Reducing Downtime for Hazardous Area PC Controllers

Daniel Liu
Project Supervisor

Kyle Pearson
Technical Writer

MOXA®

Executive Summary

IPC platforms are becoming increasingly popular in remote process control automation; however, traditional PC platforms are not engineered to the standards required by industrial networks. Consequently, when building IPC platforms for industrial control, the first hurdle engineers encounter is how to ensure the high reliability and data security demanded by industrial systems. This is a challenge because IPCs were originally designed and engineered for use in enterprise networks, where the consequences of system failure are much less severe. Thus, reducing or eliminating the system downtime that is so common in enterprise networks is the first concern for automation engineers who are considering IPCs for their network.

The Benefits and Problems of IPC-based Automation

Over the past few decades PCs were only suitable for use in SCADA systems, where the mild conditions of comfortable, climate-controlled offices could be guaranteed. But as Ethernet technology has advanced, the opportunity to build distributed control networks using relatively inexpensive IPCs has become a valuable alternative. The result is that today, IPCs are displacing PLCs and RTUs from industrial control systems. One of the advantages IPCs bring is a significant increase in processing power. Increased efficiency in a production system typically means more and more information must be acquired and analyzed, and that translates into a significant increase in data rates. The only way to achieve high speed, front-end data collection and analysis is with a faster CPU. Thus, one key value point that distinguishes IPCs is the increased processing performance they offer relative to RTUs and PLCs.

These increases in efficiency come with a price, though: where IPCs' high processing power makes them a useful application for device control, it also significantly increases the complexity of the platform, so that slowdowns and failures become much more likely. Yet, in remote automation systems—and especially in oil and gas processing control—any failure incurs heavy costs, and if IPCs are installed in remote systems at the device layer then they are naturally beyond the timely reach of system maintainers. For these reasons, whenever IPCs are considered, downtime prevention is the foremost topic in mind.

In enterprise systems, recovery of lost data or crashed devices may be accomplished using redundant drive arrays (RAID), backup system images, or some other rescue and backup mechanism. Following a crash, however, most of these methods require operator intervention to start a recovery, and additionally none of these approaches prevent cumulative slowdowns, or system failure. In contrast, most of the devices that comprise automated oil and gas control

Released on May 15, 2013

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa's solutions is available at www.moxa.com. You may also contact Moxa by email at info@moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®
Reliable Networks ▲ Sincere Service

systems are located remotely, far afield, and require much stricter failsafes and guarantees than enterprise devices can provide.

Process control for oil and gas systems is so widely distributed that all networked devices must meet strict stability and reliability requirements even without operator presence. One powerful tool that can help guarantee that is an automated OS backup and recovery system. Unfortunately, these tools are mainly useful only after failure has already occurred; ideally, all failures should be prevented with such timely maintenance and oversight that process controls would never crash. But how can that be achieved?

Remote Management and Self-Diagnosis Using PC-Based Controllers

The solution to this problem requires only a few relatively simple steps, and result in increased system reliability and overall uptime:

1. Automate regular system cleanups with full OS rewrites.

Everyone who has ever spent a lot of time using computers has experienced how performance cumulatively drops and the system slows down over time. In an automation system, slowed performance means reduced yield, so to maintain system efficiency an IPC should be able to restore itself to a pristine state according to a preset schedule.

2. Hardware failures increase in hazardous environments, so critical components need to be monitored.

Rough environments are commonplace for remote oil and gas control systems. Very high and very low (sub-zero) temperatures, high humidity, corrosive sedimentation, and electrical interference all expedite the aging process. To make sure the system administrator can address system instability before the system crashes, hardware health indicators must be monitored and made remotely available for use in predictive maintenance.

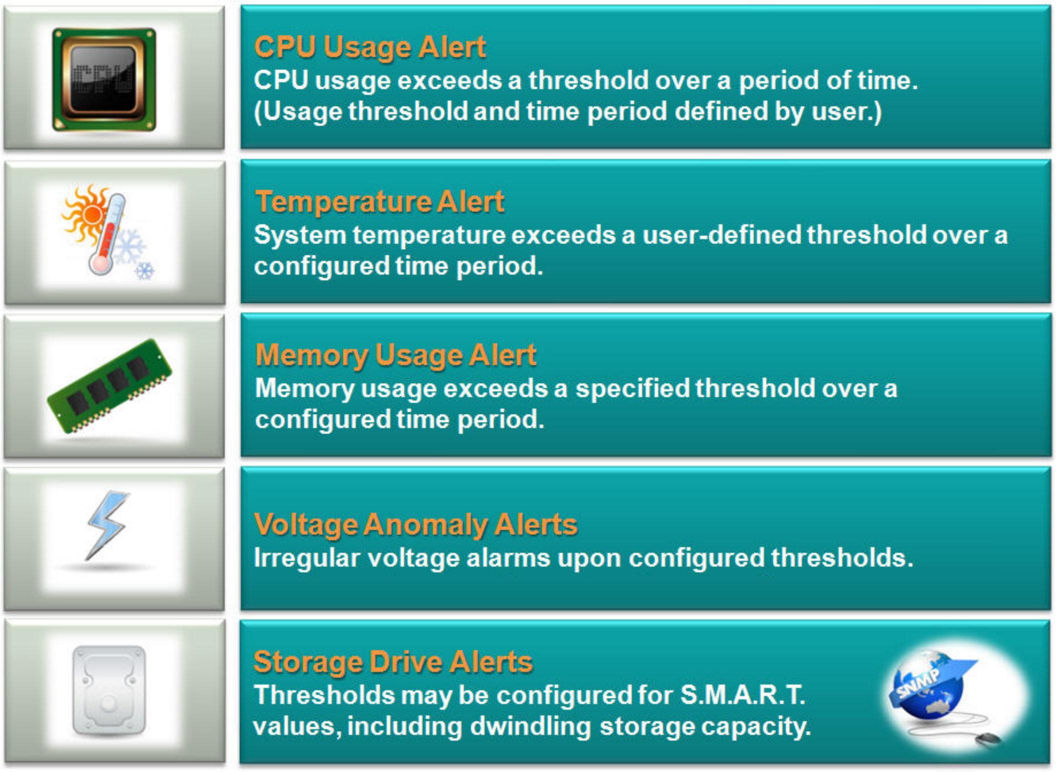
3. Use IP communication for remote triggering of the IPC’s self-healing process.

In the past, when IP technology was alien to industrial control networks, most automation systems relied on hardware and software watchdogs to do hard resets to restore the system. There was little a system administrator could remotely see, or do. Normally, to diagnose and fix a problem an engineer had to be physically present at the site; of course, sending an engineer to an offshore platform or remote pumping station incurs high expense, and repair times can be measured in days. Today, however, IP communication allows engineers to both constantly monitor an IPC’s health, and to remotely trigger OS re-writes to a tagged disk image created when the IPC was confirmed to run normally and efficiently.

None of these methods are new to the computer world, but when put together into a ready-to-run software application this trio of automated monitoring and recovery features constitute a powerful weapon in the fight to ensure a control network's reliability. To integrate these features, a solution is required that will run not only as an application, but also as a background system process. One protocol that is already widely used to achieve this in remote automation networks is the Simple Network Management Protocol, or SNMP

SNMP as a Remote IPC Management Interface

SNMP was originally created for IT personnel to monitor process efficiency and hardware status on network nodes like routers, switches, and power sources. Yet in the last decade it has also aroused the interest of traditional automation engineers, for a variety of reasons.



CPU Usage Alert
CPU usage exceeds a threshold over a period of time. (Usage threshold and time period defined by user.)

Temperature Alert
System temperature exceeds a user-defined threshold over a configured time period.

Memory Usage Alert
Memory usage exceeds a specified threshold over a configured time period.

Voltage Anomaly Alerts
Irregular voltage alarms upon configured thresholds.

Storage Drive Alerts
Thresholds may be configured for S.M.A.R.T. values, including dwindling storage capacity.

1. First, the protocol is open and free, and is readily available to everyone. This is in contrast to most of the Fieldbus protocols, which are typically owned by a vendor who has set a price that puts them beyond the budget of many operators. SNMP is, instead, an effective, inexpensive protocol.
2. SNMP carries a light memory footprint while supporting active reporting ("traps"), making it ideal for remote data acquisition where network bandwidth is a concern. The innovations that came with SNMP v2 allow SNMP agents to return active reports to the network management software (NMS) upon operator-configured exceptions. These active reports are called SNMP traps, and they give SNMP a powerful alarming capability.
3. SNMP v3 supports data encryption, a critical feature for data that must travel across public WANs. Because they were created for LAN applications, encryption is not available on most Fieldbus implementations.
4. SNMP is a protocol that has grown in step with IP technology, being keenly honed with every passing generation. The prospects for SNMP are bright, compared to traditional Fieldbus technology.
5. Finally, there is a wide variety of readily available SNMP-compatible network management software (NMS). Many of these implementations are cheap while others are even free,

giving industrial control engineers an economical and effective means of monitoring field equipment.

In Summary: Expanding SNMP into a Remote IPC Management Tool

With IPCs so widely used in so many different automation roles, industrial control engineers will clearly find a remote management system that combines both monitoring and control a valuable—perhaps critical—feature. A fully automated system can be made intelligent by empowering remote IPCs with self-diagnostic routines that utilize SNMP to access diagnostic data, receive alarms, and to trigger recovery tools whenever system resets are required. All of these indicators are readily available using standard SNMP polling.

Disclaimer
This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied by law, including implied warranties and conditions of merchantability, or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document.