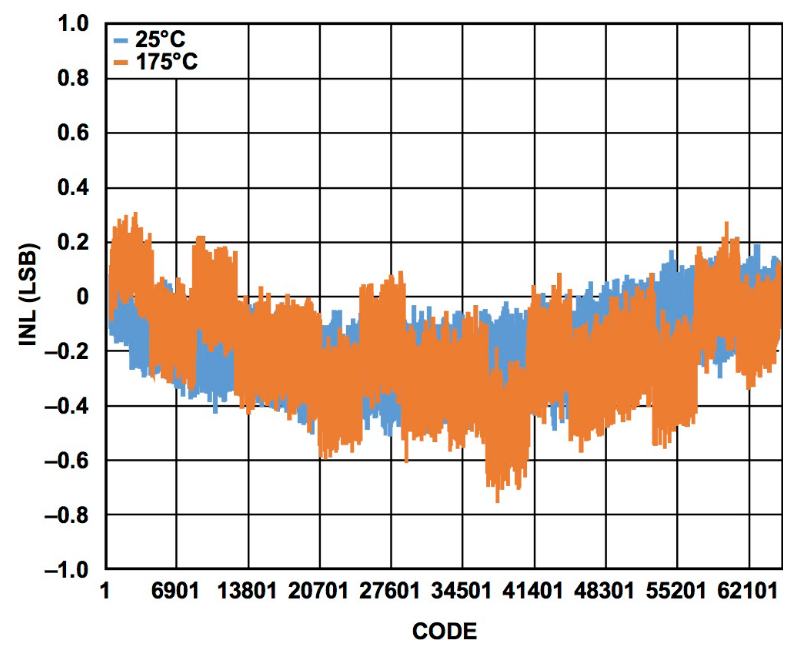


Figure 2: AD7981 Nonlinearity Error vs. Temperature

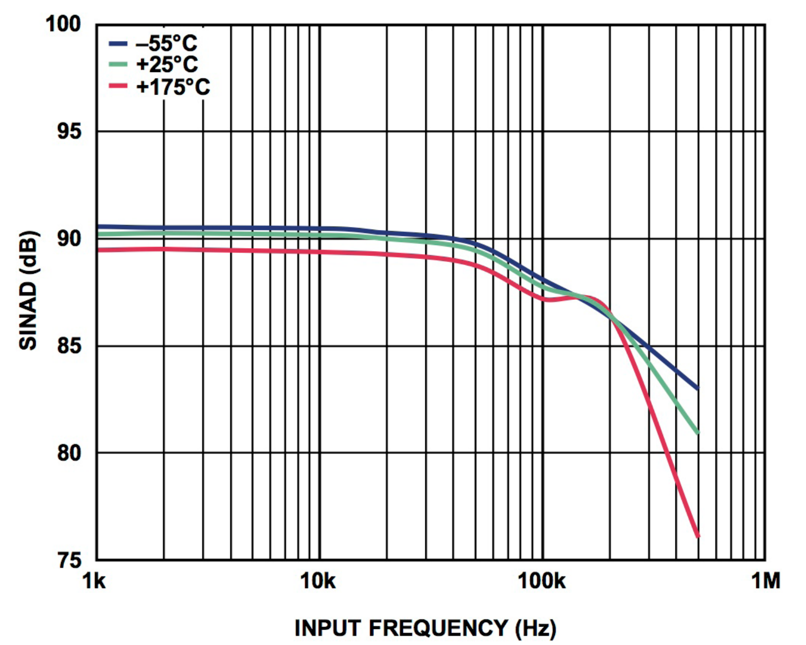


Figure 3: SINAD vs. Frequency Over Temperature

The AD7981 signal-to-noise and distortion (SINAD) performance for a wide input frequency range over various temperatures is shown in **Figure 3**.

The AD7981 maximizes battery life in harsh environments by scaling power linearly with throughput rate, dissipating typically around 4 mW at full throughput of 600 kSPS, and 70 μW at 10 kSPS, as shown in **Figure 4**. The AD7981 powers down automatically between conversions in order to save power. This makes the part dually suited for low sampling rate applications, even of a few Hz, and enables very low power consumption for battery-powered portable systems.

The AD7981 offers a flexible serial digital interface compatible with SPI and other digital hosts. It can be configured for a simple 3-wire mode for the lowest I/O count, or 4-wire mode that allows options for the daisy-chained readback and simultaneous sampling. For multichannel data acquisition systems, the AD7981 can easily be used with a multiplexer because it integrates an on-chip, track-and-hold circuit, and the SAR architecture does not exhibit any pipeline delay or latency.

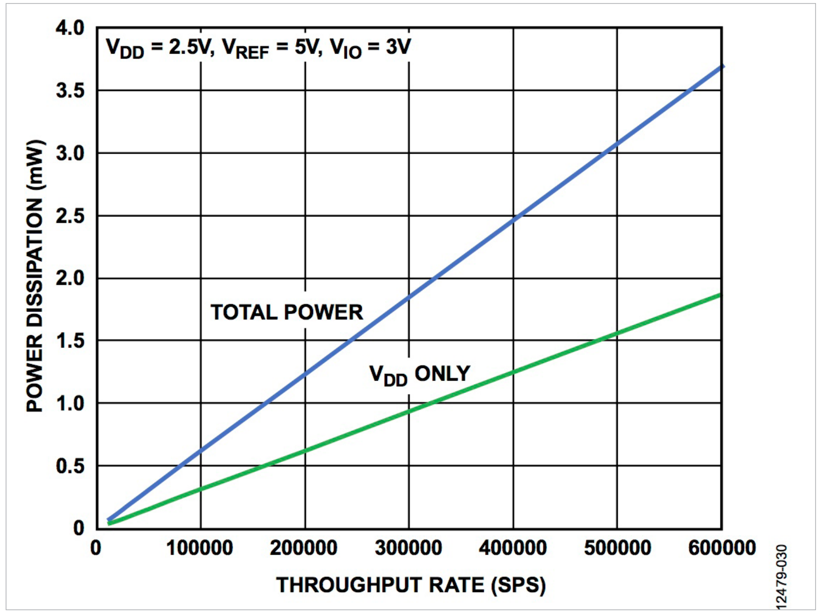


Figure 4: AD7981 Power Dissipation vs. Throughput Rate

High temperature packaging

Once we have high performance silicon that operates at high temperature, only half the battle is won. Robust packaging is critical for integrated circuits that must survive harsh high temperature environments. The package must provide adequate protection from the environment and reliable interconnect to the PCB while having a form factor appropriate for the mission profile of the system.

While there are many considerations to reliable packaging, one of the major failure points at high temperature is the wire bond. This failure has been particularly problematic in plastic packaging commonly found in the industry, where gold bond wires and aluminum bond pads are the standard. Elevated temperature accelerates the growth of AuAl intermetallic compounds. These intermetallics are associated with bond failures such as brittle bonds and voiding, which can happen as quickly as hundreds of hours.

In order to avoid these failures, ADI uses an over pad metallization (OPM) process to create a gold bond pad surface for the gold bond wire to attach. This monometallic system does not form intermetallics and has been proven reliable in our qualification testing with over 6000 hours soak at 195°C. Although ADI has shown reliable bonding at 195°C, the plastic package is rated for operation only up to 175°C due to the glass transition temperature of the molding compound.

Application example

The above combination of the AD7981 key features such as high performance, robustness, low power, and flexible configuration addresses critical performance criteria for precision measurement applications in harsh, high temperature environments, such as downhole oil and gas drilling, as well as industrial, instrumentation, and avionics applications.

The AD7981 is a member of a growing portfolio of high temperature products that enable precision analog signal processing from the sensor up to the processor. The AD7981 is complemented by the ADR225 2.5 V output voltage reference and AD8634/AD8229 amplifiers for signal conditioning. High temperature rated MEMS inertial sensors such as the ADXL206 accelerometer and ADXRS645 gyroscope provide designers with information about the orientation and motion of the system. A simplified signal chain of downhole drilling instrument using these components is shown in **Figure 5**.

In this application, signals from various downhole sensors are sampled in order to collect information about the surrounding geologic formations. These sensors could take the form of electrodes, coils, piezo, or other transducers. Accelerometers, magnetometers, and gyroscopes provide information about the inclination, azimuth, rotation rate, shock, and vibration of the drill

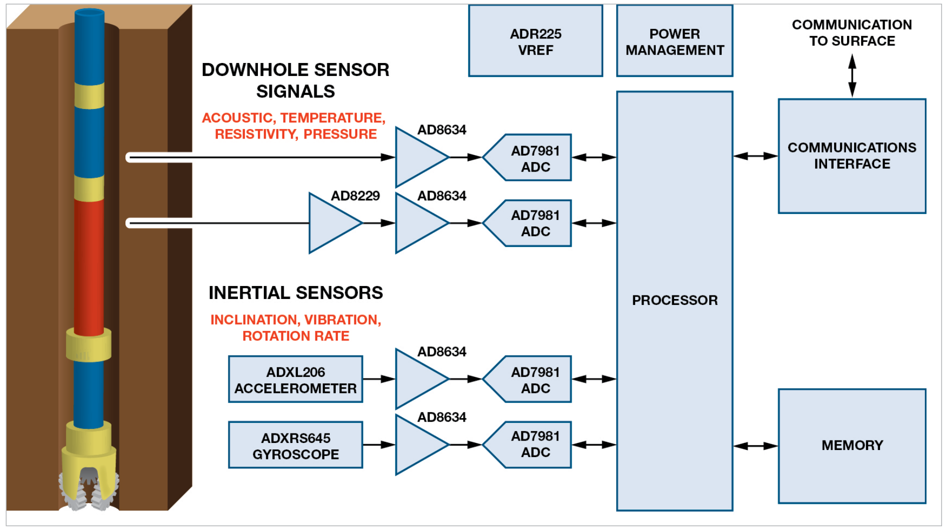


Figure 5: Simplified Signal Chain of Downhole Drilling Instrument

string. Some of these sensors are very low bandwidth, while others could have information in the audio frequency range and higher.

The AD7981 is able to sample data from sensors with varying bandwidth requirements while maintaining power efficiency.

The small footprint makes it easy to include multiple channels even in space constrained layouts, such as the very narrow board widths prevalent in downhole tools. In addition, the flexible digital interface allows for simultaneous sampling in more demanding applications, while also allowing simple daisy-chained readout for low pin count systems.

www.analog.com

Special Report: Internet of Things

PSD EUROPE
Empowering Global Innovation

INSIDE:

Advanced linear charging

Traditional linear-topology battery chargers are often valued for their compact footprints, simplicity, and lower cost

By: Steve Knoth, Linear Technology

Switch-mode battery chargers are popular choices in applications due to their topology flexibility, multi-chemistry charging, high charging efficiencies which minimize heat to enable fast charge times and wide operating voltage ranges. Nevertheless, some downsides of switching chargers include relatively high cost, more complicated inductor-based designs, potential noise generation and larger footprint solutions.

On the other hand, traditional linear-topology battery chargers are often valued for their compact footprints, simplicity and lower cost. Drawbacks of traditional linear chargers have included limited input and battery voltage ranges, higher relative current consumption, excessive power dissipation, limited charge termination algorithms and lower relative efficiency (efficiency ~ $[V_{OUT}/V_{IN}] * 100\%$).

Modern lead acid (LA), wireless power, energy harvesting, solar charging, remote sensor and embedded automotive applications have been traditionally powered by switch-mode chargers for the positive reasons stated above; however an opportunity exists for an ultra-low consumption current, high voltage linear battery charger that negates its usually associated drawbacks.

Cutting-edge apps demand effective linear chargers

Some leading edge application spaces, where innovative, high voltage and ultra-low quiescent current linear chargers can be beneficial include the following:

- Sealed lead acid (SLA) applications with low charge current. Many remote sensor / control applications benefit from the wide temperature range of an SLA battery. These remote applications are usually very low power and don't need to charge quickly, therefore low charge currents can be used – they just need to keep the battery topped off.
- For wireless power, charging is done at very low power levels, typically less than 100mW.
- In energy harvesting applications with any micro-powered source, low quiescent current is essential to avoid competing with the downstream load current demands.
- Solar charging has voltages, both from the panel and the battery, that vary widely. For low power applications a linear charger works well.
- Remote sensors for monitoring or control, typically found in low power industrial applications, have batteries used primarily for backup. As a result, charge time is rarely important and input / battery voltages vary widely depending on the specific application. A low IQ linear charger would charger fits well here.
- Embedded automotive applications have input voltages >30V, with some even higher. For example, consider GPS location systems used as anti-theft deterrents; a linear charger with the typical 12V to 2-in-series Li-Ion (7.4V typical) with added protection to much higher voltages would be valuable for these applications.

A novel linear charger solution

It is clear that a linear topology IC charging solution that solves the applications and associated issues already discussed needs to possess many of the following attributes:

- Low quiescent current - more energy is transferred from weak / intermittent input sources to the battery, reducing power dissipation. Further, low battery IQ also extends the lifetime of the battery when charging has terminated and when an input is not present.
- Wide input voltage range to accommodate a variety of power sources
- Wide battery charge voltage range to address multiple battery stacks
- Ability to charge multiple battery chemistries (Lithium, lead acid, Nickel)
- Simple and autonomous operation with onboard charge termination (no µC needed)
- Input voltage regulation for solar input sources
- Small and low profile solution footprints
- Advanced packaging for improved thermal performance and space efficiency

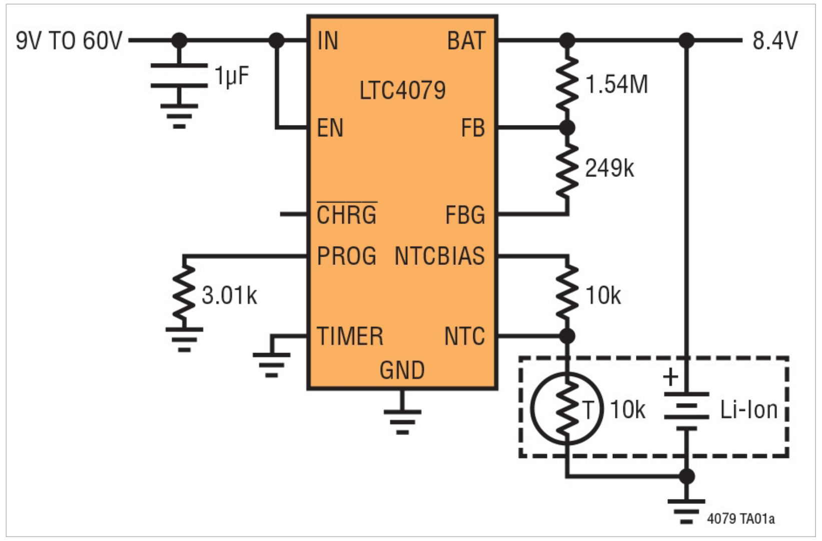


Figure 1: LTC4079 Typical Application Circuit for Charging a 7.4V Li-Ion Battery

For example, Linear's recent LTC4079 linear battery charger has most of these attributes already. The LTC4079 is a 60V, constant-current/constant-voltage 250mA multi-chemistry battery charger with low quiescent current (only 4µA while charging); its linear topology offers a simple inductorless design and accepts a wide 2.7V to 60V input voltage range. A resistor-programmable 1.2V to 60V battery charging voltage range with tight ±0.5% voltage accuracy and onboard adjustable charge termination makes the LTC4079 suitable for many battery chemistries, including Li-Ion/polymer, Li-Iron Phosphate (LiFePO4), Nickel and lead acid.

The charge current is adjustable from 10mA to 250mA via an external resistor and unlike competing chargers the device maintains high accuracy at low charge currents. While 3-stage lead acid charging is possible using a few external components, the relatively low charge current of the LTC4079 makes it more suitable for float charging lead acid batteries. Similarly, no fast charge Nickel termination algorithms are implemented, so Nickel batteries should only be trickled charged with the LTC4079. Applications include embedded automotive and industrial systems, backup battery charging, energy harvesting applications and thin film battery-based products.

The LTC4079's input voltage regulation function can regulate the IN pin to a constant voltage or to a constant differential voltage above the battery. These features can be used to prevent the input voltage of a current limited power source, such as a weak battery or solar panel from collapsing below the undervoltage lockout (UVLO) voltage. The charge current is reduced as the input voltage falls to the programmed threshold. This regulation mechanism allows the charge current to be selected based on the battery requirement, while letting the LTC4079 take care of situations when the input source cannot provide the full programmed

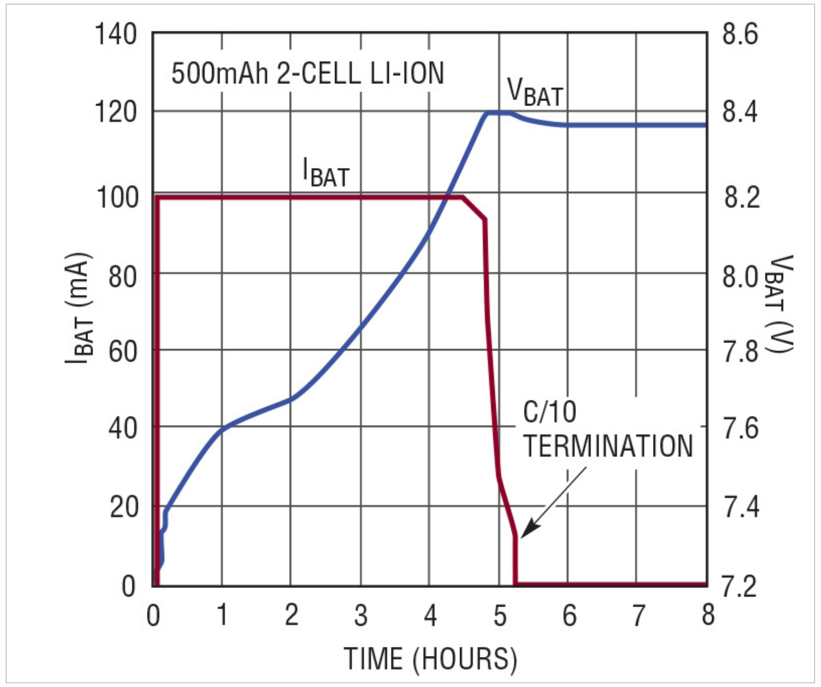


Figure 2: LTC4079 Li-Ion Charge Cycle

charge current (see **Figure 1**).

The LTC4079's thermal regulation feature ensures maximum charge current up to the specified limit without the risk of overheating. Charging can be terminated via C/10 or an onboard adjustable timer. Other features include NTC thermistor temperature-qualified charging, bad battery detection, automatic recharge with sampled feedback in standby for negligible battery drain and an open-drain CHRG pin status output. Once the battery is charged, the battery voltage is sampled via a feedback network every 3 seconds to minimize battery drain, thus prolonging battery run time.

Figure 2 shows the LTC4079's typical full Li-Ion charge cycle, with C/10 charge termination.

The LTC4079 is housed in a low profile (0.75mm) 10-pin 3mm x 3mm DFN package with backside metal pad for excellent thermal performance. The device is guaranteed for operation from –40°C to 125°C. Its key features are:

- Wide Input Voltage Range: 2.7V to 60V
- Adjustable Battery Voltage: 1.2V to 60V
- Adjustable Charge Current: 10mA to 250mA
- Low Quiescent Current While Charging: $I_{IN} = 4\mu A$
- Ultralow Battery Drain When Shutdown or Charged: $I_{BAT} < 0.01\mu A$
- Auto Recharge
- Input Voltage Regulation for High Impedance Sources
- Thermal Regulation Maximizes Output Current without Overheating
- Constant Voltage Feedback with ±0.5% Accuracy
- NTC Thermistor Input for Temperature Qualified Charging
- Adjustable Safety Timer
- Charging Status Indication
- Thermally-Enhanced 10-Lead (3mm x 3mm) DFN Package

Solar charging - input voltage regulation & differential voltage regulation

Solar panel-based charging applications are increasing for many varieties of battery chemistries, but Li-Ion/polymer/phosphate and lead acid are the most popular. The LTC4079's voltage regulation can handle these cases without an issue. The IC can regulate a constant voltage on the IN pin when charging from a current-limited power source such as a weak battery or a solar panel. This feature can be used to prevent the input voltage from collapsing below the UVLO, or to maintain the input source voltage at peak power. The charge current is reduced as the input voltage falls to the threshold set by an external resistor divider from the input power source to the EN pin and GND, as shown in **Figure 3**.

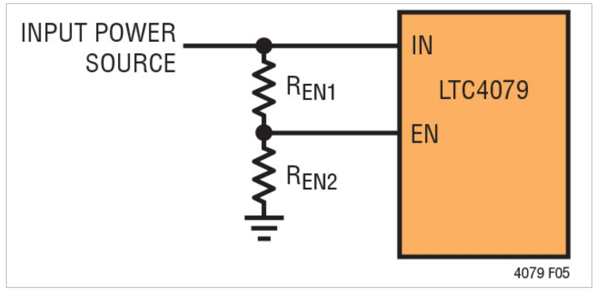


Figure 3: Setting LTC4079's Input Voltage Regulation

The input voltage regulation threshold, $V_{IN(REG)}$ is calculated as follows:

$$V_{IN(REG)} = 1.190V \bullet \left(1 + \frac{R_{EN1}}{R_{EN2}}\right)$$

This regulation mechanism allows the charge current to be selected based on the battery's requirement and the maximum power available from the charging source. The LTC4079 automatically reduces the charge current when the input source cannot provide the programmed charge current.

The LTC4079's Differential Voltage Regulation (V_{IN}-V_{BAT} provides an additional method to keep the input voltage from collapsing when the input power comes from a weak power source. If the input voltage falls close to the battery voltage, the differential voltage regulation loop in LTC4079 keeps the input voltage above the battery voltage by 160mV (typical value) by reducing the charge current as the input voltage to battery differential voltage falls. In both of the above regulation conditions, the input source must provide at least the quiescent current of the device to prevent UVLO. The charge timer is paused whenever the charge current is reduced due to input voltage regulation or differential voltage regulation conditions.

Nickel Charging

The LTC4079's design can also handle Nickel batteries. For nickel-chemistry batteries (e.g. Nickel Cadmium [NiCd] and Nickel metal hydride [NiMH]), the possibility of overcharging must be considered. A typical method is to trickle charge with low currents for a long period of time. Since NiCd and NiMH batteries can absorb a C/300 charge rate indefinitely, shorter duration charging is possible using a timed charge algorithm. It is advisable to charge the battery to no more than 125% of its capacity. For example, a 1000mAh NiMH battery can be charged at a 100mA charge current setting for 12-14 hours. The constant voltage regulation safely tapers the charge current to near zero once the battery reaches its full capacity.

The LTC4079's wide input voltage and charge voltage range, multi-chemistry operation, solar capability, ultra-low quiescent current both while charging & upon termination, simple solution and compact footprint enable it to achieve high performance in leading-edge applications where only more complicated switching regulator-based topologies were once the only option.

www.linear.com

Root of Trust approach secures the IoT

The Internet of Things (IoT) brings challenges, particularly in respect to security

By: Steve Hanna, Infineon Technologies

The easily discerned lines separating cyberspace and the "real world" are disappearing. With the advent of the Internet of Things (IoT), physical objects are increasingly integrated in information systems and individuals are interacting with vast distributed networks dozens of times a day. Clearly, the IoT will change the way people live and work, while changing the way the world itself works around us. With these changes come challenges, particularly in respect to security.

The threat environment faced in implementing the IoT is directly related to the strength of the Internet. The standardized technologies that allow global connectivity are well understood by the engineers and developers building the IoT, but also by villainous characters. To a large extent the architecture of the Internet relies on software-based cryptographic mechanisms to provide security functionality. Inevitably, vulnerabilities in the overall network architecture and the devices connected to this network will be found and exploited at large scale. What is missing is a strong Hardware Root of Trust (HRoT), with dedicated cryptographic functionality, to provision and enforce security policy.

Stronger security from a hardware Root of Trust

There are examples of distributed networks, such as those in the financial industry, where computer servers and systems employ a secured processor or co-processor to protect against exploits that can undermine software-based security software. Such well-designed systems protect against three categories of attack.

1. Semi-Invasive attacks are those in which an adversary tries to induce faulty behavior in the system, which can allow circumvention of security, data manipulation or even extraction of a secret key. An HRoT built with a dual-processor architecture, comprehensive hardware error detection, and protective sensors can detect these types of attacks and then report/act appropriately.
2. Observing attacks are those in which the physical behavior (power consumption, electromagnetic emanation, and photon or heat emissions) is analyzed to yield information about the programming inside the system. Full encryption of all data on an HRoT device and massive randomization generate a highly efficient barrier against such attacks.
3. Manipulative attacks, in which micro-scale devices are used to intercept on-chip signals, can extract useful secret information from unprotected chips. By utilizing memory and data path encryption as well as physical countermeasures, an HRoT can be protected from manipulation threats.

Proving the identity of "Things"

Before any exchange of data between two points on the Internet, connected devices need to verify that transactions take place between "trusted" points. Thus, the basis of security in the IoT is the verification of the identity of billions of devices and users. Today, HRoT devices that are certified by the global Common Criteria evaluation methodology are deployed in hundreds of millions of devices, demonstrating the required interoperability and strength of a security ecosystem that is capable of verifying identity and protecting the integrity of each device. Below examples demonstrate several use cases for this strong identity technology when we build the IoT.

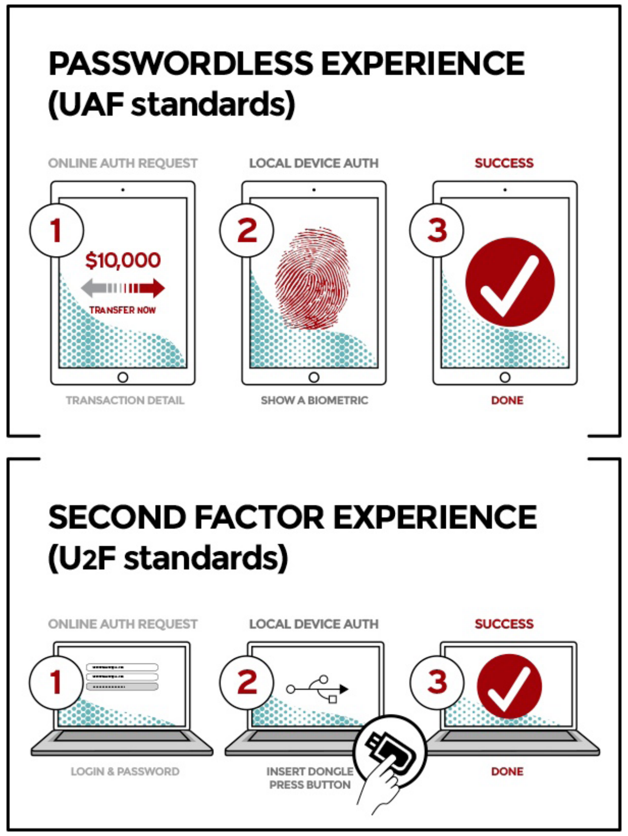


Figure 1: Strong Authentication according to FIDO (Image courtesy of FIDO Alliance)

User identity for IoT

IoT users demand remote access to their devices from anywhere, but still need ease of use and strong security. The simple approach of the username and password authentication fails to meet these requirements since strong passwords are infrequently used (and easily stolen even when used). Recently, the FIDO (Fast IDentity Online) Alliance has released standards for an open, scalable, and interoperable set of multi-factor authentication mechanisms.

As illustrated in **Figure 1**, FIDO permits users to associate their online accounts with a local hardware security token. Then they can use this token to authenticate with other systems, either with or without a PIN. There are two benefits of the FIDO approach for IoT users. First, they get stronger security. Second, the complexity of managing device credentials is vastly reduced.

Device identity for IoT

Ultimately, IoT devices will control thousands of critical systems, ranging from door locks and security cameras, to cars, factory systems and public infrastructure. All will be, or already are, exposed to a variety of network-based threats. To block access by unauthorized parties trying to tamper with device controls, IoT devices must be able to conduct mutual authentication with users, other devices, and the cloud. Fortunately, device identity technologies (e.g., IEEE 802.1AR) are well established and widely available. In this approach, a secure device identifier (DevID) is cryptographically bound to a device and supports authentication of the device's identity.

With an HRoT, the cryptographic authentication can be protected from the types of attacks discussed earlier. IoT devices that are fully capable of establishing, maintaining, and employing long cryptographic keys can be implemented using any of several authenticated and secured processing devices.

Some security chips – such as the open standard Trusted Platform Module (TPM) – go further than establishing device identity by also performing encryption and detecting when a device is compromised. Monitoring system integrity is especially important for IoT, because a rogue device with valid credentials can cause real physical damage.

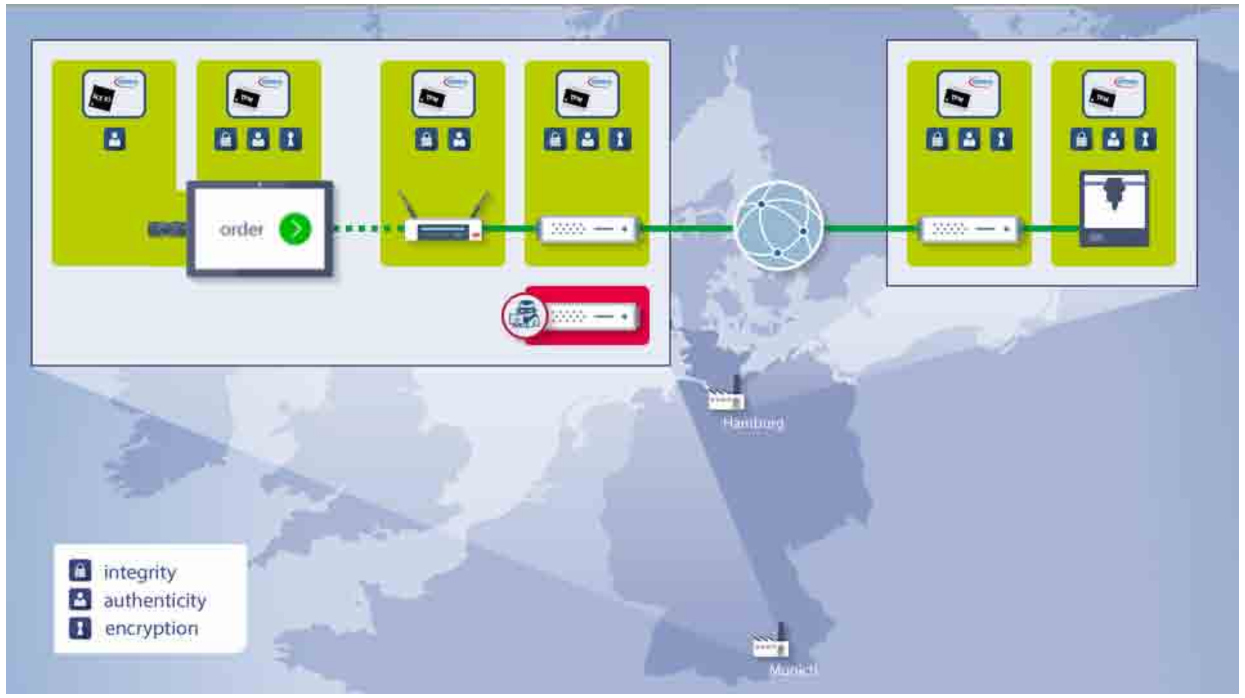


Figure 2: End-to-end Security for the Industrial Internet

Identity for the industrial internet

The Industrial Internet is the application of IoT concepts and technologies in industrial settings. For example, advanced factory automation uses networking to integrate the entire supply chain from supplier and customer, enabling suppliers to customize production to match demand. In such an environment, identity must be verified and communications must be protected end-to-end to make sure that system integrity is maintained. Therefore, all elements of the system from customer to supplier must be secured (see **Figure 2**).

To improve system security and integrity, an HRoT can be integrated in all parts of an Industrial Internet system from a tablet used by customers ordering products to the factory line where the products are manufactured and beyond into shipping, distribution, wholesale, and retail. Different HRoT devices can be used to establish product, device, and user identity, to protect identity and perform encryption and authentication, and to maintain device integrity from the core network server to all network edge points. Such security solutions also offer protection of sensitive IP and process knowhow.

Looking forward

Strong identity authentication and protection for users and devices is a critical requirement for successful build-out of the Internet of Things. We have already seen attacks across cyber-physical boundaries that could have been stopped, or limited, by strong identity protection. Because of the many applications envisioned for the IoT, the impact of these attacks is not restricted to the smart home or connected car, but extends to industrial automation, health care, and many other domains. Fortunately, standards and technologies for strong identity are available without sacrificing ease of use. Hardware security is an essential element in implementing these technologies. When designing for any system that links cyberspace and the physical world, strong identity implemented with secure hardware should be a requirement. Only in this manner can safety be protected

www.infineon.com

Combining security and power efficiency

Power management is critical in hyperconnected systems

By: Shakeel Peera, Microsemi

In today's increasingly hyperconnected world, it is essential that all new designs minimize power consumption and are protected from being cloned, reverse engineered, or tampered with in order to protect embedded intellectual property, system data, and the system itself. FPGAs play a key role in meeting these objectives.

On the power front, FPGAs enable today's high-speed, DSP-intensive system designs by delivering not only the lowest possible static power, but the lowest total power, as well, especially at lower frequencies and high temperatures. This requires a comprehensive approach encompassing process technology, architecture, and the design of configurable logic, as well as the inclusion of embedded features including SerDes, DDR2/3 and DSP blocks.

On the security front, FPGAs are delivering advances in device security by making base-level security easy to use and adopt by system architects. As FPGAs with embedded processors becoming the core of the new systems, the ideal solution is to provide SoC FPGAs with leading-edge embedded security that works inherently, and allows the system architect to plan its security architecture at the core level rather than as an afterthought.

FPGA advantages

Technology companies developing products for the hyperconnected world typically rely on one of the following three fundamental design methodologies to incorporate required functionalities into one or more highly-integrated devices: application-specific standard products (ASSPs), application-specific integrated circuits (ASICs), and field-programmable gate arrays (FPGAs).

While ASSPs are frequently an ideal solution for a new design, developers cannot always find an ASSP-based solution that encompasses all the required functions for a new design on a single device. Additionally, companies that are designing the latest ASSPs are interested mostly in very high-volume applications to amortize their extremely high-cost of ASSP development. This leaves many applications without a "so-called" off-the-shelf ASSP solution.

ASICs have also traditionally been excellent solutions for single-device integration, but as the industry moved toward smaller geometries, overall design cycle times and high tool and other costs have prevented their use. Designers have been forced to look for other methodologies to solve their complex design and integration challenges.

FPGAs, on the other hand, offer the fastest way to integrate a specific design into a single device. The cost of FPGAs is traditionally higher than ASSPs or traditional ASICs, but they provide huge advantages in supporting and facilitating field upgradability, design flexibility, and faster time-to-market. They also promise a significantly better overall total cost of ownership (TCO) compared to ASICs in many next-generation designs.

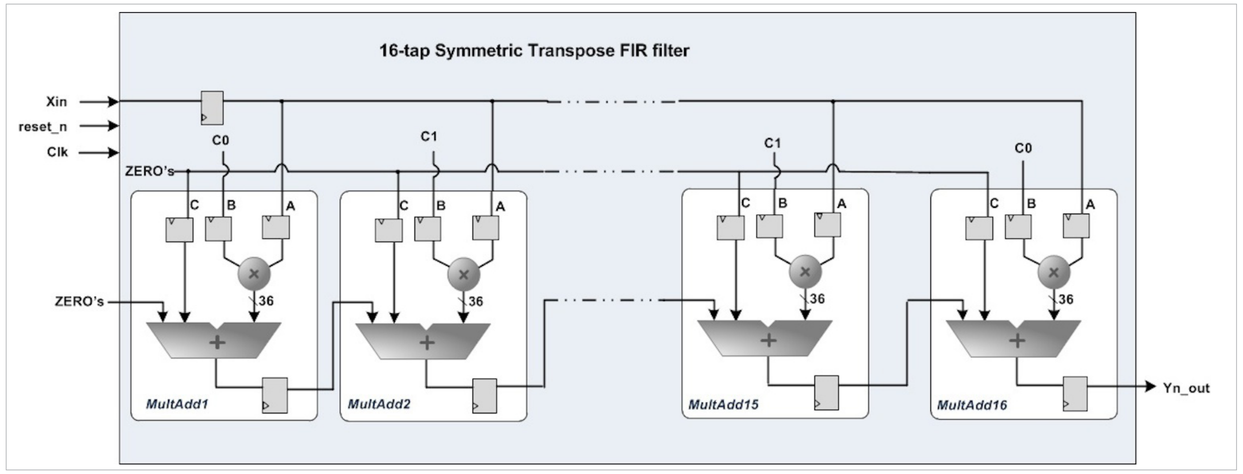


Figure 1a: Architecture of Symmetric Transpose and Systolic 16-Tap FIRs

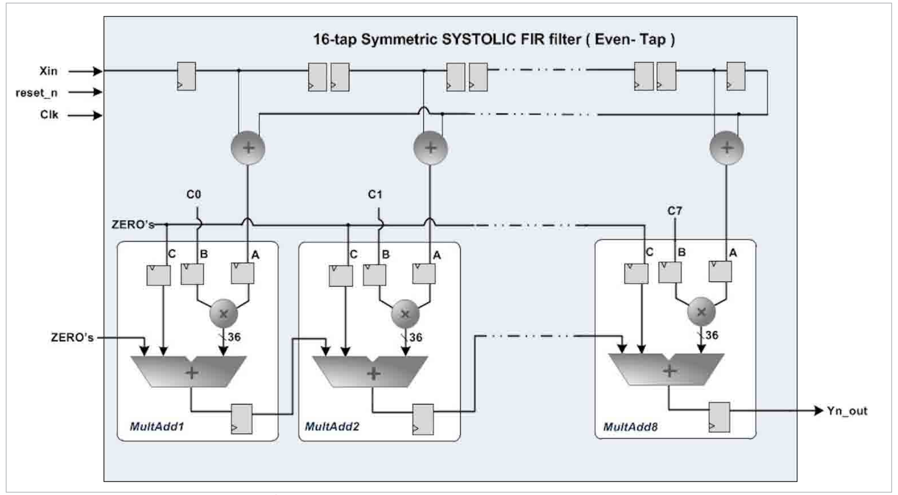


Figure 1b: Architecture of Symmetric Transpose and Systolic 16-Tap FIRs

Power-aware design

While previous generations of FPGAs at the heart of today's IoT systems delivered the lowest static power in their class, the latest solutions deliver not only the lowest static power, but also the lowest total power. This is achieved with through comprehensive power-conscious approach spanning process technology, architecture, the design of the configurable logic, and embedded features such as SerDes, DDR2/3, and DSP blocks.

Additionally, these devices offer special power modes that reduce the power consumption to even less than the static power. In the last two decades, many advanced CPUs and MCUs have architected various power-saving modes to address the power consumption issues caused by higher-frequencies and higher-integrations. Only the most advanced FPGAs have been architected properly to provide similar advanced low-power capabilities while offering higher-frequency devices. Customers now have access to low-power modes implemented in non-volatile memory-based FPGAs for the first time.

All of these features and capabilities are particularly important in high-speed, DSP-intensive system designs. Finite Impulse Response or FIR filters are among the DSP blocks widely used in a large number of applications to remove unwanted noise, improve signal quality, or shape signal spectrum. Several architectures of these FIR filters (Transpose, Systolic with or without symmetry) have various characteristics such as the total initial latency, the number of DSP blocks, the throughput or performance, and the number of pipeline registers. **Figure 1a & b** depicts the symmetric versions of Transpose and Systolic 16-Tap FIRs and illustrates the differences between these architectures.

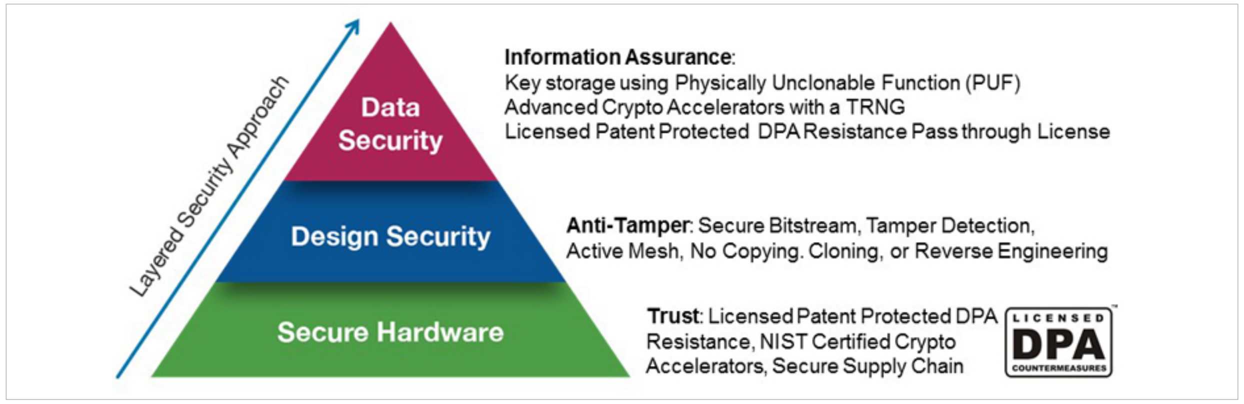


Figure 2: The best device security is achieved using a layered approach encompassing secure hardware, design security and data security.

In a nutshell, systolic architectures use pipeline stages and reduce the inputs fanout to increase the frequency of operations. However the initial latency for N-Tap systolic FIR is (2*N -2)-cycles. The transpose architectures run at a lower frequency but have a better initial latency of (N-1)-cycles and use less sequential resources. Other criteria related to filter stability arise in particular when the number of taps is very large and weighting features need to be considered. For instance, in a voice processing application dealing with echo cancellation, the weights need to be higher at the near end, where most of the echo resides, and decrease on the later filter taps as the echo is lower.

There are dramatic differences in how much power FPGAs consume across these architectures. Studies have been done on FPGA development kits covering 32-, 64- and 128-Tap Transpose FIR implementations using power estimation tools and – more importantly – actual silicon measurement at various temperatures. These silicon measurements show that, when properly designed and implemented, FPGAs deliver significant power savings that are even more substantial at lower frequencies and high temperatures.

For the best-performing FPGAs, power dissipation is linear to the number of Taps. Power dissipation figures are worse for some poor-performing FPGAs when the number of Taps is low; in others, these figures get worse when the number of Taps grows, which may highlight architectural issues. When choosing an FPGA solution, it is important to carefully review available data for power dissipation – both static and total.

Security considerations

The IoT is essentially a collection of electronic networks that need end-to-end layered security beginning at the device level. FPGAs can play a pivotal role in improving security through the use of unique built-in features and differentiated capabilities. It is essential that all FPGAs used in IoT and other hyperconnected system designs be protected from cloning, reverse engineering and tampering in order to protect these embedded IPs.

In addition, FPGAs need to become the root of trust in complex applications. When FPGAs include embedded device security technology that works inherently, they also make base-level security easy to use and adopt. A multi-layered approach is required, including secure hardware, design security and data security (see **Figure 2**).

One of the issues with SRAM-based FPGAs is the need to configure the device every time it is turned on from an external memory device. This vulnerability exposes the design to reverse engineering. Storing the configuration information in non-volatile memory on the chip makes it impossible to capture the information and prevents reverse engineering and tampering with the design for malicious effect.

Data security is particularly important, including protecting the application data that the FPGA is processing. Examples of data security features necessary for new applications in our hyperconnected world include:

- Hardware protection from differential power analysis (DPA) attacks. Simple and differential power analysis (SPA/DPA) can extract secret keys by measuring power consumption during cryptographic operations like bitstream loading
- The use of a Physically Unclonable Function (PUF) to generate a private public key pair is essential to authenticating machines in the IoT. Additional cryptographic functions like random number generators, hashing functions, and symmetric encryption/decryption functions are also essential and included in SmartFusion2 and IGLOO2 devices.

The IoT and other hyperconnected networks require secure and extremely power-efficient devices. By reducing total rather than just static power and supporting a multi-layered approach to embedded security, today's FPGA technology is helping to enable a new generation of system designs.

www.microsemi.com

What the IoT and Smart Grid tech brings to utilities

Next-generation software and hardware infrastructures are critical to a robust and reliable Smart Grid

By: Malcolm Loro, Ciena

Smart Grid technologies, including tools such as smart meters, intelligent network management, and performance monitoring are helping utility companies better track grid operations, keeping those operations visible at all times so that they can assess the status of individual endpoints and take efficient countermeasures before critical situations arise. Proper implementation of next-generation software and hardware infrastructures are critical to a robust and reliable Smart Grid.

Despite a traditionally low tolerance for risks, utilities today face incredible pressure to adapt, modernize and streamline their operations to meet demands for new energy sources (such as solar and wind), and keep operations securely protected and in full compliance with evolving regulatory standards. Industry observers maintain utilities are increasingly embracing high-performance, optical and packet networks to better leverage the benefits of the Internet of Things and Smart Grid technologies. In addition, the promise of integrating alternate-energy tech like solar into smart households provide even more opportunities for utilities within the Smart Grid (see **Figure 1**).

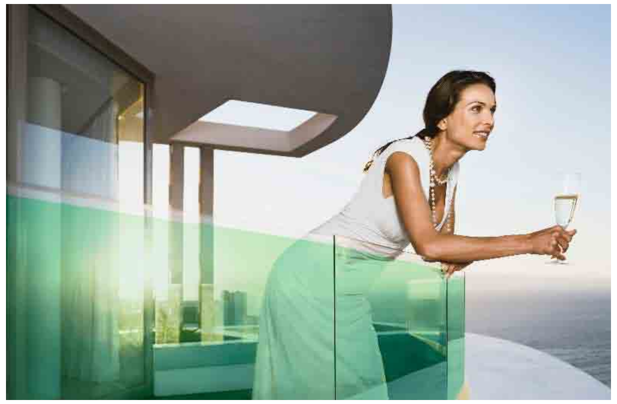


Figure 1: Integrating alternate-energy tech like solar into smart households provide even more opportunities for utilities within the Smart Grid (Image from Heliatek)

Smart Grid tech and the IoT

Characterized by a two-way flow of electricity and information between utilities and consumers, smart grid technologies deliver real-time information and enable the near-instantaneous balance of supply (capacity) and demand at the device level. A national smart grid would integrate and enhance electrical elements, including traditional upgrades and new grid technologies with renewable generation, storage, increased consumer participation, sensors, communications, and computational abilities.

Meanwhile, the Internet of Things (IoT) also plays a key role. Market research firm Gartner Inc., defines IoT as "the network of dedicated physical objects (things) that contain embedded technology to sense or interact with their internal state or external environment. The IoT comprises an ecosystem that includes things, communication, applications and data analysis."

IoT is already driving innovations such as smart homes, smart cities, renewables integration, and the intelligence now built into automobiles and countless other devices. Gartner analysts, meanwhile, estimate the utilities sector will be among the top three biggest adopters of IoT in the coming years. Manufacturing, utilities and transportation will be the top three verticals using Internet of Things (IoT) devices in

2015, with 736 million connected devices in use next year, according to Gartner predictions. In total, the market research firm forecasts there will be 4.9 billion connected devices in use next year, with total IoT services spending nearing $70 billion in 2015.

Utilities are expected to leverage IoT for smart metering and SCADA. Smart metering is used to remotely collect customer meter data at frequent intervals, such as every 15 minutes, rather than monthly or quarterly as completed by traditional analog meter-readers. SCADA (Supervisory Control & Data Acquisition) systems will be increasingly automated to improve their use, along with the repair of utilities operations networks (see **Figure 2**).

It's crucial for utilities to be able to continuously monitor and streamline all of the processes associated with the delivery of power. Many utilities currently face challenges in integrating aging IT infrastructures with mission-critical operational processes, along with growing requirements to expand 'green' services, such as providing solar energy, for example. IoT will enhance Smart Grid technologies to bring much-needed transparency and visibility to daily utility sector operations.

Central control

Ultimately, all components, including embedded systems, sensors, and software MUST be centrally managed and controlled, so that IT departments are able to analyze data to gain greater value from the information that flows through the organization. Undoubtedly, the need for greater integration and collaboration across operational units makes a compelling argument for the adoption of Smart Grid and IoT.

Utility operations around the globe are already embracing Smart Grid and IoT to improve operational efficiency and deliver better services to their consumer audiences. In some areas, technologies such as sensors and two-way communications networks are being used by grid operators to identify problems rapidly and avert or isolate outages and blackouts. Utilities can juggle demand more easily and even lower their costs. In addition, smart grid technologies make it easier to integrate renewable power into the grid.

Figure 2: Utilities are expected to leverage IoT for smart metering and SCADA

By 2020, Gartner analysts predict utilities sector businesses will take over the No. 1 spot among all vertical industries investing in IoT, due primarily to investments in smart meters. The manufacturing sector and government will round out the top three IoT adopters, with 1.7 billion IoT units installed.

Smart Grid and IoT technologies will drive a greater focus on digital security as new devices, apps and standards are brought online. Increased connectivity brings more data, gathered frequently from more devices in all kinds of locations. This information is only useful if harnessed by a high-performance network that offers the scalability, reliability and resiliency to provide real-time access and end-to-end security. The intersection of devices, machines and advanced networking is unleashing new opportunities to analyze, and deliver intelligence that utilities can use to innovate. Networks play a crucial role in providing the intelligence, management and secure infrastructure that can scale to support billions of context-aware devices.

www.ciena.com

Podcast highlights

By: Alix Paultre, Editorial Director, PSD

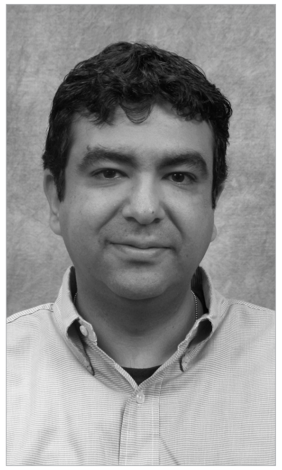
Recent episodes from the "Paultre on Power" podcast series on the latest trends in the electronic design industry

Electric Imp

Bryan Kennedy of Electric Imp on intelligent connected devices

In this podcast Bryan Kennedy, VP Strategic Development of Electric Imp, talks about issues involved in creating connected IoT devices. The Electric Imp connectivity platform, featuring fully integrated hardware, software, OS, APIs, cloud services and security, can effectively enhance powered devices with greater functionality, efficiency and performance.

tinyurl.com/PSD-IMP | www.electricimp.com



Microsemi

Shahin Sadeghi of Microsemi on powerline comms in the IoT

In this podcast Shahin Sadeghi of Microsemi talks about the issues involved in device communications within the Internet of Things (IoT). With the plethora of devices demanding bandwidth in a business, home, or community, the ability to use other communications infrastructures can significantly ease the wireless broadband demand. Shahin also talks about the collaboration with STMicroelectronics on a new electric vehicle car charger solution using Microsemi's innovative PLC line driver.

tinyurl.com/PSD-MICRO | www.microsemi.com

Keysight

Bob Zollo of Keysight on power test

In this podcast Bob Zollo of Keysight talks about the complexity, speed, and high sensitivity of power test today. The IoT has spawned devices that demand the latest in test equipment available. In today's world of ever increasing focus on efficient energy and power utilization, engineers are under increasing pressure to find every possible way to reduce consumption in their designs for their power converters.

tinyurl.com/PSD-KEY | www.keysight.com

How do you launder e-clothing?

By: Alix Paultre, Editorial Director, PSD

People have been wearing clothes almost since we began walking erect, and one thing we've learned over the millennia in our evolution in both ourselves and in our habiliments is that people have funky, dirty bodies. We have been strapping technology about ourselves and stuffing tools and devices into our clothes for a long time. In fact, a great deal of the clothing we wear today carries fashion hints from when it was purpose-built for some specific functionality. The problem is the human body can be a hostile environment.

The big problem (some would say our greatest gift) is that we are animals. Animals are biological systems, and biological systems use ablative processes for surface maintenance. In addition, for thermal management and lubrication biological systems exude a variety of liquids. In other words, to maintain our skin we shed it constantly and sweat a lot, among other things. Human skin is an abrasive as lethal as a rat's incisors over time, and sweat is an insane corrosive that has damaged materials from silk to steel.

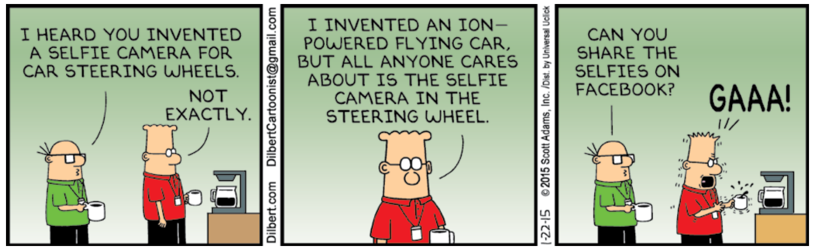
From worn stone balustrades in cathedrals to computer keys with no faces, the evidence of the deterioration of surfaces due to the human touch is all around us, and if it weren't for people like Thomas Jennings (the first African American to receive a patent, BTW) who created the various ways to clean clothes without water or soap (he invented a dry-cleaning process called "dry scouring", and used the money to buy his family's freedom) we'd still be severely restricted in the materials and fashions we could conveniently wear.

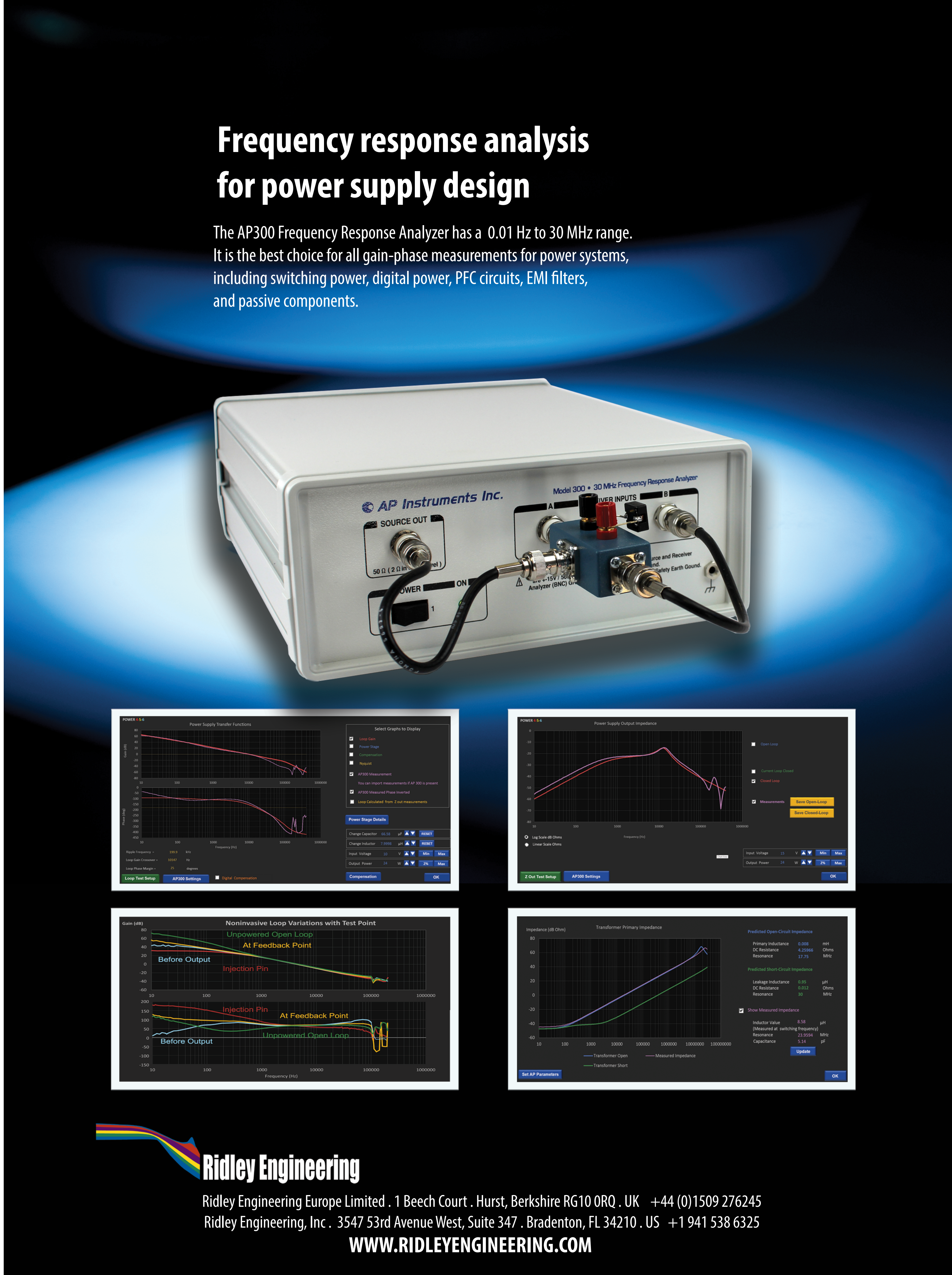
None of this bodes well for today's electronic devices. From smartphones carried in hot sweaty pockets to implantable medical devices, anything touching the human body must take into account our dirty, sweaty bodies. Environmental issues such as humidity, shock, and vibration must be a consideration in every electronic device intended for intimate human use. (I won't even think about the number of people who use their smart device on the toilet, and those related hygiene issues.

Handheld electronics are pretty mature in this sense; the first few generations of cell phones taught everyone about the importance of ruggedness and durability in a portable personal device. Then again, people have been taking technologies as delicate as watch movements and vinyl record players putting them in rugged boxes for centuries. I have an old 1935 Weston Analyzer on my shelf, and if I could find batteries that would fit it the test device would still work today.

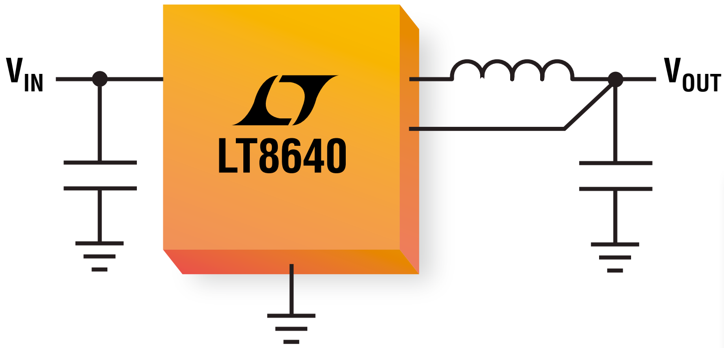
The biggest issues are in the area of wearable and semi-implantable devices. Anything held close against the human body for any length of time must address cleanliness and hygiene issues, and that includes things like straps and harnesses. Clothes get dirty remarkably fast, and need to be cleaned thoroughly and relatively often. That fact will not change for wearable tech. Who will open the first e-clothing Laundromat?

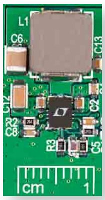
www.powersystemsdesign.com



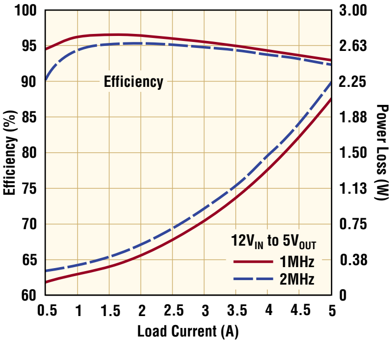


42V, 5A Silent Switcher®
More Power & Spread Spectrum





Actual Size
Demo Circuit



Low EMI/EMC Passes CISPR25 Class 5, 95% Efficient at 2MHz

The LT®8640 joins our growing family of ultralow quiescent current high voltage monolithic synchronous buck regulators. Its inherent ultralow EMI/EMC emissions, coupled with spread spectrum capabilities, allows it to comfortably meet CISPR25 class 5 radiated emissions requirements for automotive environments. The LT8640 consumes only 2.5µA of quiescent current while regulating an output of 3.3V from a 12V input source. It also delivers up to 5A of output current with efficiencies as high as 96%.

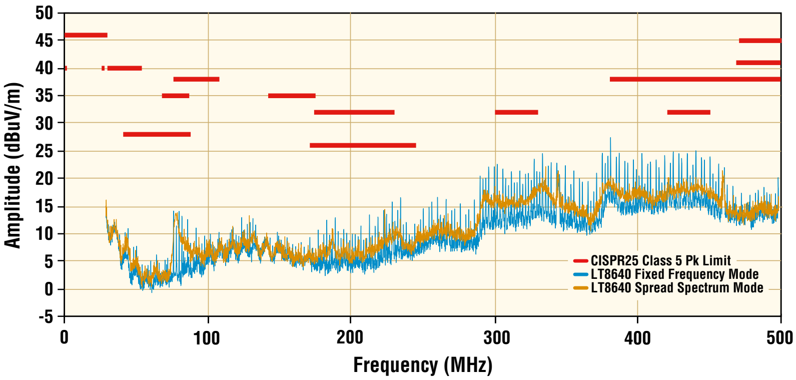
Features

- Ultralow EMI/EMC Emissions
- Spread Spectrum Frequency Modulation
- Input Voltage: 3.4V to 42V
- Ultralow Quiescent Current in Standby: 2.5µA
- Low Dropout: 100mV at 1A All Conditions
- Small 3mm x 4mm QFN Package

www.linear.com/product/LT8640

+49-89-962455-0

Simplified LT8640 EMI/EMC Curve, I_{OUT} = 4A



Europe Sales offices: **France** 33-1-41079555 **Italy** 39-02-38093656 **Germany** 49-89-9624550 **Sweden** 46-8-623-1600 UK 44-1628-477066 **Finland** 358-9-88733699 ***Distributors:*** **Belguim** *ACAL* 32-0-2-7205983 **Finland** *Tech Data* 358-9-88733382 **France** *Arrow Electronique* 33-1-49-784978, *Tekelec Airtronic* 33-1-56302425 **Germany** *Insight* 49-89-611080, ***Setron*** 49-531-80980 **Ireland** *MEMEC* 353-61-411842 **Israel** *Avnet Components* 972-9-778-0351 **Italy** *Silverstar* 39-02-66125-1 **Netherlands** *ACAL* 31-0-402502602 **Spain** *Arrow* 34-91-304-3040 **Turkey** *Arrow Elektronik* 90-216-4645090 **UK** *Arrow Electronics* 44-1234-791719, *Insight Memec* 44-1296-330061