Maxim > Design Support > Technical Documents > Application Notes > 1-Wire® Devices > APP 5689
Maxim > Design Support > Technical Documents > Application Notes > A/D and D/A Conversion/Sampling Circuits > APP 5689
Maxim > Design Support > Technical Documents > Application Notes > Embedded Security > APP 5689

Keywords: distribution automation, smart grid security, asset management and protection

APPLICATION NOTE 5689

Distribution Automation and the Smart Grid: Coming of Age with a New Set of Challenges

By: David Andeen, Strategic Segment Manager for Energy

Nov 22, 2013

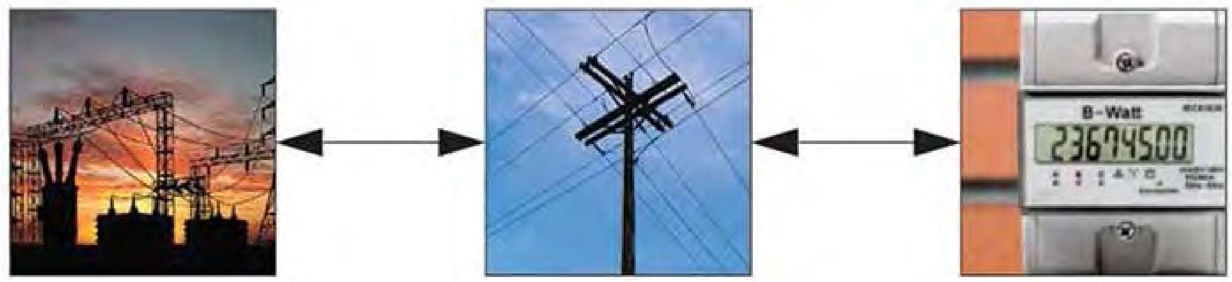
Abstract: The combination of aging electricity grid infrastructure and renewable portfolio standards present new challenges in the distribution automation space worldwide. In this application note, we review three key areas: asset protection, security, and asset management. In each area, device-level silicon provides benefits to ease the transition to a complete smart grid.

A similar version of this article appears on *EDN*, October 2013.

Introduction

You may think that today is a smartphone/tablet world. In fact, there are more “smart” devices around than most realize. Take, for example, the smart grid with smart meters. Every day utilities are installing a shiny new smart meter on our house and encouraging us to take control of our energy future. We are to monitor and report consumption on websites and sign up for programs, such as those monitoring time of use, - aimed at conserving electricity. It may not be a surprise, but managing all this mounting, distributed “smart” data is one of industry’s newest challenges. Smartphones and tablets require a host of computational power behind them, known as the “cloud.” Because of this, smart meters and the smart grid require effective infrastructure support to assess the data gathered and to optimize energy delivery. Witness the ongoing importance of computer technology. Enter the emerging role of distribution automation.

Distribution Automation Comes of Age



Distribution automation is not new. Since the 1960s, the promise of applying computing technology to the electricity grid has captured the attention of the utility industry. However, until recently the real benefits of such an implementation were questionable. With an extremely reliable grid in the developed world, some were asking, “why risk the reliability of that system by adding more control systems?" A "smart" system? What were the real benefits? Admittedly, the theoretical benefits made it difficult to justify the cost.

In 2013, however, the utilities serve a different world. The aging grid, its efficiency (or inefficiencies), and environmental concerns all now drive a shift toward enhanced control and performance, toward distribution automation. In the United States, the average transformer is 40 years old, the equivalent of a transformer's recommended operating life—the utility infrastructure needs upgrading. This is not just seen in the U.S., but is becoming a worldwide issue. The widespread blackout in India in July 2012 affected 680 million people—and that occurred when India already could not meet its daily peak power needs. Add to that, India expects its power output needs to grow by 45% in the next five years.

The renewable portfolio standards (RPS) in many countries around the world exemplify the international drive toward efficiency and distributed generation. Now 30 of the 50 U.S. states[1] require specific percentages of the power generated to come from renewable sources, such as wind and solar. California requires 33% of electricity to come from renewable sources by 2020.[2] The European 2020 targets[3] require 20% of power to come from renewable sources by the year 2020 and a concurrent 20% increase in energy efficiency, presumably leading to a reduction in overall power consumption. Similar legislation exists in China with the Medium and Long-Term Energy Conservation Plan (November 2004), the Medium and Long-Term Development Plan for Renewable Energy (September 2007), and the Renewable Energy Law (January 2006).[4]

Today distribution automation is recognized as "the extension of intelligent control over electrical power grid functions to the distribution level and beyond… [It] can be enabled via the smart grid."[5] The benefits of distribution automation are generally well accepted, but that does not make it easy to implement successfully, or reliably. There are profound challenges to its widespread application.

Challenges to Implement Distributed Automation

Yesterday's utility is now becoming a power generation and distribution company. The world races to both rollout smart meters and implement an infrastructure change in the distribution grid. What are the key challenges to managing so widespread an implementation? At Maxim Integrated, we see three critical areas to address: asset protection, grid security, and asset management. These critical areas are also opportunities for grid suppliers. Let's look briefly at each.

Asset Protection

Asset protection means that utilities must invest in high-performance components that reliably monitor the grid and protect their high-cost assets. This protection ensures the longevity of their investments.

Investments in the equipment for distribution automation are expensive, and automation upgrades run in the range of $10M to $20M for a single substation.[6] Consequently, no modern utility begins a major upgrade project without a long project scope and well-documented justification. Project costs , often result in rate adjustments High-quality semiconductor sensors and optimized components ensure the uptime of the grid and, thereby, provide the most cost-effective protection for the utilities' investment.[7]

An analog signal chain lies at the heart of any grid-connected device. Each device in the distribution network needs to measure electricity. The simplest grid-connected devices measure current faults only, while the most complex relays implement full four-quadrant measurement up to multiple harmonics.

This signal chain (**Figure 1**) generally consists of a voltage or current transformer, an op amp, a voltage reference, and an analog-to-digital converter (ADC) for the actual electricity measurement. Isolation and DC-DC converters provide the necessary protection and power rails to run the system.

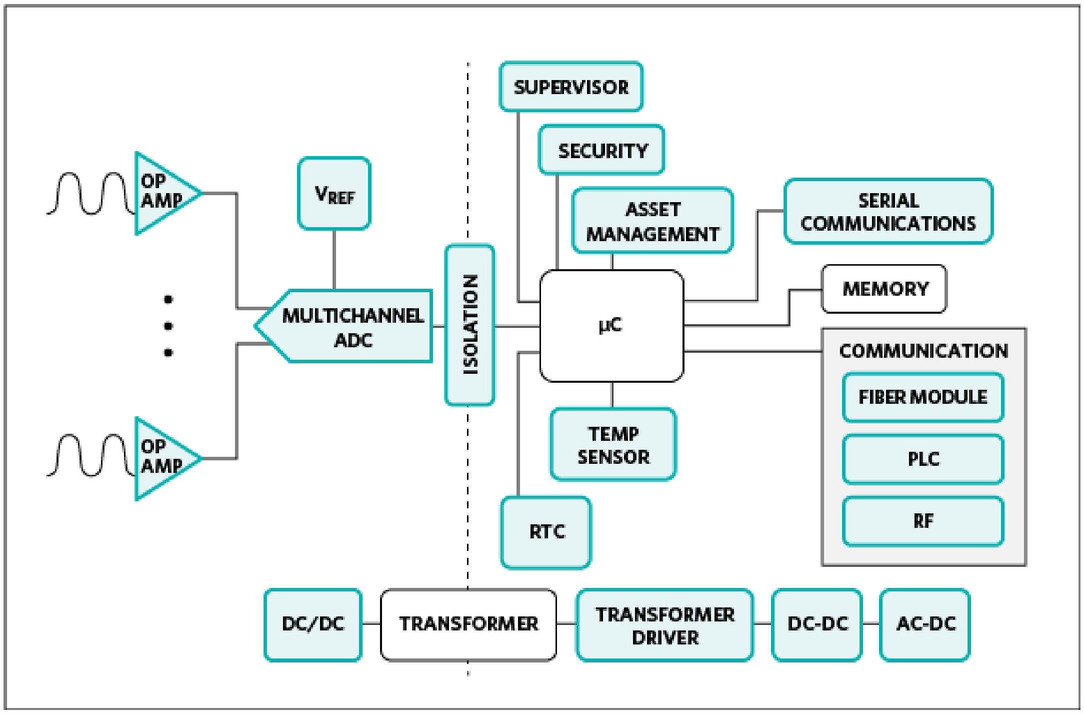


Figure 1. Essential components in a signal chain that lies at the heart of a smart grid implementation.

The ADC is the central component of the signal chain and must provide optimized performance specific to distribution automation. The MAX11040K exemplifies the high performance required by featuring 24-bit resolution and a sample rate up to 64ksps. This 4-channel ADC simultaneously samples channels to prevent any synchronization errors between lines. Multiple MAX11040Ks can be cascaded to achieve sampling of up to 32 channels.

Most semiconductor companies demonstrate their knowledge of distribution automation equipment with a simple block diagram of one signal chain. That presentation is no longer adequate. The diversity of equipment required for the smart grid demands a deeper knowledge of each component and product. From phasor measurement units to capacitor bank controllers, the accuracy and timing requirements of each system vary drastically and require components with quite distinct performance specifications.

Grid Security

Because the infrastructure of any distribution grid must be protected from cyber attack, security for the grid and all its data is critical.

Security is the most discussed facet of advanced distribution automation rollouts today. The discussion often migrates to network security and encryption, but while encryption is critical, it is not a modern panacea. A system security solution uses advanced physical security to deliver unsurpassed low-cost IP protection, clone prevention, and peripheral authentication.[8] Bidirectional authentication, multiple layers of encryption, and physical tamper detection all protect aspects of the grid—hardware, data transmission, and data storage—from cyber threats.

When protecting hardware, a culture of security considers the entire product life cycle, from manufacturing to installation to operation. A combination of secure hardware and security protection schemes must be built in. It is critical that manufacturing partners be prevented from accessing private security keys or from developing ways to hack a system. This very breach of security was done on smart meters in Puerto Rico in 2012 and completely disrupted their new grid rollout. During installation, secure assets must perform a strong authentication, optimally a bidirectional challenge and response, to confirm that the hardware and software are legitimate. Such mutual authentication confirms that neither the devices nor the software have been tampered with during manufacturing, especially when in the hands of third-party contractors. During operation, physical security is needed to ensure that the systems are not subject to tampering. Multiple layers of encryption are also necessary to prevent interception, modification, or otherwise tampering with communication messages that contain the power to switch power on or off.

The MAXQ1050 microcontroller integrates all of these security features to provide life-cycle security. Authentication prevents the loading of bad software and prevents malicious parties from removing the loaded software for cloning purposes. Multiple layers of symmetric and asymmetric encryption protect data; on-board key generation protects secret keys. Tamper pins and physical mechanisms for key erasure provide protection from mechanically, thermally, and by other means removing secure keys and system data.

Asset Management

Asset management includes both simple and complex methods of tracking assets so that the status of field equipment is known at all times. Such management is invaluable for ensuring performance and monitoring maintenance.

Strategic asset management is explained with the following scenario. During a massive storm, outages occur at many points on a utility's grid. Crews from various utilities are brought in to help with repairs; the mantra of "keep the lights on" wins the day. Lines get repaired, equipment gets swapped out, and the power gets turned back on. That was fast. At the end of the crisis, however, assets are operating in the field without the complete knowledge of and careful tracking by the utility. Given the cost of equipment and the need to secure distributed resources and power delivery, an advanced grid cannot afford to have unknown or suboptimal assets operating in the field.

Strategic asset management requires complete top-to-bottom implementation, authentication, and tracking of *all* processes, software, and systems required for efficient grid operation. Authentication is paramount. Embedded secure authentication is fundamental for equipment to self-identify and, therefore, acknowledged as part of the system, making it easier to track and manage.[8] For a modest investment, simple silicon can be used to uniquely identify any piece of equipment on a distribution grid, from a line sensor to a transformer to a recloser controller. The unique challenge-and-response identification allows each piece of equipment to be tracked and then communicated with throughout the utility's advanced metering infrastructure AMI network. This is actually where security overlaps with reporting: asset identification, location, operational status, latest maintenance date, or any of myriad other reporting functions.

The Meaning and Directive for Us

The modern utility was once a power generation and distribution company with strong expertise in power electronics. Now the paradigm has shifted as utilities integrate complex IT operations with multiple layers of complex equipment and the management of resources and data. As utilities purchase new equipment to upgrade their infrastructure, they need new devices and security algorithms that build that infrastructure from the bottom up and throughout the grid. These grid devices need more than Ethernet and simple encryption; they must be equipped with robust protection, management, and security functions.

The smart grid is often described as the overlaying of energy measurement and communication on the electricity grid. This definition is too simple. The smart grid should integrate secured hardware with intelligent energy-management software. The grid needs advanced sensing and communication to create a robust, efficient, and secure power delivery system that improves system efficiency and the ability to accommodate distributed resources. Only then will we have efficient distribution automation operating on a broad scale.

References

1. "Most states have Renewable Portfolio Standards," U.S. Energy Information Administration, February 3, 2012, www.eia.gov/todayinenergy/detail.cfm?id=4850.
2. "California Renewables Portfolio Standard (RPS)," California Public Utilities Commission, www.cpuc.ca.gov/PUC/energy/Renewables/index.htm.
3. "Europe 2020 Targets," European Commission, http://ec.europa.eu/europe2020/europe-2020-in-a-

nutshell/targets/index_en.htm.

4. “Renewable Energy and Energy Efficiency in China: Current Status and Prospects for 2020,” Worldwatch Report 182, Worldwatch Institute, October 2010, www.worldwatch.org/system/files/182%20China%20Energy.pdf.

5. “Advanced Distribution Automation”, June 28, 2013, http://en.wikipedia.org/wiki/Advanced_Distribution_Automation.

6. “Electric Distribution System”, SmartGrid.gov, U.S. Department of Energy, March 31, 2013, updated June 28, 2013, www.smartgrid.gov/recovery_act/deployment_status/distribution.

7. For an overview of Maxim Integrated’s distribution automation solutions, see www.maximintegrated.com/solutions/distribution-automation/.

8. For an overview of Maxim Integrated’s embedded security solutions, see www.maximintegrated.com/products/embedded-security/deepcover.cfm.

Related Parts		
MAX11040K	24-/16-Bit, 4-Channel, Simultaneous-Sampling, Cascadable, Sigma-Delta ADCs	Free Samples
MAXQ1050	DeepCover Secure Microcontroller with USB and Hardware Cryptography	

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 5689: http://www.maximintegrated.com/an5689
APPLICATION NOTE 5689, AN5689, AN 5689, APP5689, Appnote5689, Appnote 5689