WIND™

Virtualization and the Internet of Things

WHEN IT MATTERS, IT RUNS ON WIND RIVER

EXECUTIVE SUMMARY

Industrial control devices have been around for years. The initial devices were manufactured with a personality, a business logic that was already built in when they left the manufacturing plant to perform one fixed function (and nothing else). They were deployed for specific tasks such as controlling industrial equipment, electricity generation, power plants, trains, planes, or automobiles.

But times have changed. Today, devices are shipped comparatively bare and are then given a personality through software download from USB devices, flash cards, or other programming over some form of connection. These more generic devices can be manufactured with a limited set of functionality and given more content during deployment by a system integrator.

Responding to and driving these developments, technology for industrial control devices has also changed dramatically in recent years—from 8-bit to 64-bit processors, from micro-controllers to multi-core—and now the Internet of Things (IoT) is changing the game again. As device manufacturers aim to take advantage of the opportunities created by IoT, one new technology is embedded virtualization. This paper discusses how embedded virtualization enables the device flexibility and security required for IoT.

TABLE OF CONTENTS

WIND

EMBEDDED VIRTUALIZATION

Embedded virtualization allows consolidation of multiple different workloads on a single piece of multi-core silicon. An industrial process may use one system for data collection, one system for signal processing, one system for vision, one system for control, and one system for a human–machine interface (HMI). These many different systems each require a piece of hardware that costs money, takes up space, and requires power, spare parts, and an update and replacement strategy—and in general has a big impact on capital expenses (CAPEX) and operating expenses (OPEX).

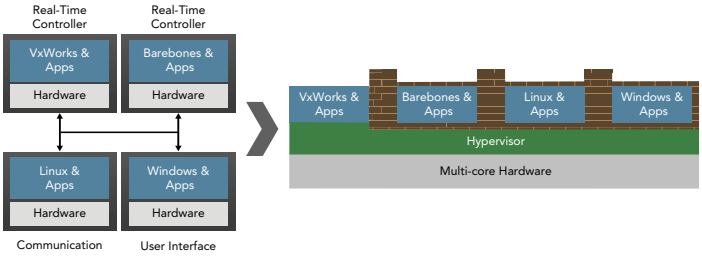

Figure 1: Consolidation of heterogeneous operating systems and functionality with Virtualization Profile for VxWorks

Embedded virtualization provides the capability to combine all these different functionalities on a single piece of hardware. While the new piece of hardware may be more powerful, and typically more expensive, than one of the original pieces of hardware, the consolidation of the multiple systems into one removes a lot of complexity from the end system, simplifies the maintenance and replacement process, and in general reduces CAPEX and OPEX.

Today's computing hardware allows efficient virtualization for embedded systems—so efficient that the impact on the performance of the end system is minimal. Indeed, embedded virtualization has minimal impact on memory size, memory performance, device access, interrupt latency, jitter, and so on.

INTERNET OF THINGS

With the advent of IoT, industrial control devices are now also connecting to the cloud, for benefits including optimizing production efficiency, minimizing environmental impact, and minimizing down time. In IoT, the cloud provides control for the devices, and the devices provide information back to business control logic in the cloud.

One of the capabilities that vendors often associate with IoT is provisioning of the industrial control devices. In other words, the devices are given a personality through the cloud. Provisioning involves initial provisioning, updates, and upgrades.

INTERNET OF THINGS AND EMBEDDED VIRTUALIZATION

When people think of provisioning, they tend to think of downloading applications, where the device has most of its personality already and is given final instructions through software download. Initial personality in such a case includes device drivers, operating system, base management layer, and so on.

But embedded virtualization allows an additional level of abstraction, making it possible to provision a device with a generic management layer only, and "empty slots" into which to provision functionality. These empty slots are called virtual machines, and can be provisioned with logic consisting of operating systems as well as business logic. The device as produced in the factory would have just the hardware, as well as the virtualization layer and the management layer. The management layer connects into the cloud and can download its content from there; the downloaded content is the business logic that allows the device to perform its specific function.

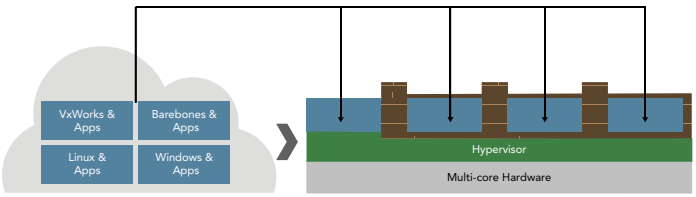

Figure 2: Provisioning functionality into the virtual machines on a device with a generic management layer

Because the board as shipped only has logic that ties it into the cloud, device manufacturers can create a generic device that knows nothing about its eventual functionality. The device is connected to, for example, a power generator, and it obtains the generator's identity through a standard interface. It reports that identity up into the cloud, which has been prepared and is expecting the connection-report; the cloud then provides the device with the required software content. The device then downloads that content, instantiates virtual machines, and is ready to function.

The management layer also makes it possible for the business content to safely communicate with the cloud through the management interface.

SECURITY

In this cloud-connected system, security is of paramount importance. The devices that are being provisioned might control anything from home heating systems to power generation or trains.

Security needs to start from the ground up when the device is booted. The management layer needs to make sure it is running on an authorized device, and that it has not been tampered with from either a hardware or software perspective, and the cloud needs to make sure it is communicating with the right management software on the right hardware.

This can be accomplished through a hardware-based root of trust, a piece of hardware called a Trusted Platform Module that is provisioned at manufacture time with encryption keys. These keys then allow the management layer to initiate a secure connection to the cloud. This secure connection can be used to download the business logic, but it can also be used to proxy communication between the business logic and the cloud. In this way, the management layer has multiple functions: it makes sure the device boots the correct software and that the device is the right device, it makes the secure connection to the right cloud, and then it allows the business logic to connect to the cloud securely.

Of course, these security concerns exist for currently fielded devices as well, but they have needed to be solved multiple times, for multiple boxes, in different fashions that all have to be developed, maintained, and monitored.

CONCLUSION

Embedded virtualization provides the benefit of consolidation, which is a main driving factor in industrial control systems today. However, with its dynamic capability of instantiating software loads, it also provides a valuable flexibility for IoT, as well as security from the ground up. The results are not just CAPEX and OPEX savings for the manufacturing floor, but also significant savings in development time for end devices.

WIND

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.