Keywords: uptime, maintenance, predictive, preventive, proactive, reactive, production, factory, process, facility, industrial, maintenance, reliability, security, safety, FMEA, authentication, preventative

TUTORIAL 5518

Uptime Protects the Bottom Line

By: John Mossman, Control & Automation Marketing Manager

May 30, 2013

Abstract: This tutorial examines various considerations to increase uptime and how they impact the bottom line. These include approaches to maintenance in industrial facilities, such as factories, commercial facilities, power plants, or other installations where the proper maintenance approach can prevent catastrophic failures. However, maintaining the bottom line requires more. One must also consider reliability, security, power dissipation, fault detection, and properly designed equipment to meet industry standards.

A similar version of this article appeared in German in the November 2012 issue of *Elektronik Informationen*.

Introduction

If you have been in business or industry, you have heard it before: maximize return on investment (ROI) to keep your business healthy and growing. It's a simple goal, but not simple to achieve. To maximize ROI, industrial facilities must be kept running at maximum capacity 24/7/365. "Uptime" is now the mantra, the figure of merit. Not only must cloud servers and critical military security systems meet "five 9s" or "six 9s" ("five 9s" means 99.999% availability which is equivalent to about 5 minutes of downtime per year), but this is now the expectation for factories, commercial facilities, power plants, and any installation where the capital investment and the needs of the community behoove the owners and operators to strive for maximum uptime at maximum capacity.

Downtime Is Loss of Productivity and Revenue

We have all heard the phrase, "time is money." For industrial facilities, it has never been more true. Unexpected downtime in factories can be extremely costly, as loss of output has a direct, negative impact on revenue. Furthermore, an unexpected factory shutdown can cause loss of work in progress (WIP), wasted resources, and potential future losses if a restarted production line does not immediately produce output that meets specifications.[1] Some production facilities take days to stabilize after a restart, before the output product qualifies for release. If the downtime is due to a catastrophic failure, there could be consequential environmental pollution, collateral damage, legal ramifications, injuries, and even loss of life.

In discrete manufacturing, individual items are assembled or fabricated on production lines. This can include anything from cell phones to automobiles. Certainly some of these lines move very quickly so uptime is critical.

Downtime in public facilities can cause different, but similarly detrimental consequences. An airport that shuts down when its lighting system fails would be extremely disruptive to thousands of people.

Equipment Maintenance—Make Uptime 100%

It is thus no surprise that today we, as both the operators of industrial facilities and the patrons of those facilities, expect 100% uptime. To increase uptime and maximize production efficiency, one must choose the highest reliability equipment and implement an appropriate maintenance program to keep that equipment running at peak performance.

Industry typically uses a variety of approaches for equipment maintenance.

Reactive maintenance or “run to failure” offers the lowest initial cost. Basically, no effort is put into maintenance; equipment simply runs until it fails. While this might sound misguided, it has its place in applications where maintenance is either impossible or cost prohibitive, and where the failure mode is predictable and anticipated. Systems with low criticality, some redundant systems, or systems that are unlikely to fail are appropriate for this approach.

Preventive maintenance is the standard method used in many installations, but it is proven to be one of the most costly approaches. Nonetheless, it also has its place. This approach is simply based on time of use, run time, or even more crudely on calendar-time-since-the-last-maintenance activity. A prime example is with automobiles and the use of mileage to determine when to change the engine oil. The approach does not take into consideration the fact that some cars experience much less harsh driving conditions than others. There is a good chance that in most driving scenarios, the oil is being changed sooner than necessary—wasting time, oil, and money. We accept this expense as an “insurance policy” and worth the money due to the lack of an indication as to when the oil really needs changing. That being said, there are many cases where equipment (and its associated lubricants) predictably wears out or down. Erosion and other material property changes can sometimes be directly correlated to service hours or just simply to aging. In these situations, preventive maintenance is warranted.[2]

Predictive maintenance (PdM) or condition-based maintenance (CbM) is effective when failures are generally random or when it is difficult to predict the wearout rate. Both of these approaches are based on tracking condition changes over time. In most cases either of these approaches is more effective than preventive maintenance for increasing uptime while costing less over time. However, the upfront costs to implement are higher since more resources, both human and equipment, are needed to gather the machine condition data and convert it into useful information.

Continuous condition monitoring (CCM) uses permanently installed sensors and data acquisition systems (DASs) to provide the ultimate protection and ensure uptime. The extra equipment cost and the associated training or contracting fees to implement the program equate to a relatively high initial setup cost. Payback comes from the prevention of unanticipated equipment failures. CCM is often the best approach where failures are random in time and where sensors can be installed to detect condition changes that provide the warnings needed to plan shutdowns.

Proactive maintenance is a forward-thinking maintenance philosophy. Central to this approach is the use of the knowledge learned from the maintenance history. By focusing on failure root-cause analysis, changes are put into place to reduce future maintenance needs. The goal here is to ultimately improve the equipment or its operating environment so failures are prevented wherever possible.

Self-maintenance is the most forward-looking approach. Now the machine or system monitors itself; it diagnoses itself and can self-calibrate to continue operation until it is convenient to be brought down. This method requires equipment to have advanced intelligence; self-monitoring of more functions; and to be able to close the loop to implement the adjustments automatically and in the proper amount. Finally, equipment must be able to detect when these automatic adjustment ranges have reached their limit, at which time the machine requests maintenance, with some time allotted for a response. The result of self-maintenance is obviously more uptime. These systems are already in place on some equipment. Higher-end automobiles, for example, can now indicate the condition of engine oil, based on *sensing* the real oil condition and not merely on monitoring a record of engine run time. It is only a matter of time when the additional cost of these capabilities will be justified for more industrial equipment.

Reliability-centered maintenance (RCM) draws from all of the above maintenance types with the realization that different approaches are appropriate for different equipment and different usage in the specific installations. The focus here is on the optimal combination of maintenance approaches to maximize plant efficiency.

The Importance of Reliability, Robustness, Safety, and Security

Equipment maintenance is not the whole story for industrial uptime and the consequent improvement to the bottom line. In some cases the cost of maintenance operations is not what drives decisions about uptime. In batch processes such as brewing or pharmaceuticals, for example, maintenance can be performed between batches. However, it can be extremely expensive or, more importantly, dangerous for a process to go down in the middle of a batch. This is when safety monitoring equipment and fail-safe systems become critically important for system uptime.

In production facilities equipment can be exposed to many common environmental conditions: high-voltage transients, cable damage, miswiring during modifications or repairs, extreme temperatures, harsh electromagnetic interference (EMI)/radio frequency interference (RFI), corrosive or explosive atmospheres, high vibration, humidity, and dust. If these conditions compromise the accuracy of the equipment sensors and the sensor signal-conditioning electronics, then false readings or erroneous control signals are possible. This can lead to, at best, inferior results and, at worst, catastrophic failures. These are issues that clearly go beyond normal equipment maintenance.

In industrial situations when redundant systems cannot be justified, a high-reliability system must be designed. During the equipment design and development process FMEA (failure mode effects analysis), FMECA (failure mode effects and criticality analysis), or FMEDA (failure mode effects and detection analysis) can be used to assure that all failure modes have been anticipated.[3] A passing result from an FMEA confirms that the system detects, properly responds to, and reduces the criticality of every possible failure in the system. Industry standards such as IEC 61508 also apply to equipment used to carry out safety functions, such as some programmable logic controllers (PLCs) used to monitor and shut down a dangerous process when a problem is detected. These requirements often lead to additional electronics to monitor the original signal path or power system. This is all well and good for reliability, robustness, safety, and security, but this added circuitry exacerbates the ever-present challenge to shrink the size, reduce its power consumption, and ultimately, simplify the design.

Self-Monitoring Circuits Increase Industrial Uptime

By implementing self-monitoring features on ICs, new devices can flag problems to alert the system that an anomaly has occurred. The response to these warnings is at the discretion of the system programmer or operator, but at least the data on the event was captured. New power-management ICs are, moreover, reducing power consumption wherever possible. Reference designs for these highly integrated solutions reduce the design time needed to get to market quickly. Let's consider some examples.

Example: Low-Power Industrial Digital-Input Serializer

A common problem today is that digital-input modules must dissipate significant amounts of power to be able to handle 24V signaling levels. When one tries to shrink these modules, the power dissipated in the enclosure leads to heat buildup and, therefore, limits the maximum operating temperature range. Meanwhile, if the equipment is placed close to the machine, a high operating temperature range is required. That, in turn, requires a lower power solution.

The MAX31911 industrial, octal, digital input translator/serializer reduces the power dissipation in input modules by up to 60% compared to the traditional discrete resistor-divider approach. It meets the IEC 61131-2 PLC standard for digital inputs types 1, 2, and 3. It serializes the eight inputs and translates them to CMOS-compatible 5V levels. Adjustable lowpass filtering enables flexible debouncing. The serial SPI output reduces the number of optocouplers for further power, size, and cost reduction. To assure valid data on the SPI interface, a CRC code is generated for each 8 bits of data. A similar device, the MAX31910, provides an even lower power input using advanced techniques. This device lowers power consumption by up to 40% over the already low-power MAX31911.

For systems with more than eight inputs, multiple MAX31910s and MAX31911s can be easily daisy chained. **Figure 1** shows a 16-channel solution using two MAX31911s. Notice that no additional isolation channels or SPI chip selects are needed.

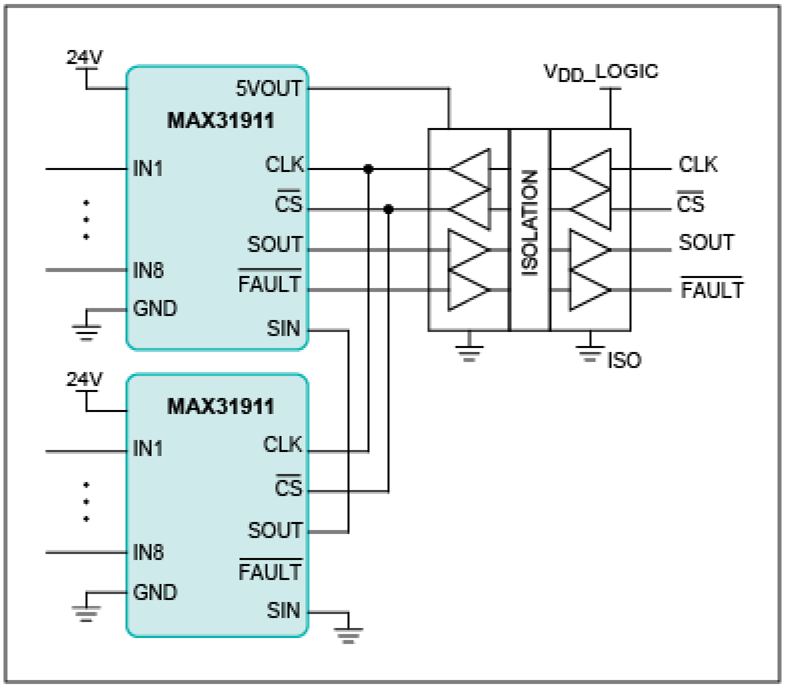

Figure 1. In a daisy-chain configuration, external components used to enhance EMC robustness do not need to be duplicated for each device on a circuit board. A 16-input application circuit is shown here.

With any parallel-input to serial-output system, the first question is, “How fast can it sample the input channels while maintaining valid data and throughput?” The fastest mode is to select no debounce. At 0s debounce, there is no filtering so the outputs of the eight internal comparators are latched into the serializer on the falling edge of chip select (CS). Every clock edge thereafter will clock out 1 bit corresponding to each input. In this case, speed is limited by the input bandwidth which is 1MHz, so clocking the serializer at 8MHz will deliver 1Mbps throughput per channel (in 8-bit mode). If four chips are daisy chained for a 32-input application, now the maximum clock speed of the serializer will limit throughput. This is because clocking 32 bits out of the serializer at the maximum SPI clock rate of 25MHz gives a throughput per channel of 25MHz/32 = 0.8Mbps (instead of 1Mbps in the previous example). If filtering is enabled, throughput will be further limited by the debounce time used.

To support industrial applications, the MAX31911 has built-in high ±15kV ESD protection (HBM) on all field inputs and is rated for operation up to +150°C junction temperature. It comes in a 6.5mm x 9.8mm x 1.1mm, 28-pin TSSOP-EP package.

Example: Secure Coprocessor and Secure Authenticator

The trend toward Internet-connected industrial equipment offers many benefits, but the added security risks are real. Indeed, cyber warfare is a real threat to uptime and the bottom line.

New security solutions need to provide silicon level, standards-based encryption, authentication, and secure key storage that do not require a human to follow complex data handling rules and procedures to maintain facilities firewalls. New solutions from Maxim Integrated prevent unauthorized communications, and they encrypt communications exposed to the world outside the IC. They actively respond to a long list of physical and electrical attacks. The risk of infections from malware, the risk of theft of encryption keys, and the risk of cloning authorized equipment are greatly reduced. These proven solutions have been in use for years in automated teller machines and point-of-sale (POS) terminals, successfully protecting financial transactions and personal identities. With these secure devices built in, hacking into a system is virtually impossible.

We can examine a new SHA-256 authentication solution composed of two ICs: the DS2465 secure coprocessor for the master, and the DS28E15 1-Wire® SHA-256 secure authenticator for the slave device. They communicate over a single wire, and they enable a challenge/response authentication process. The algorithm rejects any newly connected module that does not calculate the proper result; the only way to calculate the proper result is to know the internal secret key. Both the master and the slave need to use this key in the hash algorithm along with a random number challenge. If the challenge-and-response results are not identical, the authentication fails and the newly connected device is prevented from communicating.

The DS2465 has a built in 1-Wire master that handles the 1-Wire bus timing. It also provides user EEPROM and the crypto-industry-vetted SHA-256 hash algorithm so the system host processor is unburdened from these tasks. A simple I²C interface connects it to the host. The 1-Wire IO line has high ±8kV ESD protection (HBM) and the device is rated for operation from -40°C to +85°C. It is packaged in a small 4.0mm x 4.45mm x 1.5mm, 6-pin TSOC package.

The DS28E15 combines secure challenge-and-response authentication based on the FIPS180-3 Secure Hash Algorithm (SHA-256). It has 512 bits of user EEPROM and additional secure memory holds the secret key. Every device has a unique 64-bit ROM ID number factory programmed into the chip. No two devices will ever be alike. A secure, low-cost factory service is available to preprogram device data, including the secret if desired. A variety of different methods exist to keep the secret under complete control, even in contract manufacturing environments. **Figure 2** shows how simple the implementation is.

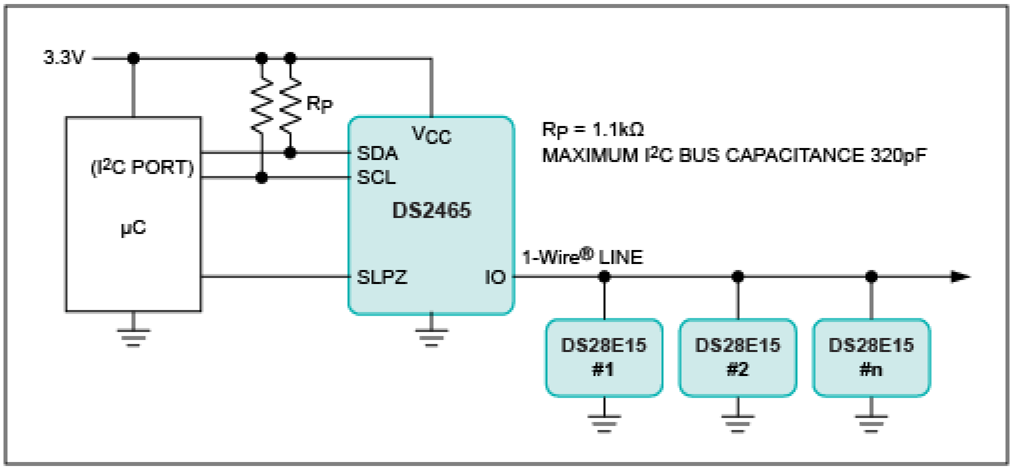

Figure 2. Typical implementation of the DS2465 SHA-256 coprocessor and three DS28E15 secure slaves on the 1-Wire bus.

In Figure 2 each slave device needs only a single DS28E15 imbedded in it. When connected to a host, the challenge/response process is initiated. Only when the correct result is calculated by the slave, will the module be allowed to communicate with the master.

Conclusion

There is a critical need to maximize uptime in process automation, building automation, and motor control applications to help maximize the bottom line. A variety of maintenance methods discussed here help in this regard. Nonetheless, equipment maintenance alone will not let plant operators achieve the maximum uptime nor ensure the optimal safety and security of their operation.

This is where, and how, equipment designers play an important role. We need to keep uptime, safety, and security goals in mind when developing products for the industrial market. When highly integrated solutions like those discussed above are available to industry, they definitely reduce the cost, complexity, size, and power consumption of systems. Ultimately, these integrated systems become integral to helping our customers increase their uptime. And that protects the bottom line.

References

1. A 1992 survey of 450 Fortune 1000 companies, conducted by the Strategic Research Division of Find/SVP, found that downtime costs U.S. business over $4 billion per year. The equivalent number for that downtime today would be staggering. For more background information, go to www.manageinc.com/itera.php.
2. The U.S. Department of Energy's "Operations and Maintenance Best Practices" manual states that the savings realized by moving from reactive maintenance to preventive maintenance can amount to 12% to 18% on average. See https://www1.eere.energy.gov/femp/pdfs/OM_5.pdf.
3. For general background information, go to http://en.wikipedia.org/wiki/Functional_safety.

1-Wire is a registered trademark of Maxim Integrated Products, Inc.

Related Parts		
DS2465	DeepCover Secure Authenticator with SHA-256 Coprocessor and 1-Wire Master Function	Free Samples
DS28E15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples
MAX31910	Industrial, Octal, Digital Input Translator/Serializer	Free Samples
MAX31911	Industrial, Octal, Digital Input Translator/Serializer	Free Samples

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 5518: http://www.maximintegrated.com/an5518
TUTORIAL 5518, AN5518, AN 5518, APP5518, Appnote5518, Appnote 5518