Determining if an embedded system will operate securely in the field as shipped can be difficult to accomplish as standardization has allowed devices to become more interconnected and thus more open to security, software control, and compliance pitfalls. Change control software can help overcome these challenges by giving device manufacturers greater jurisdiction over what software gets changed on an embedded system.

Technology is revolutionizing every industry, from retail to health care to finance. The need for reduced time to market and advanced hardware/software technologies is driving the embedded systems market, including devices such as Point-Of-Sale (POS) terminals, self-checkout terminals, point-of-care medical modalities, ATM machines, thin client computers, and gaming systems, to create a richer customer experience while keeping the total cost of ownership low.

While embedded systems of the past used specialized hardware running proprietary software, a shift has been made toward standardizations such as Unified Point-Of-Sale (UPOS) in the retail industry. Standardization has enabled devices to become increasingly interconnected and allowed off-the-shelf software to be used in commoditized hardware running commercial or open Operating Systems (OSs) such as Windows XP Embedded, Windows Embedded for Point of Service, and Linux. Both these standards and general-purpose OSs have provided greater flexibility for software selection, faster time to market, and midcycle adoption of new technologies.

Yet this flexibility has come at the expense of security, software change control, and compliance challenges associated with these difficult-to-service embedded systems. Similar to a PC in a networked environment, today’s embedded devices are susceptible to security risks, constant patching, and performance-draining antivirus software applications. Embedded systems also have become vulnerable to unauthorized and inappropriate changes as they flow through a typical multiparty distribution channel, which often results in field breakage. These factors can lead to noncompliant devices operating in the field. Figure 1 illustrates how increased functionality is creating the need for more control.
Until recently, device manufacturers did not have control over what software is installed and who installs it after the device leaves the manufacturing process, leaving no way to ensure the device will continue to work in the field as shipped.

Controlling the production image
When installed as a foundation of an embedded system, change control software controls what software can change and how, when, and by whom it can be altered as well as what software can run based on authorized change control policies and procedures. It ensures that only the changes done by approved and authorized change control procedures get added to the production software image of the embedded system. This includes in-process approved and documented changes and undocumented emergency changes. It automatically denies any ad hoc, unapproved, undocumented changes that may be done via internal unapproved administrator changes, or attacks or external malware, including zero-day attacks (see Figure 2).

Change control software is a low-footprint, low-overhead piece of software that runs transparently on an embedded system. It generally is installed and set up quickly with low initial and ongoing operational overhead and is designed to lock down or harden a device’s gold base image certified by the device manufacturer. Change control allows device builders and manufacturers to dictate the degree of flexibility given to the distribution channel, which translates into greater control over what is installed on an embedded system once in production.

Change control technology offers the capability to enforce what is installed, uninstalled, upgraded, or modified to the base software image of a networked device in production in two distinct workflows. First, the software provides control as a device flows through its multistage manufacturing life cycle and as various channel vendors attempt to install their own software. Second, it controls the state of a device once in production to ensure operational maintenance and support are conducted in accordance with the device manufacturer’s policies.

No need for antivirus
From a security perspective, change control helps manage what can run, providing protection against existing and unknown zero-day polymorphic threats. By acting as a “concrete wrapper” around the gold base image of an embedded system, change control software can ensure a device in production is secure and cannot be compromised. And because changes attempted by malicious code or unauthorized users are prevented, the need for antivirus and other security software packages is eliminated. This lock-down mode cuts down on emergency patching, reduces the number and frequency of patching cycles, and allows more time for testing before patches are deployed to in-production systems.

Patch systems on schedule
The runtime control element of change control software can help minimize operating costs by reducing both planned patching and unplanned recovery downtime, thereby
increasing device availability. This often becomes an ideal feature for difficult-to-service, remote, and lower-margin devices running vulnerable commercial OSs and applications. The capability can lower support costs by reducing the number of touch points needed.

[Editor’s note: Solidcore Systems, Inc. recently announced the creation of an embedded change control advisory council. Members include representatives from Microsoft, NCR, Confirma, NEC, StoreNext, and Wyse Technology. The advisory council will help drive new innovations in change control and work to accelerate the adoption of standards for controlling change on embedded systems in diverse vertical markets.]

Case study: locking down POS systems
NEC Infrontia (NEC-i) is one example of change control software implementation. The POS device manufacturer wanted to provide an enhanced customer experience with its devices by building Windows XP Embedded-based POS terminals. However, because these devices were more highly networked and dependent on general-purpose OSs, they became more vulnerable to unauthorized changes and constant patching. NEC-i also faced a significant performance drain on its POS devices because of antivirus software running on the systems.

To alleviate these problems, NEC-i built devices with change control from Solidcore as the foundation, which enabled the company to transparently control devices as they passed through multiple dealers. With change control installed at the heart of these systems, NEC-i prevented unauthorized code from breaking unpatched systems and removed the antivirus software that was diminishing its devices’ performance.

Foundation for better management
Change control is quickly becoming a new standard to ensure embedded device uptime and reduce support costs. By providing complete command over what is allowed to change on the device, change control is proving to be a beneficial tool for embedded device manufacturers.

As the market continues to evolve, leaders in the embedded systems space are coming together to develop standards for architecting embedded systems with change control as the foundation. In the future, embedded systems may converge in enterprise, with IT organizations managing embedded devices like ATMs and POS systems in remote locations such as bank branches and grocery stores.

Monica Chauhan is director of embedded solutions for Solidcore Systems in Cupertino, California, where she is responsible for product management, strategic alliances, and outbound marketing activities for embedded solutions. She has been active in defining, delivering, and marketing software solutions in the arena of security and enterprise management for more than eight years. Prior to Solidcore, Monica was director of engineering for four product lines at Ensim and in development at Sun Microsystems. Monica holds an MS in Computer Science from Stanford University.

Solidcore Systems, Inc.
650-565-5024
monica@solidcore.com
www.solidcore.com