Keywords: Industry 4.0, IO-Link, PLC, distributed computing and control, security, authenticated security, embedded security, pervasive sensing, distribution and automation

APPLICATION NOTE 5991

REALIZING INDUSTRY 4.0: ESSENTIAL SYSTEM CONSIDERATIONS

By: Suhel Dhanani, Sr. Principal MTS, Control and Automation Strategic Marketing, Maxim Integrated

Abstract: This application note examines various system design hurdles to resolve before implementing the needed infrastructure for Industry 4.0 and looks at some of the key system challenges.

Introduction

Everyone in the automation industry has heard the buzzword of "Industry 4.0," a phrase first coined in 2011 at the Hanover fair. This industrial concept envisions the factories of tomorrow as vastly more integrated, automated, and flexible. Faster and more efficient, they will churn out the goods desired by a changing market place.

Industry 4.0, by its very name, implies that we have already gone through three industrial revolutions and are on the cusp of the fourth (Figure 1).[1]

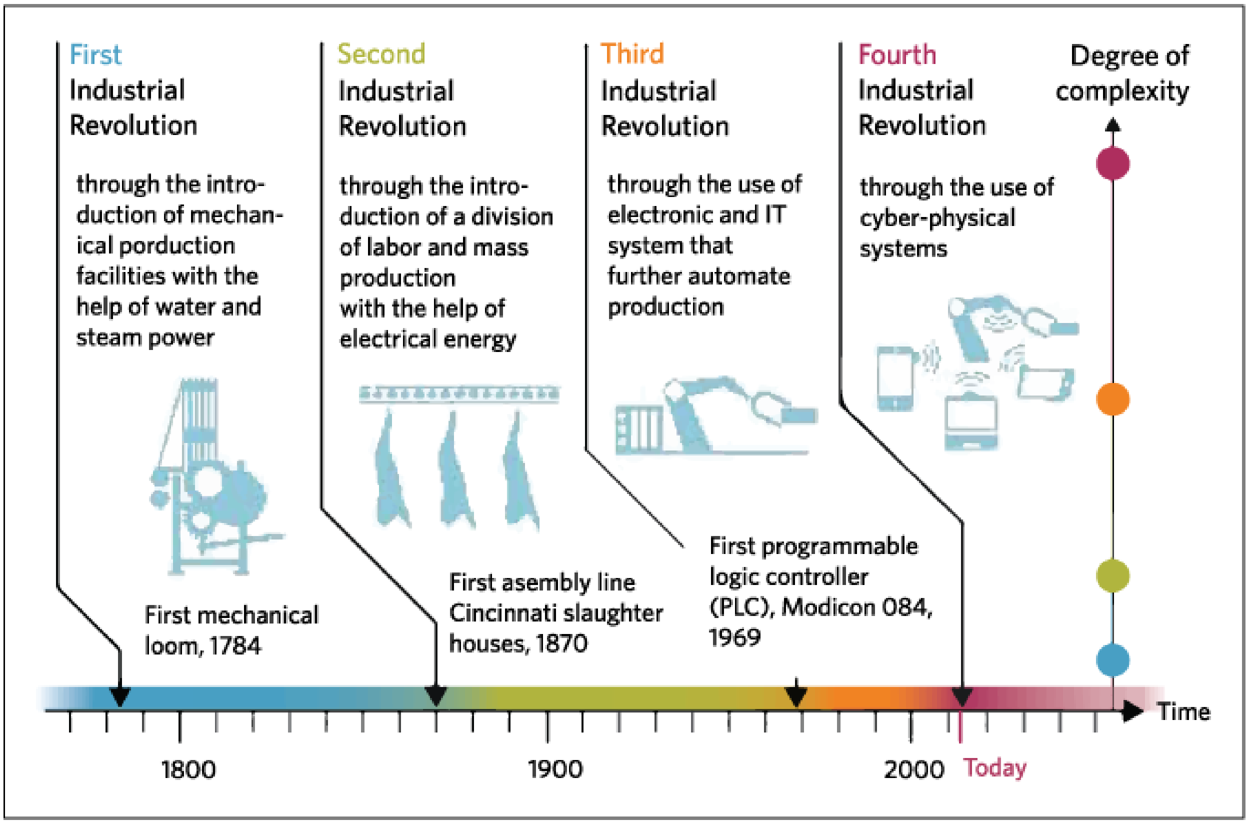


Figure 1. Looking back through recent times, we can identify four distinct pivotal moments for the evolution of industrial automation. Graphic source is DFKI.

It is clear that this contemporary fourth revolution in manufacturing and process automation will advance on the backbones of connected systems: sensors, actuators, control systems all linked through different types of networks via the Internet protocol. Once all the machine/sensor data is on the cloud, interesting analyses can be done to optimize manufacturing, predict failures, schedule maintenance, automatically replenish inventory, and even customize finished product specifications to reflect market dynamics.

One interesting, contemporary example of Industry 4.0 is General Electric's newest U.S. factory in Schenectady, New York. This sodium-nickel battery manufacturing facility has more than 10,000 sensors spread across 180,000 square feet of manufacturing space; all sensors are connected to a high-speed internal Ethernet.[2] As **MIT Technology Review** writes: "[Sensors] monitor things like which batches of powder are being used to form the ceramics at the heart of the batteries, how high a temperature is being used to bake them, how much energy is required to make each battery, and even the local air pressure. On the plant floor, employees with iPads® can pull up all the data from Wi-Fi nodes set up around the factory."[3]

This article starts with the premise that this fourth industrial revolution is underway. It argues that the ubiquitous connectivity on the shop floor will lead to productivity and predictability gains powered largely by ever-improving software and algorithms. Yes, impressive and quite attainable. However, there are various system design hurdles to resolve before we get the infrastructure in place and this revolution really going. This article looks at some of these key system challenges.

System-Level Design Considerations for Industry 4.0

The realization of the Industry 4.0 vision will most likely span a decade or two, but it is already impacting various system designs. The automation in **Figure 2** shows the three, key system design aspects that must be implemented as we move towards Industry 4.0.

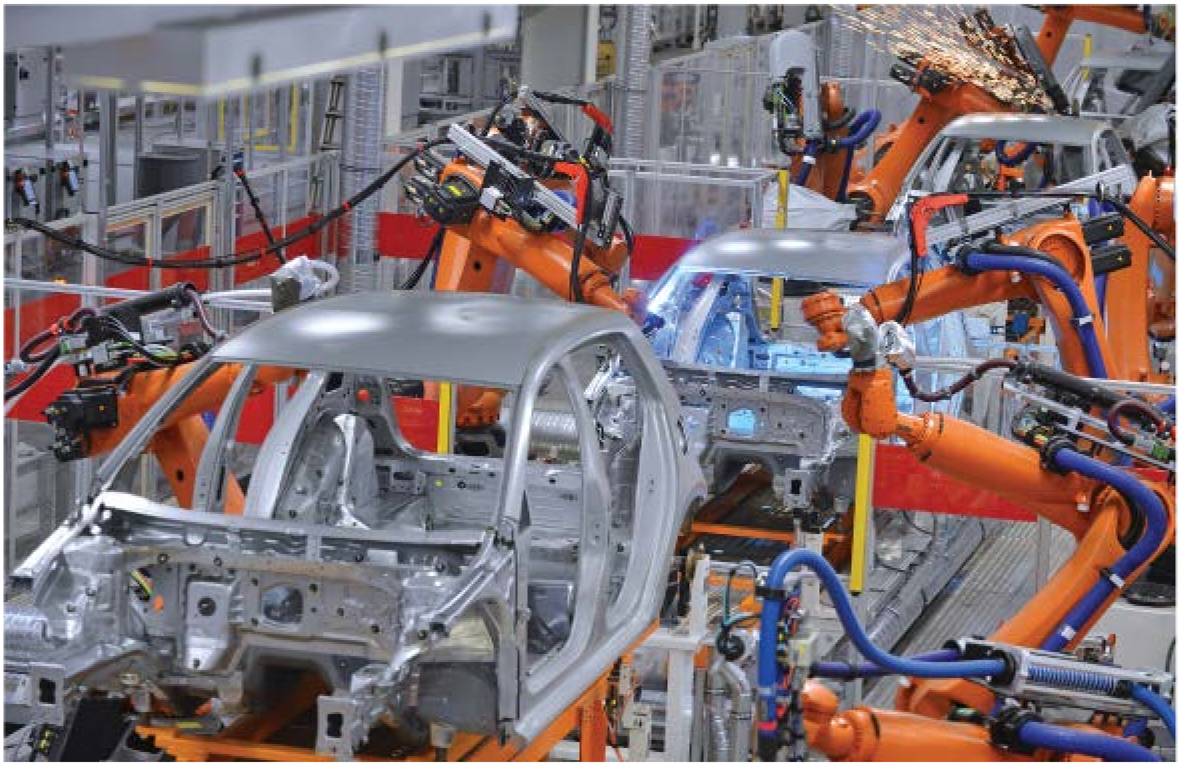


Figure 2. Industry 4.0 is driving three fundamental industrial system requirements: distributed computing and control; pervasive sensing, and authenticated and secure systems.

Distributed Computing and Control

One key system-level trend already underway is the localization of the compute and control systems. Distributed control is required to add flexibility to a complex assembly line, provide low-latency control, and alleviate the main PLC's processing requirements. In the next-generation factories this will become even more prevalent. PLCs will continue to shrink in size and process an increasing number of I/O channels, both analog and digital. PLCs will also have to support various I/O protocols, including newer ones such as the IO-Link® standard.

Pervasive Sensors

What about all the disparate sensors? The Industry 4.0 basic premise is that manufacturing data is shared, but this means that an ever-increasing amount of data must first be collected. This avalanche of data results from the explosion in the number of sensor systems both inside a factory and a process facility and spread throughout remote operations. Even if a process parameter does not impact your control algorithm today, its data must still be collected for probable use in the future. We can anticipate that the rapid and expected innovation of algorithms running on the cloud today may eventually "reinvent" an older process parameter to predict an important system failure mechanism. The phrase often used in the industry to describe this rise in sensing solutions is "pervasive sensing." We will say more about this below.

Authenticated Security

Finally, connecting all the sensors, control systems, and actuators via the Internet protocol to enable "big" data analysis definitely increases security concerns. A large part of the industrial security issues are addressed with software firewalls and secure Internet switches/gateways. But security concerns go beyond these communication portals to the hardware itself. New defense-in-depth standards require that the end-device network (e.g., sensors and PLCs for this discussion) be authenticated and secure. This broad-based software and hardware security has a direct, system-level impact on the design of these systems.

Distributed, Local Control: the Rise of the Micro PLC

A smaller, yet powerful PLC that enables local control of a process or assembly line is quite attractive because it enables low-latency, distributed control. But a micro-PLC design must grapple with significant technical challenges for analog I/O integration and heat dissipation, challenges resolved successfully in the Micro PLC proof-of-concept design developed by Maxim (**Figure 3**).

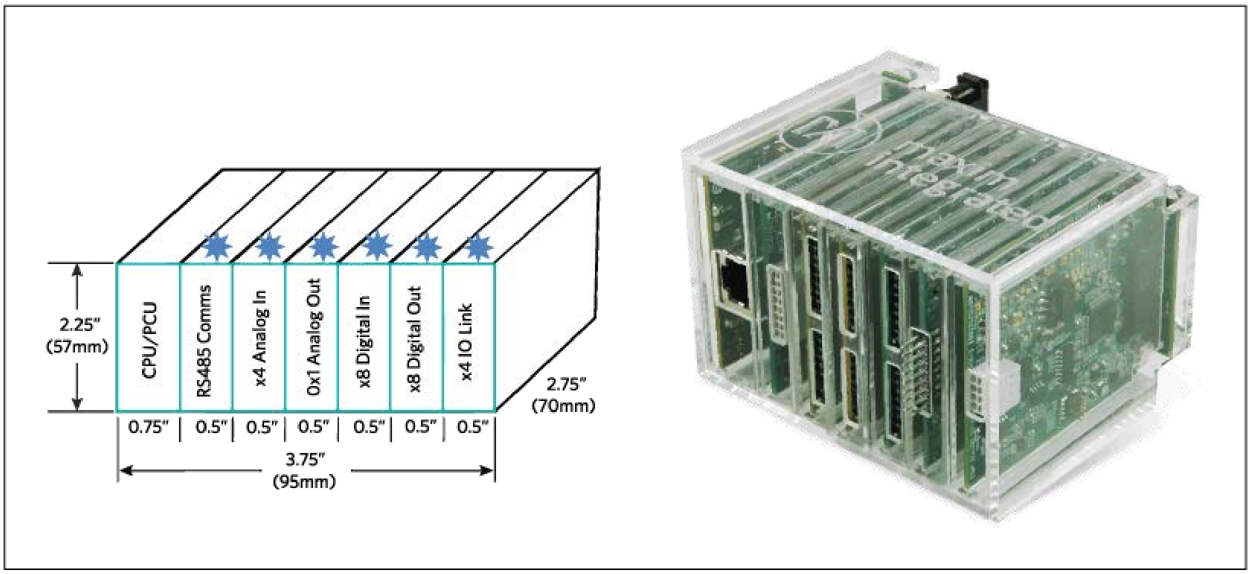


Figure 3. This Micro PLC proof of concept integrates a 32-bit microcontroller, Ethernet connectivity, and 25 I/O channels. The total area is 23 cu in (406,125 mm^3).

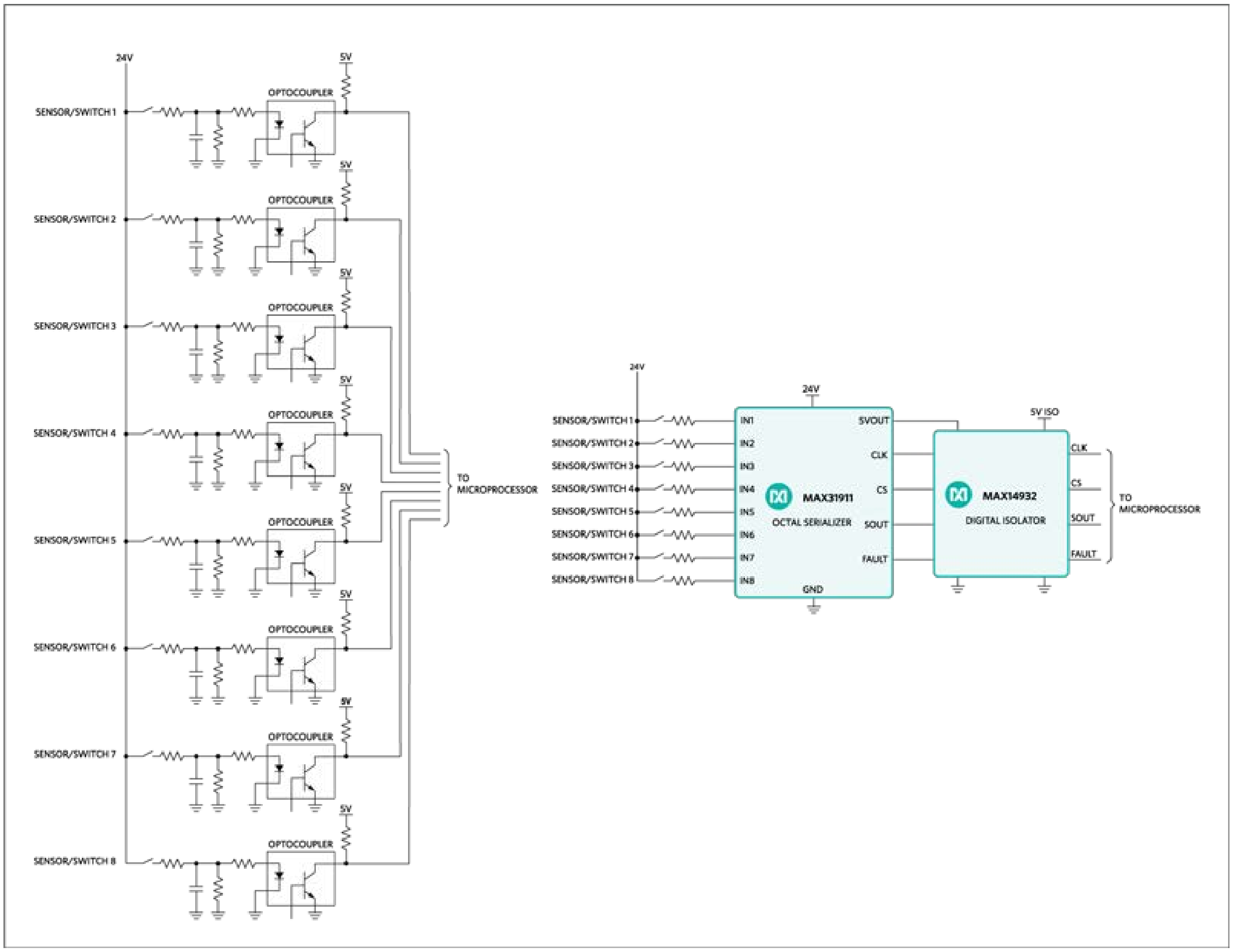
This Micro PLC fits in the palm of your hand. It integrates the necessary 32-bit microprocessor and Ethernet connectivity; it processes and interfaces with a total of 25 I/O channels. Specifically, it provides:

- Four analog IN and 1 analog OUT channels
- Eight digital IN and 8 digital OUT channels
- A quad IO-Link module that interfaces with 4 IO-Link-enable sensors

Successful Analog Integration

We know that analog and discrete components represent 50% to 70% of the board space on PLC I/O modules. We also know that I/O modules require the bulk of the space in any PLC. Consequently, shrinking a complete PLC system to this micro-form factor requires us to solve the analog I/O integration challenge.

One way to achieve this tiny form-factor is to use integrated analog devices instead of numerous–even hundreds of–discrete components. Board size shrinks, power consumption drops, and reliability increases. **Figure 4** shows an octal serializer (MAX31911) and a quad-channel data isolator (MAX14932) that replace the dozens of discrete optocouplers and hundreds of resistors and capacitors in the traditional design at the left. This compact Micro PLC solution has the same I/O channel capacity of a regular PLC.



More detailed image.

Figure 4. This two-chip Micro PLC proof-of-concept replaces hundreds of discrete components.

Heat Dissipation and Efficient Power Conversion

When you integrate these many channels into such an aggressive form factor, heat dissipation and the power conversion efficiency of the on-board DC-DC switcher become major issues. Higher power efficiency leads to a much cooler operation. **Figure 5** shows some power efficiency curves for the MAX17505 DC-DC synchronous switching regulator driving different load currents with a 5V output.

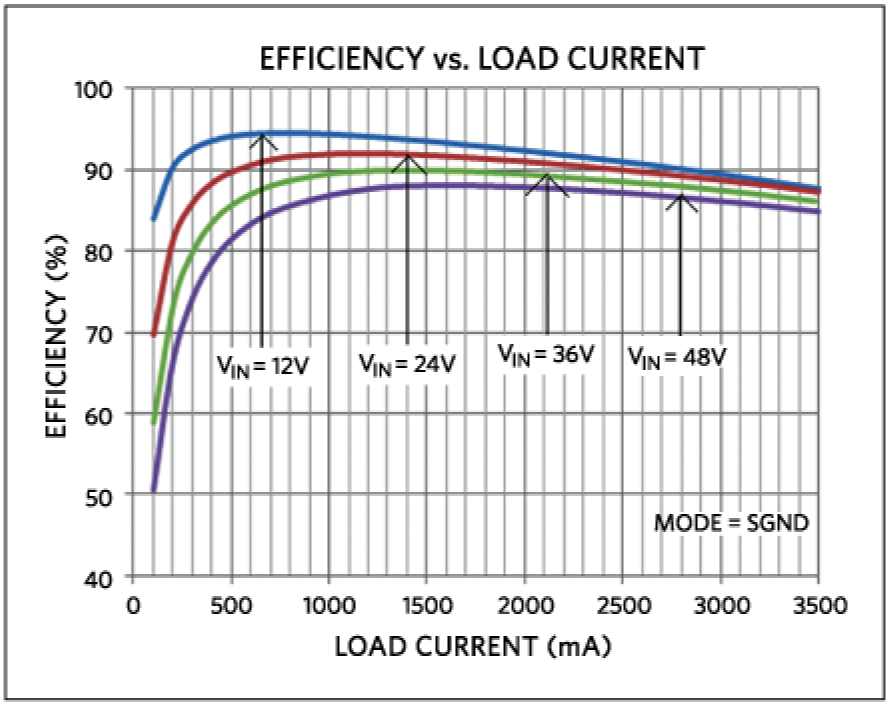


Figure 5. Efficiency versus load current. The data shows higher than 90% efficiency across a wide range of V_{IN} and load currents.

With higher than 90% efficiency (given a backplane input voltage of 24V and a current drive > 1A), this family of voltage regulators run anywhere from 30% to 50% cooler than legacy solutions. This translates into significanly lower temperature rise so it is easier to pack more I/O modules into a smaller Micro PLC.

Much can be said about the MAX17505 high-efficiency, high-voltage, synchronously rectified step-down converter (**Figure 6**). With dual integrated MOSFETs, it operates over a 4.5V to 60V input and delivers up to 1.7A and 0.9V to 90%V_{IN} output voltage. Built-in compensation across the output voltage range eliminates the need for external components. The feedback (FB) regulation accuracy over -40°C to +125°C is ±1.1%. This downconverter is available in a compact (4mm x 4mm) TQFN, lead (Pb)-free package with an exposed pad. Simulation models are available.

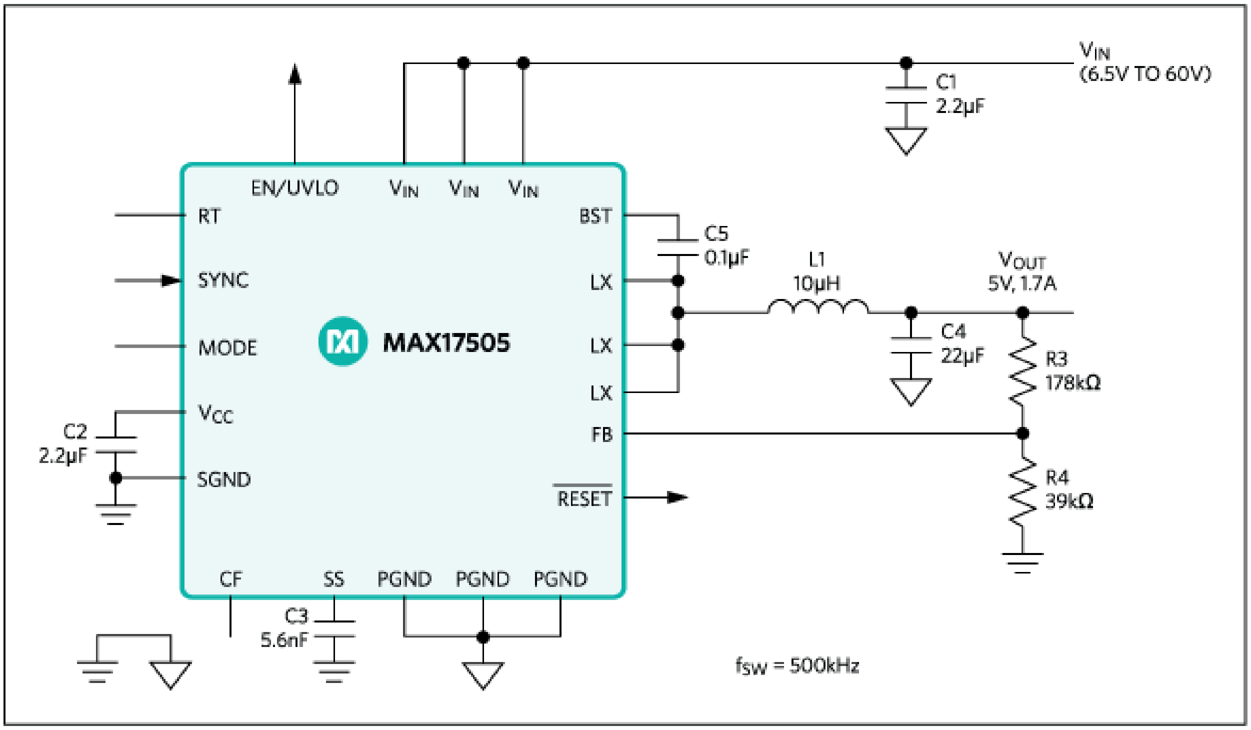


Figure 6. The MAX17505 high-efficiency, high-voltage, synchronously rectified step-down converter has dual integrated MOSFETs, operates over a 4.5V to 60V input, and delivers up to 1.7A and 0.9V to 90% V_{IN} output voltage.

The MAX17505 uses a peak-current-mode control architecture with a MODE feature to operate the device in multiple control schemes: pulse-width modulation (PWM), pulse-frequency modulation (PFM), or discontinuous-conduction mode (DCM). The PWM operation provides constant frequency operation at all loads, and is useful in applications sensitive to switching frequency. PFM operation disables negative inductor current and additionally skips pulses at light loads for high efficiency. Featuring DCM with constant frequency operation down to loads lighter than PFM mode, the MAX17505 does not skip pulses but only disables negative inductor current at light loads. The DCM operation offers efficiency performance that lies between PWM and PFM modes. The low-resistance, on-chip MOSFETs ensure high efficiency at full load and simplify the layout.

Pervasive Sensing with the IO-Link Communication Standard

In the factories of tomorrow, sensors will be everywhere and connected via different interfaces to gateways or PLCs directly. No longer sending merely an ON/OFF signal, sensors will soon be transmitting rich data. This is when and where the IO-Link protocol, one of the industry's fastest growing sensor communication technologies, emerges as so important. While IO-Link is an IEC® standard, it is based on the established 3-wire sensor and actuator connection.

Since the 1980s, industrial field buses have allowed smarter devices, quicker installations, reduced wiring, and easier maintenance. However, the lack of a single, universally accepted field bus has also created confusion, training challenges, high costs, and compatibility issues among equipment. The IO-Link protocol is the first open, field-bus-diagnostic, low-cost, point-to-point serial communication standard used for communicating with sensors and actuators. It has been adopted as an international standard (IEC 61131-9).[4]

The IO-Link protocol standardizes interoperability among industrial equipment from all over the world. This standard can exist directly on the PLC or be integrated into all standard field buses. This flexibility quickly makes it the de facto standard for universal communication with smart devices like Maxim Integrated's Santa Cruz optical light sensor, the MAXREFDES23# (**Figure 7**).

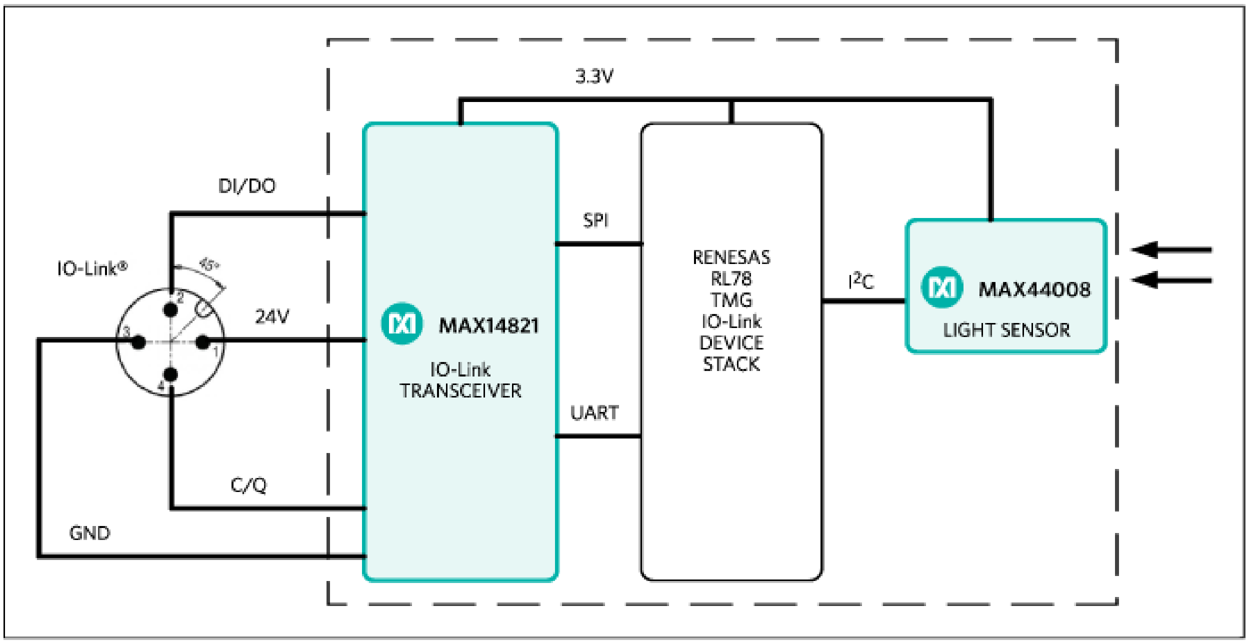


Figure 7. The reference design block diagram for the Santa Cruz optical light sensor.

IO-Link technology, along with the continued miniaturization of sensors, facilitates the deployment of ultra-small, power-efficient sensors throughout the factory. **Figure 8** shows the Santa Cruz IO-Link color sensor.

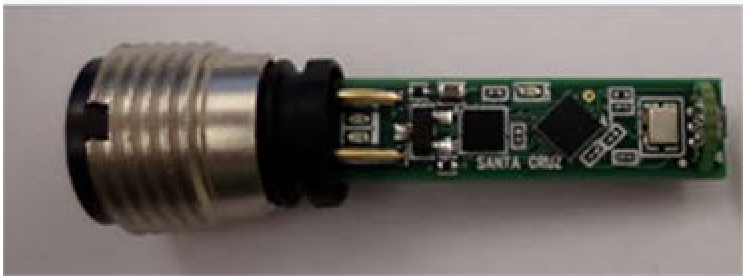


Figure 8. The MAXREFDES23# is a tiny IO-Link light sensor that integrates six sensors: ambient light (clear), red, green, blue, infrared, and temperature. All are on a tiny printed circuit board (PCB) that is 6.5mm x 25mm.

One of the world's smallest IO-Link light sensors, the Santa Cruz MAXREFDES23# system has six integrated sensors–ambient light (clear), red, green, blue, infrared, and temperature–all on a tiny PCB. The

Santa Cruz design consists of an industry–standard Maxim IO-Link device transceiver (MAX14821); a Renesas® Electronics ultra-low-power, 16-bit microcontroller (RL78) utilizing the Technologie Management Gruppe Technologie und Engineering (TMG TE) IO-Link device stack; and a Maxim Integrated MAX44008 light sensor (Figures 7 and 8). This collaboration made Santa Cruz an IO-Link version 1.1/1.0-compliant light sensor reference design. Compact sensing systems like Santa Cruz make it simple and convenient to deploy many widespread sensors that provide useful data via the IO-Link protocol to a sensor hub connected either to the cloud or to a PLC.

Today's industrial sensors such as Santa Cruz must be ultra-power efficient since they are small and enclosed for safety. Increasingly, many of these sensor designs will use a high-efficiency DC-DC switching regulator rather than the traditional LDO. Products such as the MAX17550/MAX17551 DC/DC regulators shown in **Figure 9** are architected to deliver > 90% efficiency even when driving small 25mA and 50mA load currents.

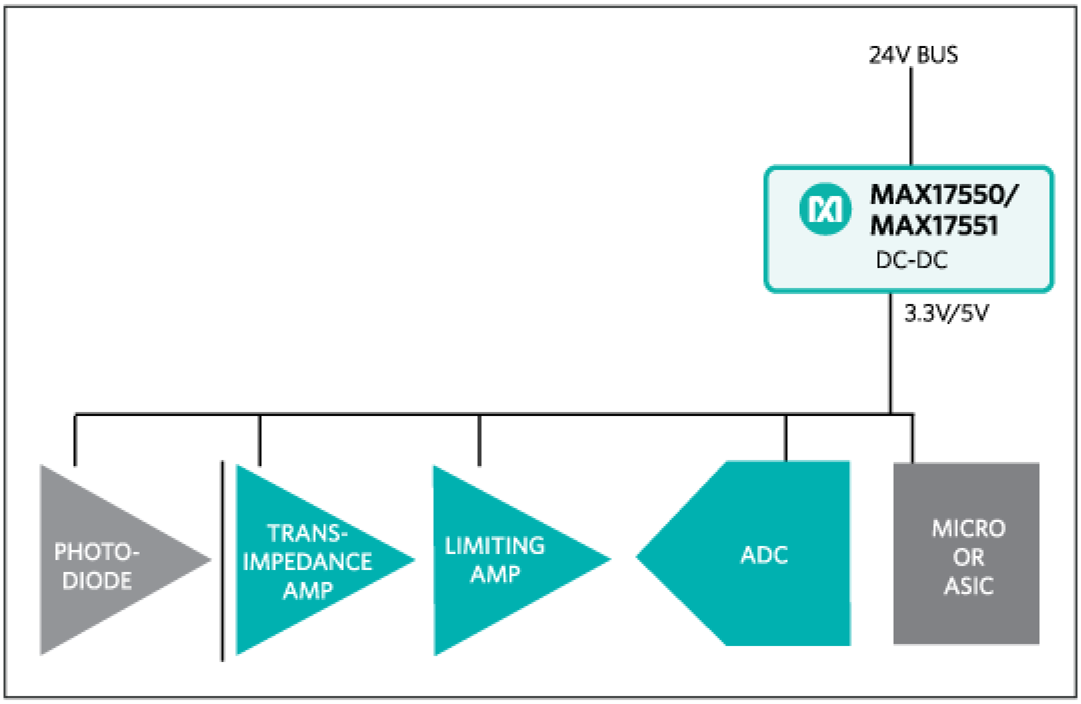


Figure 9. The MAX17550/MAX17551 high-efficiency DC-DC switching regulators are designed to drive low load currents for sensor system applications.

The Need for Embedded Hardware Security

It is no secret that security is not always considered critical by IC vendors. Consider a recent survey of 599 Global IT and IT security executives in 13 countries sponsored by Unisys "in partnership with the Ponemon Institute." Their results found that only 28% of respondents agreed that security is one of the top five strategic priorities across their enterprise. Almost 60% of the same people, however, acknowledged that cyber threats are putting their control systems and SCADA systems at risk.[5]

Only 28% of respondents prioritize security. That should be disturbing to readers because we know that distributed control and ubiquitous connectivity are already driving the growing need for security. Most of the security issues revolve around the need for better firewalls, intrusion detection systems, and a secure switching architecture. But equally important is the need for trusted hardware, especially an I/O module and a remote field sensor. These devices can be cloned or spoofed, especially if there is little physical security around them. When any such breach happens, the industrial internet that is making critical decisions based on the data collected from these devices is seriously compromised. Consequently, it is critically important to ensure that these systems are authenticated and secured. Ultimately, without secure embedded hardware, we will not experience the potential of Industry 4.0 to its fullest.

Our focus on secure systems for Industry 4.0 must begin with a trusted sensor that is sending the data to the cloud or the PLC. The implications of a remote security breach are profound. If, for example, a compromised sensor sends spurious data about the level of oil in a tank or the pressure in a pipeline, the actions taken (or not taken) based on that data could potentially have catastrophic consequences. Am I being too dramatic here? Not at all. But there are, admittedly, less catastrophic outcomes from compromised sensor data. A big data analytics program that uses sensor data to predict maintenance requirements can be completely thrown off if that data has been compromised. At stake here is uptime, predictable maintenance, and overall industry efficiency–the cornerstones of Industry 4.0.

Physical security of all sensors may not always be possible, especially when the sensor is very remote like this one (**Figure 10**) used to monitor oil and natural gas fields. Inaccessibility makes it vulnerable to physical attacks, so it essential to authenticate all these sensors before their data is accepted.

Figure 10. A remote sensor is especially vulnerable to a physical attack or breach of security. A secure authentication scheme eliminates false positives and inaccurate status information.

Fortunately, an authentication scheme was instituted years ago for medical and consumer products such as printer cartridges. Today authentication is very standards based and must be implemented with a tamper-proof device that adheres to the authentication protocol.

A simple conceptual block diagram of a hardware-based authentication scheme based on the symmetric SHA 256 algorithm is shown in **Figure 11**. The SHA-256 protocol, based on a challenge-and-response exchange between authorized devices, will authenticate the sensor before its data is accepted and read. SHA-256 authentication makes it impossible for an attacker to connect to a network and pretend to be a sensor or even to replace the sensor system with a compromised system.[6]

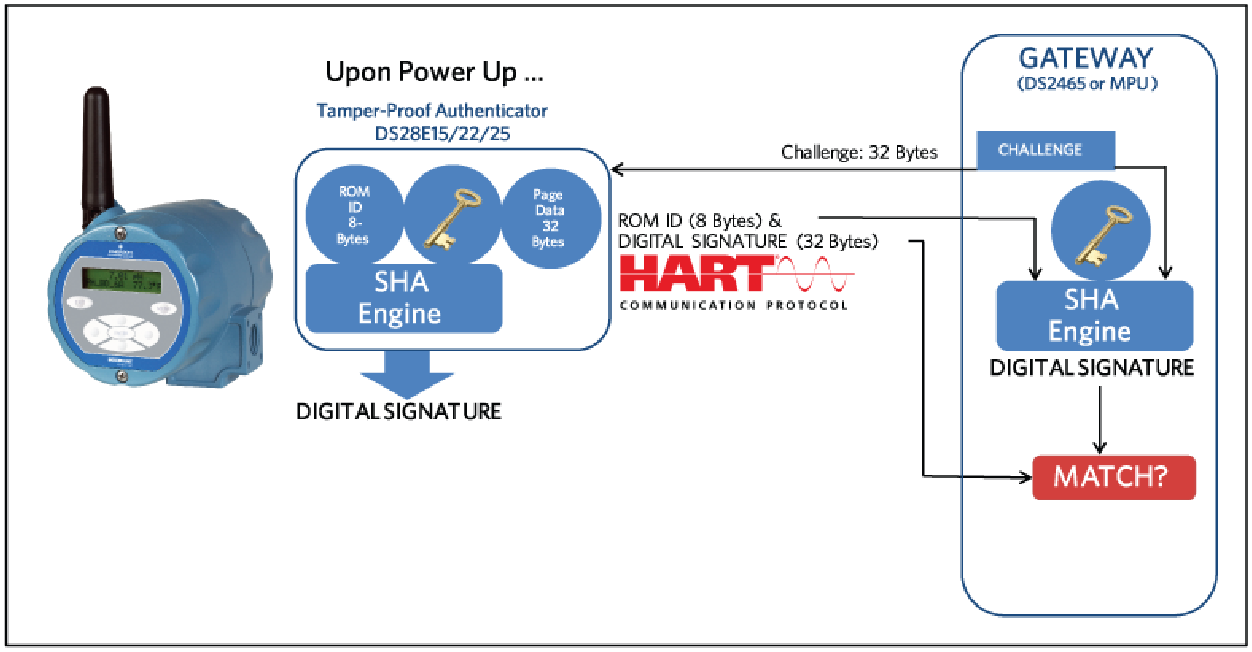


Figure 11. SHA-256-based authentication for remote field sensor systems over HART or any other communication standard. The page data (32 bytes) and the key (2 bytes) are known to both sensor and the host. There will be a small overhead in the number of bytes transferred. HART® is a registered trademark of the HART Communication Foundation. The image of the wireless transmitter provided courtesy of Emerson Process Management.

Summary

Industry 4.0...the modern way to describe a connected manufacturing operation where data from different distributed PLCs, sensors, and other field devices are aggregated to harness the benefits of analytics and optimization software. Industry 4.0 has the promise of optimizing manufacturing assets in terms of uptime, scheduled maintenance, power efficiency, and more efficient utilization of all resources. Manufacturing data can also be integrated within the ERP and CRM software of the firm to efficiently plan manufacturing processes and to even use a customer's information to change assembly lines and process parameters.

However, there are important system design factors to consider when you embark on interconnecting all disparate manufacturing systems. We have discussed a few of these considerations in this article. We have shown how new silicon technologies, especially within the analog/mixed-signal domain, can be used to address some of these industrial system challenges. These new integrated technologies not only allow you to shrink the sensor systems and the PLCs, but also provide a way to cost effectively add embedded security in some of the critical IO devices in the field.

As we embark upon this Industry 4.0 transition, no doubt we will find and solve additional system design considerations within our factory systems. We will definitely use the latest technology to achieve the requisite power, performance, and communication profiles.

References

1. "Self Organizing Factories," **Pictures of the Future**, Magazine Spring 2013 by Siemens. For more background information, go to www.siemens.com/innovation/apps/pof_microsite/_pof-spring-2013/_html_en/industry-40.html. Also Mathas, Carolyn, "Industry 4.0 is closer than you think," EDN Network, December 02, 2013 at http://edn.com/design/wireless-networking/4425363/Industry-4-0-is-closer-than-you-think. For additional general background information, go to http://en.wikipedia.org/wiki/Industry_4.0.
2. "An Internet for Manufacturing," **MIT Technology Review**, January 28, 2013. See www.technologyreview.com/news/509331/an-internet-for-manufacturing/.
3. Ibid.
4. For more information, you can start here: https://www.profibus.com/newsroom/press-releases/new-io-link-design-guideline/
5. See "Critical Infrastructure Security, Research shows critical infrastructure providers must adopt proactive, agile security strategies," **Unisys** and Ponemon Institute July 2014, www.unisys.com/insights/critical-infrastructure-security.
6. For more information on SHA-256 authentication see Linke, Bernard, "The Fundamentals of a SHA-256 Master/Slave Authentication System," **EE Times**, 6/19/2013, www.eetimes.com/document.asp?doc_id=1280942; also available as Maxim Integrated application note 5779, "Introduction to SHA-256 Master/Slave Authentication." See also Linke, Bernhard, "A SHA-256 master/slave authentication system," **Electronic Products**, 5/16/2014 www.electronicproducts.com/Digital_ICs/Communications_Interface/A_SHA-256_master/slave_authentication_system.aspx#.U778pI1dXnY; available as Maxim Integrated application note 5785, "Implement Heightened Security with a SHA-256 Master/Slave Authentication System."

IEC is a registered service mark of the International Engineering Consortium, Inc.
IO-Link is a registered trademark of Profibus User Organization (PNO).
iPad is a registered trademark of Apple Inc.
Renesas is a registered trademark and registered service mark of Renesas Electronics Corporation.

Related Parts		
DS28E15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples
DS28E22	DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb User EEPROM	Free Samples
DS28E25	DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM	Free Samples
MAX14821	IO-Link Device Transceiver	Free Samples
MAX14932	4-Channel, 2.75kV$_{RMS}$ and 3.75kV$_{RMS}$ Digital Isolators	
MAX17505	4.5V-60V, 1.7A, High-Efficiency, Synchronous Step-Down DC-DC Converter with Internal Compensation	Free Samples
MAX17550	60V, 25mA, Ultra-Small, High-Efficiency, Synchronous Step-Down DC-DC Converter with 22µA No-Load Supply Current	Free Samples
MAX17551	60V, 50mA, Ultra-Small, High-Efficiency, Synchronous Step-Down DC-DC Converter with 22µA No-Load Supply Current	Free Samples
MAX31911	Industrial, Octal, Digital Input Translator/Serializer	Free Samples

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

Application Note 5991: https://www.maximintegrated.com/en/an5991
APPLICATION NOTE 5991, AN5991, AN 5991, APP5991, Appnote5991, Appnote 5991

© 2014 Maxim Integrated Products, Inc.
The content on this webpage is protected by copyright laws of the United States and of foreign countries. For requests to copy this content, contact us.
Additional Legal Notices: https://www.maximintegrated.com/en/legal