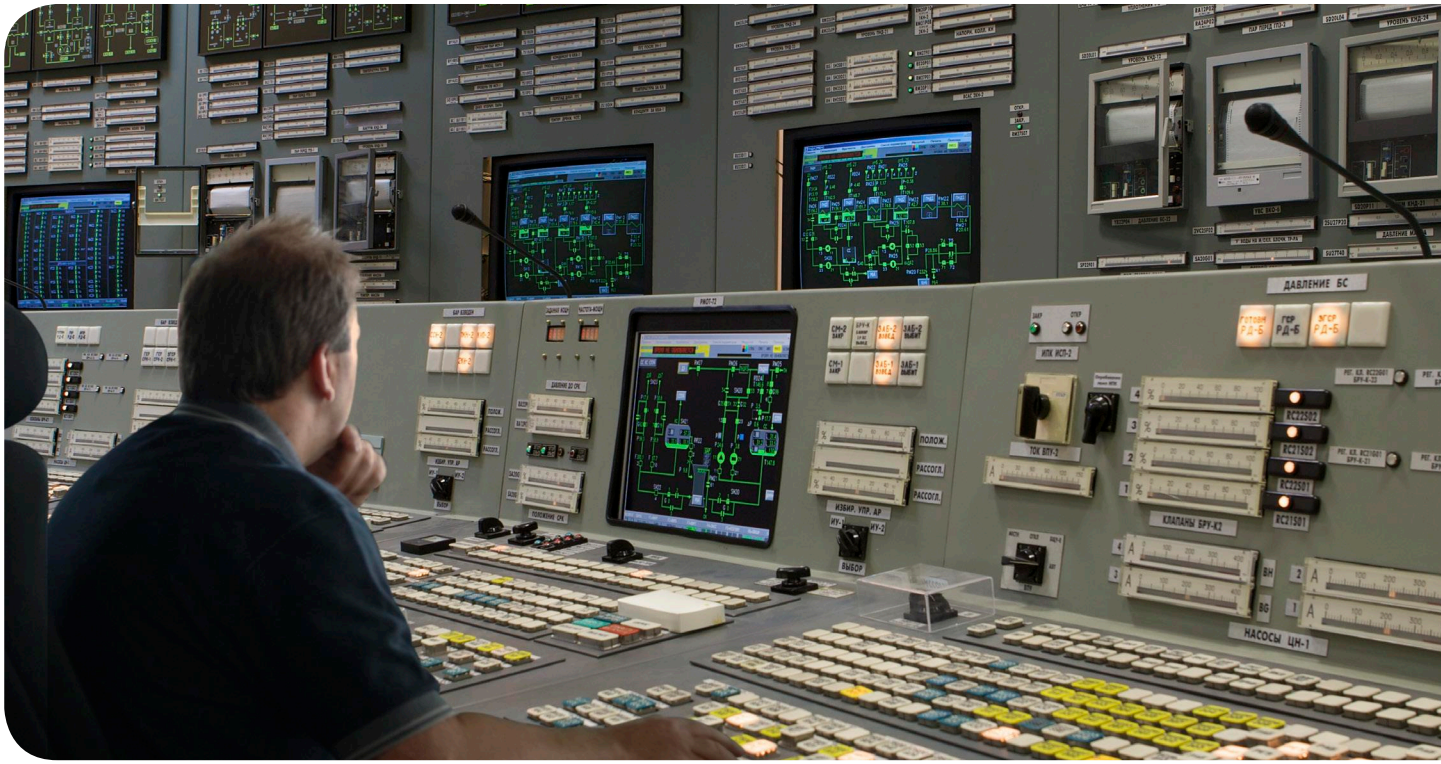

White Paper

Maximize Uptime in the Connected Factory

Securely Connect and Manage Equipment with NEXCOM XCare and McAfee Solidcore

By Joe Lin, General Manager, Industrial Computing Solutions, NEXCOM

www.nexcom.com

Reliable operation of machinery is key to productivity in the factory. However, monitoring the many devices that keep today's production lines running in optimal condition is a major challenge, especially when the machines are widely dispersed in different factories.

The Intel® Intelligent System Framework was created to address this challenge. This specification gives developers a standards-based, interoperable platform for connectivity, security, and manageability. Using the framework, an automation controller cannot only control manufacturing equipment and its subsidiary systems but also communicate with the supervisory control and data acquisition (SCADA) system in a factory's central control room and with a headquarters office. With this connectivity, factory operators and supervisors can closely monitor daily operation and perform predictive maintenance and real-time diagnostics remotely, simplifying machinery management and maximizing operation uptime. In the meantime, enterprise executives can apply business insights to production plans and make real-time adjustments accordingly.

Using the framework, NEXCOM has developed the NISE 3640 fanless computer that brings together the 3rd generation Intel® Core™ processor, NEXCOM XCare remote monitoring and management software, and McAfee Solidcore security software. This article will explain how the combination of computing and graphics power with cutting-edge connectivity, manageability, and security enables the NISE 3640 to be used as a control and communication gateway that links cross automation hierarchy levels to monitor and control the devices connected to it in real time, enabling the integration of industrial automation and information technology.

The Central Problem

It is the universal goal of factory operators to reduce the frequency and duration of maintenance. Modern factories can meet this need with a combination of automation controllers that run local machinery, and SCADA systems that enable factory-wide management. Together these systems enable predictive maintenance and real-time diagnostics. Both automation controllers and SCADA systems can benefit from industrial computers built on the 3rd generation Intel® Core™ processor family, such as the fanless NEXCOM NISE 3640 (Figure 1).

These processors integrate powerful Intel® HD Graphics, which offer up to 60 percent better 3D graphics performance than their predecessors, along with new support for DirectX 11. The processors can also drive three independent displays without a discrete graphics card, a considerable advantage with a SCADA system that uses multiple monitors.

Compute power has also been significantly upgraded. Vector processing (such as image processing) is up to 2x faster than the previous generation with Intel® Advanced Vector Extensions (Intel® AVX), which provides 256-bit floating point processing. In addition, overall compute power is increased by 15 percent over earlier processors thanks to enhancements such as the 22 nm process technology with a novel 3-DTri-Gate transistor design. For an automation controller used in machine vision, the improved computing power can translate into more accurate motion control, faster inspection speed, and higher defect coverage, bringing real gains in productivity to machinery

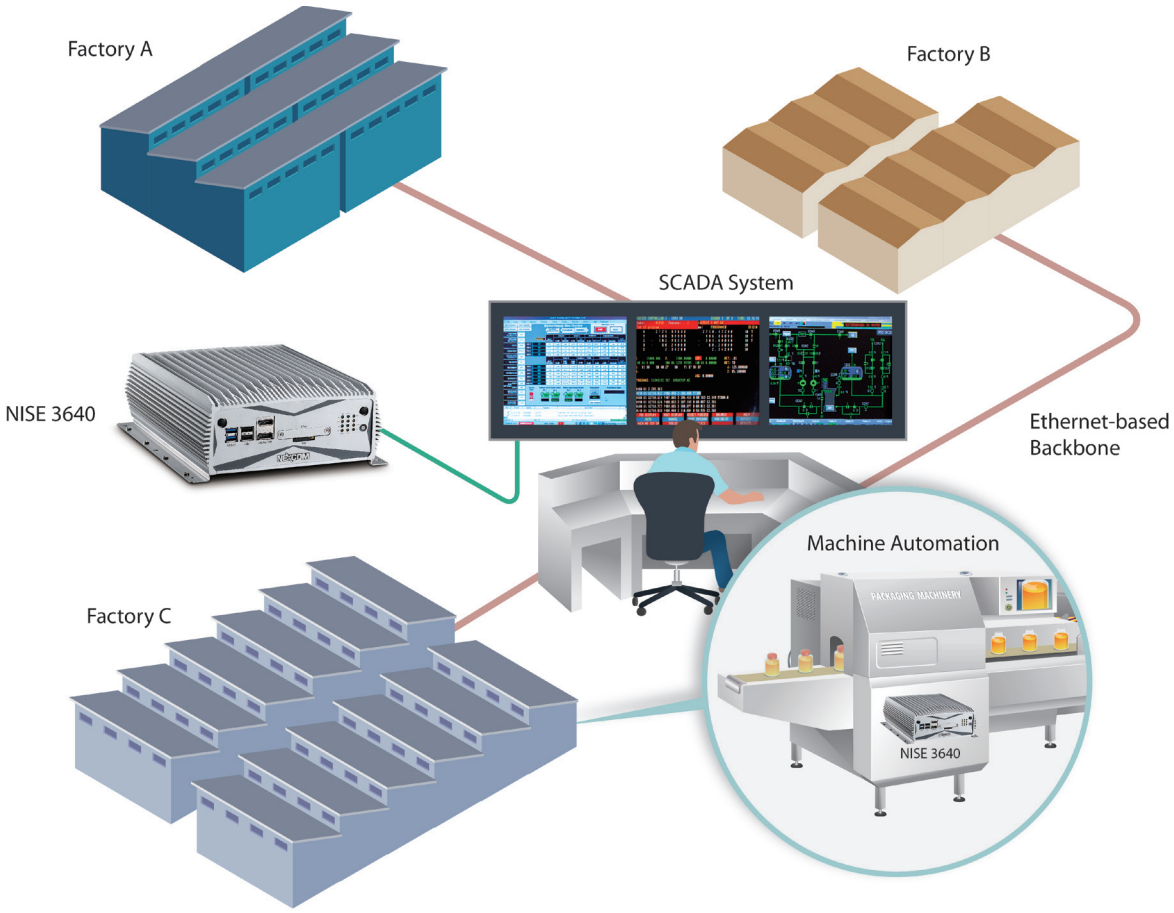

Figure 1. The connected factory enables predictive maintenance and real-time diagnostics remotely. The NEXCOM NISE 3640 can be used in both automation controllers and SCADA systems.

ranging from label printing to automated optical inspection (AOI) machines.

In addition to running the manufacturing process, an automation controller will acquire, process, and analyze the captured images and send the results to a SCADA system. The SCADA system will record and further process the field data, and compile the results into a sophisticated factory-wide graphical user interface that includes 3D graphics, trend curves, alarms, and periodic reports on multiple large screens. This information can help a factory operator monitor the operational status of machinery without onsite visits.

If an automation controller reports an above-average false call rate—that is, if it is detecting non-existent flaws—a factory operator will be informed and empowered to take corrective action. Better still, if an above-average false call rate occurs as a result of faulty equipment with an aging part or a vision tool that is out of specification, a SCADA system enables a factory operator to notice an escalating false call rate and fix the problem before an expensive failure occurs. In comparison with machine inspection at fixed intervals real-time remote monitoring makes possible prompt and immediate responses, saving the time and cost associated with machine downtime and increasing management efficiency.

Connectivity

While the benefits of this remote monitoring are clear, adoption has been hindered by the extraordinary fragmentation of the industrial device market. The proliferation of unique and proprietary hardware, communications protocols, and software stacks have made it difficult to connect the factory.

The Intel Intelligent Systems Framework can solve this problem by specifying a set of capabilities for hardware, operating systems, and software designed to address connecting, managing, and securing devices in a consistent and scalable manner. The framework can scale across applications, reducing fragmentation and speeding time-to-market.

A range of framework-ready solutions are available today from the Intel® Intelligent Systems Alliance, a global ecosystem of 250+ member companies that collaborate closely with Intel and each other to innovate with the latest technologies. For example, NEXCOM XCare is compatible with other framework-ready Alliance software including Wind River® Linux, Microsoft® Windows® 7, Microsoft® Windows® Server 2008, and McAfee® Embedded Control. These components support the defined framework capabilities, allowing developers to focus on advanced features instead of basic functionality. (NEXCOM, McAfee, Microsoft, and Wind River are all Associate members of the Alliance.)

Under the framework, manufacturing equipment on the factory floor can communicate smoothly with the SCADA system in the control room. With access to real-time status, operators can indentify early indicators of potential problems and analyze the root cause of an existing condition. Operators can reschedule planned maintenance if it is not necessary, or devise a corrective action before taking a field trip to minimize the time and effort needed onsite. As a result the frequency, duration, and the manual effort involved in maintenance can be reduced.

Of course, remote monitoring and control of hundreds of geographically distributed intelligent machines—each with numerous sensors—involves moving and processing a great deal of data in near real time. The NISE 3640 is able to handle the load through the integration of fieldbus and a total of four Gigabit Ethernet ports. With the integrated fieldbus, the NISE 3640 provides assured hardware compatibility with field devices such as programmable logic controller (PLCs). The Ethernet enables forwarding of raw data from factory floors to a SCADA system and to a headquarters office. To ensure a reliable connection, a LAN teaming feature is supported to enable automatic failover and to prevent data loss. The NISE 3640, as a typical M2M solution, also supports wireless connections including Wi-Fi and 3G connections to adapt to different installation environments.

Manageability

So far we have focused on the importance of using industrial computers to maintain equipment. However, it is just as important to ensure that the industrial computers themselves are properly maintained. With that goal in mind NEXCOM has developed XCare, which integrates software applications, API, and a cloud server to support remote monitoring and management of the NISE 3640 and other NEXCOM products (Figure 2).

The four main features of the XCare include hardware status check, system restore, remote keyboard/ video/ mouse (KVM), and remote configuration.

First the hardware status check keeps track of the processor, RAM, BIOS, operating system, system temperature, voltage, hard disk drive, and network connectivity. Second, the system restore can automatically reboot the system, recovering it from a locked-up state. Third, the remote KVM helps a factory operator to upgrade and upload drivers, patches, OS, and applications, as well as to perform troubleshooting. Finally, GPIO configuration and hardware alarm setting can also be set remotely.

XCare enables cost-effective remote management of networked embedded systems. IT personnel can discover, maintain, and protect networked embedded systems, without incurring the expense of onsite support.

XCare can simplify maintenance and increase equipment uptime. For example, XCare can detect an underperforming hard disk drive and show an onscreen alert (Figure 3). An informed factory operator can take advantage of remote KVM to perform system backup, bring the replacement to the factory floor on the first visit, and therefore prevent potential manufacturing equipment breakdown. For glitches that can be solved by system reboot, system restore is a time- and cost-saving method that doesn't requiring the physical presence of a factory operator.

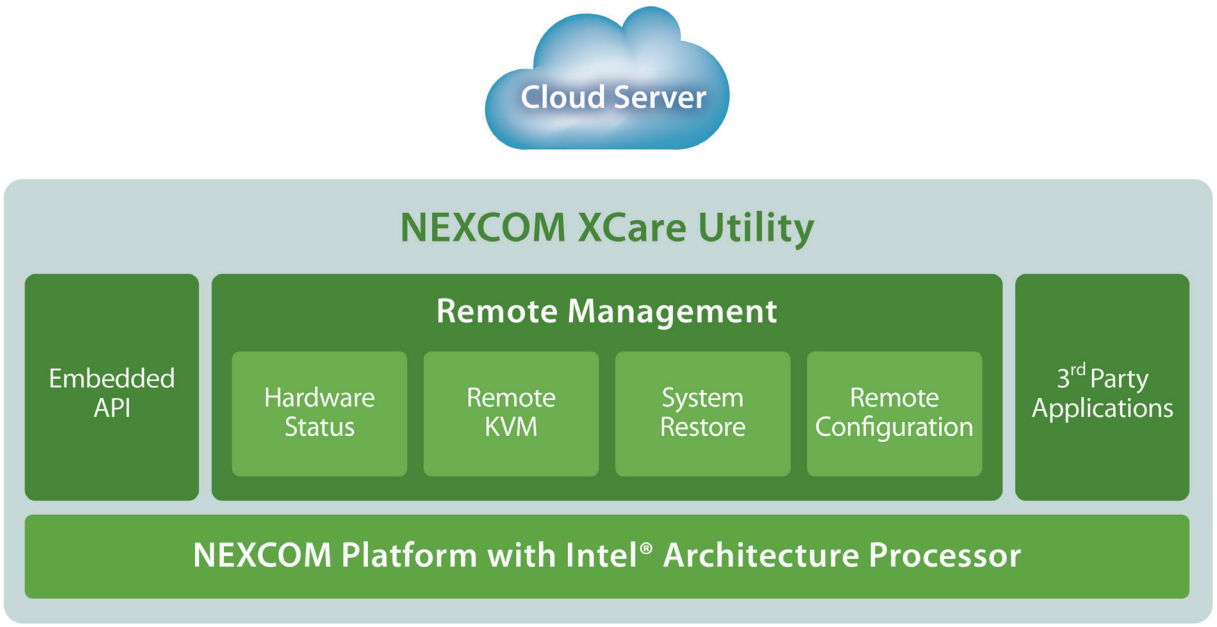

Figure 2. NEXCOM XCare integrates software applications, API, and a cloud server.

Security

A connected factory is only as strong as its weakest link, so every connected client in the factory needs protection from viruses, malware, and hacking in order to prevent costly interruptions to factory operation. To alleviate such security concerns, XCare's support for McAfee Solidcore integration is intended to

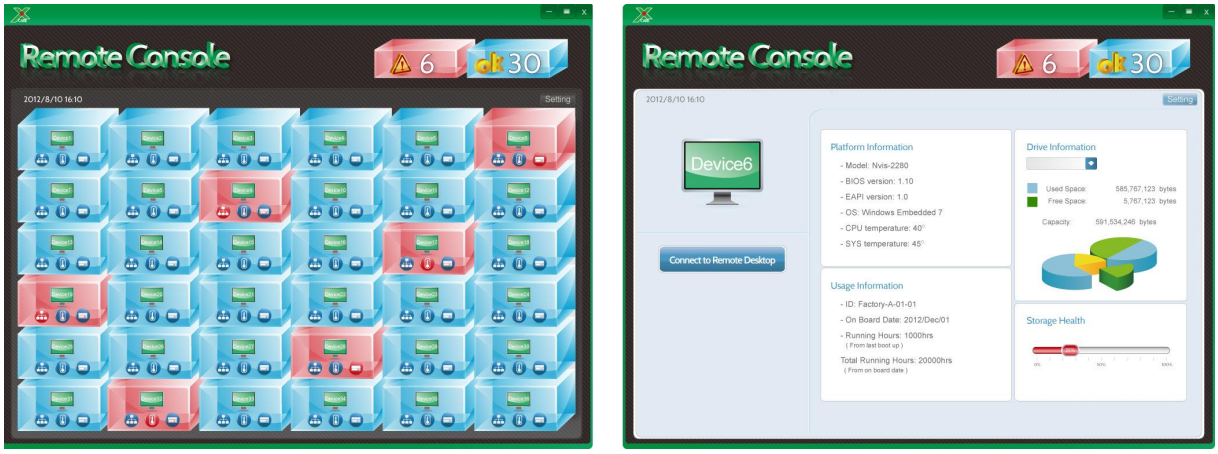

Figure 3. NEXCOM XCare gives alerts on issues across the factory (left). Operators can zoom in on individual systems (right) to quickly investigate and repair problems.

block unauthorized applications and changes to automation controllers and the SCADA system.

McAfee Solidcore includes Application Control and Change Control. Application Control adopts a whitelist approach to managing zero-day threats. This approach only allows applications in the whitelist to be installed and to run while blocking the rest. By preventing the installation and execution of unauthorized applications, risks from worms, viruses, spyware, and other malware can be reduced and failed attempts will be logged.

Change Control adopts change policies to prevent unwanted changes and to ensure file integrity. Change Control can detect, verify, and authorize changes to be made. Unauthorized modification to a file made by unauthorized personnel during an unauthorized time will be blocked. Change Control gives strong control over mission-critical devices such as manufacturing equipment.

The integration of XCare and McAfee Solidcore provides remote real-time monitoring on both hardware and security threats. For example in the case of a suspicious spike in network workload on an NISE 3640 a factory operator will be alerted to check the event log generated by McAfee Solidcore to monitor a possible ongoing malicious attack.

Secure Remote Control

Effectively monitoring, controlling, and connecting machinery that may be several time zones apart is a serious and growing challenge. NEXCOM has found that the Intel Intelligent System Framework provides a stable, secure, and extensible structure on which to design a remote monitoring and control system that can handle many types of devices. The 3rd generation Intel Core processors with integrated Intel HD Graphics—in combination with NEXCOM XCare and McAfee Solidcore software—enable the NISE 3640 to monitor and control the devices connected to it in real time, even when they're half a world away.

The article is also published in the April 2013 issue of Intel Embedded Innovator Magazine.

About NEXCOM

NEXCOM International Co Ltd. is an Associate member of the Intel® Intelligent Systems Alliance. Founded in 1992, NEXCOM has five business units which focus on vertical markets across industrial computer, in-vehicle computer, multimedia, network and communication, and intelligent digital security industries. NEXCOM serves its customers worldwide through its subsidiaries in seven major industrial countries. NEXCOM gains stronghold in vertical markets with its industry-leading products including the rugged fanless computer NISE series, the in-vehicle computer VTC series, the network and security appliance NSA series and the digital signage player NDiS series.

About the Intel® Intelligent Systems Alliance

From modular components to market-ready systems, Intel and the 200+ global member companies of the Intel® Intelligent Systems Alliance provide the performance, connectivity, manageability, and security developers need to create smart, connected systems. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies,helping developers deliver first-in-market solutions.

Learn more at: intel.com/go/intelligentsystems-alliance