

EXECUTIVE SPEAKOUT EMBEDDED TRENDS



Linux trends in Embedded Systems

By Inder M. Singh

The embedded world has been one of the more mature and relatively staid segments of the computing universe, but as of late it is undergoing a tectonic shift.

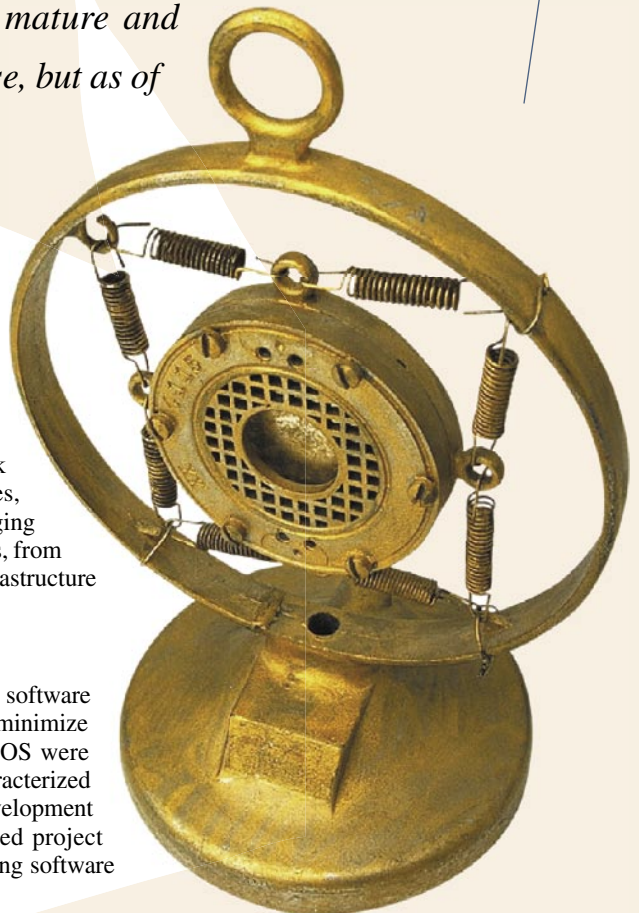
Network connectivity

Moore's law has brought plentiful computing power and memory within the range of inexpensive embedded systems. The Internet phenomenon has added the opportunity to add inexpensive network connectivity to embedded devices. As a result, any device can now be made more flexible, useful, and often less expensive by designing it as an intelligent, network connected product.

We are moving toward a world of pervasive computing and network connectivity, as intelligent embedded products surround us in our homes, workplaces, cars, and on our person as we go about our lives. Today, the emerging embedded computing universe is vast and encompasses computers of all sizes, from tiny wristwatch cameras, to telecommunication switches and a network infrastructure with thousands of nodes distributed worldwide.

Embedded software reusability

Traditionally, embedded devices have been hardware-centric, and embedded software was relatively simple and carefully designed to optimize performance, and minimize the memory footprint. Embedded operating systems such as VRTX or PSOS were simple flat address space kernels. However, the new embedded system is characterized by growing software complexity where embedded software dominates the development cost and schedule. The old way of developing software for each embedded project from scratch is giving way to the need to reuse software, and build on existing software wherever possible.



Impact of embedded Linux

The arrival of Linux has been a major factor in the changing embedded landscape. Until now, the world of embedded operating systems has been fragmented and populated by proprietary kernels. Linux, for the first time in the industry, provides the potential of an open multivendor platform with an exploding base of software and hardware support. The growth in the use of Linux in embedded systems over the past few years has been astonishing. The success of Linux in the server or desktop arena over the last few years has received the most attention, where the most ardent supporters of Linux are attempting to loosen the stranglehold of established operating systems such as Windows. In the embedded marketplace, by contrast, Linux is already moving toward world domination.

The phenomenal growth in the use of embedded Linux has been driven by its many compelling benefits that are not offered by traditional proprietary embedded operating systems. Developers appreciate having access to the source code at no cost and there are no royalty fees for incorporating Linux into their products. In addition, there is a growing base of software, both open source and licensed products, available under Linux that is helping to reduce engineers' development efforts.

The semiconductor industry has played an integral role in the emergence of embedded Linux. Software support is crucial to the success of semiconductor devices aimed at embedded markets and Linux has provided a common denominator with growing market momentum. In fact, most new devices are being launched with Linux support already available. In comparison to other proprietary operating systems, Linux supports a wide variety of hardware devices such as CPUs, network devices, and graphic devices.

The freedom and vendor-independence of Linux has extended to the semiconductor industry so that instead of relying on a Real-Time Operating System (RTOS) vendor to support a device, semiconductor companies are choosing Linux and supporting it in-house, or through one of the several embedded Linux vendors.

As further enhancements have been made to Linux it has quickly gained momentum as an ideal operating system for a wide range of embedded devices scaling from PDAs, all the way up to defense command and control systems.

“The phenomenal growth in the use of embedded Linux has been driven by its many compelling benefits that are not offered by traditional proprietary embedded operating systems.”

Defense embedded systems

The defense industry is going through a major upgrade to its systems as a part of an ambitious transformation program to support Network Centric Warfare (NCW). Implementing these programs requires large amounts of networked and heavily integrated software systems. A key factor for success is interoperability across a large number of separately developed systems as they are deployed over a period of years.

The military is realizing that Linux, as the only effective multi-vendor open standard embedded operating system, provides a solution to many of the problems of existing systems which have locked programs into proprietary solutions that make it very expensive and time consuming to upgrade to new technologies, or provide interoperability with other evolving systems. Linux is widely supported by the latest hardware devices, and there is a growing base of Linux based software, not to mention a large amount of existing software based on Solaris and other UNIX variants that can easily be ported to Linux.

Therefore, Linux is a good fit with the spiral development model where frequent technology insertions are being adopted for new defense programs. Spiral Development controls cost while decreasing cycle time for technology insertion by using features such as open architecture, module interface standards, and COTS hardware. The use of Spiral Development allows cutting-edge technologies to be fielded more swiftly.

Reliability and security

While pervasive computing and network connectivity have helped drive the explosive growth of embedded systems, it has also made information technology more vulnerable. Cyberspace is highly susceptible to attacks due to growing software complexity and Internet connectivity that could potentially paralyze the country. For example, Internet service providers, financial institutions, and power companies are considered part of the country's critical security infrastructure. The recent virus attacks have demonstrated that there is a significant need for secure operating systems that cannot be compromised. The issue is especially critical for Network Centric Warfare defense systems.

With huge amounts of both unclassified and classified data becoming accessible from a variety of users over integrated networks, security is becoming a critical requirement for embedded software in defense systems. Systems that simultaneously handle data at different classification levels have to meet stringent MLS (Multi-Level Secure) security requirements, as defined by Common Criteria Evaluated Assurance Level 7 (CC EAL-7).

No operating system has yet been certified to CC EAL-7. The main challenges are the complexity of modern operating systems, and the intermingling of security functionality with the operating system kernel, all of which run in a privileged mode. With Linux you have the additional challenge of the open source development methodology, which doesn't lend itself to the common criteria approach for assurance.

As a way around this dilemma, NSA guidance proposes a MILS architecture, which moves all but the essential security functions out of the kernel. This is based on a very small Partitioning Kernel (PK) at the lowest level of the system that is the only software allowed to run in privileged kernel mode. The PK implements time and resource partitioning to provide multiple partitions, which are isolated from each other with impregnable brick walls. Each of these can be looked upon as separate computers from a security point of view.

The new emerging paradigm is to build security infrastructures that are open standards-based, instead of the old paradigm of *security through obscurity*. Companies such as LynuxWorks are currently developing a CC EAL-7 secure separation kernel in concert with the NSA and others for the highest level of

“The new emerging paradigm is to build security infrastructures that are open standards-based, instead of the old paradigm of security through obscurity.”

security ever achieved. The separation kernel would ensure that any operating system, including Linux and other open standards-based software, could run in on top of the separation kernel in its own secure partition in an EAL-7 system environment with no vulnerabilities. Most importantly, since the application can run in an open standards-based Linux environment, the currently used embedded software tools and applications, whether in the commercial or government sectors, can easily be ported to an EAL-7 secure environment. **ECD**

Dr. Inder M. Singh

is the CEO and Chairman of LynuxWorks. He founded Excelan, an early leader in local area networks in 1982 and served as its Chairman, CEO, and President until 1985. Excelan later merged with Novell. Dr. Singh was a co-founder of Kalpana, which pioneered Ethernet switching technology, and was one of Cisco's early acquisitions. Dr. Singh is Board Chairman and ELC President for the Embedded Linux Consortium. He holds Ph.D. and M.Phil. degrees in Computer Science from Yale University, and an MSEE from Polytechnic Institute of New York.



For more information, contact Dr. Singh at:

LynuxWorks, Inc.

855 Embedded Way

San Jose, CA 95138-1018

Tel: 408-979-3900

Fax: 408-979-3920

E-mail: inside@lnxw.com

Website: www.lynuxworks.com