embedded INNOVATOR

DESIGNS, IDEAS AND SOLUTIONS FOR TODAY'S ENGINEERS

Fall 2010 Newsletter Article

Securing Smart Grid Devices

Using Virtualization to Protect the Grid

By Bill Graham, Product Marketing Manager, VxWorks, Wind River

Associate Member of the Intel® Embedded Alliance

Energy providers and governments worldwide are looking for ways to upgrade their energy systems. A big part of these efforts is the smart grid concept, which introduces networking and automation across the electrical system. The smart grid can give consumers and suppliers alike better monitoring and control of power consumption, leading to increased reliability, higher efficiency, and lower costs. However, computerization and connectivity bring with them the threat of security breaches and attacks.

The threats to the smart grid were illustrated in 2009, when researchers at IOActive infiltrated and controlled smart meters remotely, using a concerted cyber attack. They were able to take over a device, display a message on its LCD screen, and spread the attack from meter to meter. Although these researchers did not cause any damage, it is easy to imagine a similar attack causing widespread havoc by disconnecting homes and businesses from the grid. The smart grid also presents the risk of exposing information to unauthorized users. Data at risk includes:

- Diagnostic information
- Maintenance information
- Identification (potentially including personal information)
- Billing data
- System status

Protecting the operation of the grid and the related data flows is critical for the success of smart grid initiatives. One way to improve security is to separate critical and confidential portions of the system from non-critical, non-confidential parts. This article describes how to accomplish this goal using secure hypervisors and Intel® Virtualization Technology (Intel® VT).

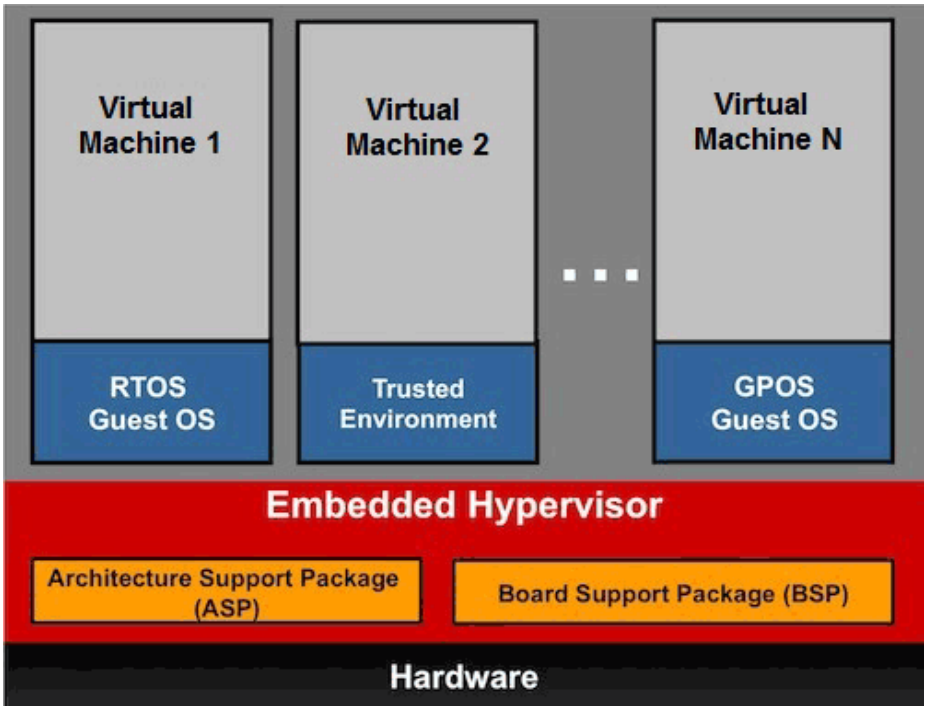

Figure 1. An example of secure partitioned architecture.

Virtualization, Partitioning, and Security

One proven approach to security is to build physically separate secure and non-secure devices and networks. For much of the smart grid, this approach is impractical because of the expense and redundancy involved. A more cost-effective solution is to leverage embedded virtualization to run both secure and non-secure software on the same device.

Virtualization enables developers to partition a single hardware platform into multiple virtual machines, each running its own guest Operating System (OS). The virtual machines are managed by a hypervisor (also known as a virtual machine monitor) that sits between the guest OSs and the hardware. With a secure hypervisor such as the Wind River Hypervisor, the virtual machines are strictly separated from one another, so that an attack, crash, or poor behavior in one partition will not impact the other partitions. This separation allows a single hardware platform to safely run secure and non-secure software side by side.

Figure 1 shows an example of a secure partitioning architecture that supports secure, trusted virtual machines. This architecture could support smart grid control and data processing in a secure, trusted partition running a minimal executive. Real-time control and device interfaces with lower security requirements could run on a Real-Time Operating System (RTOS) in a second partition.

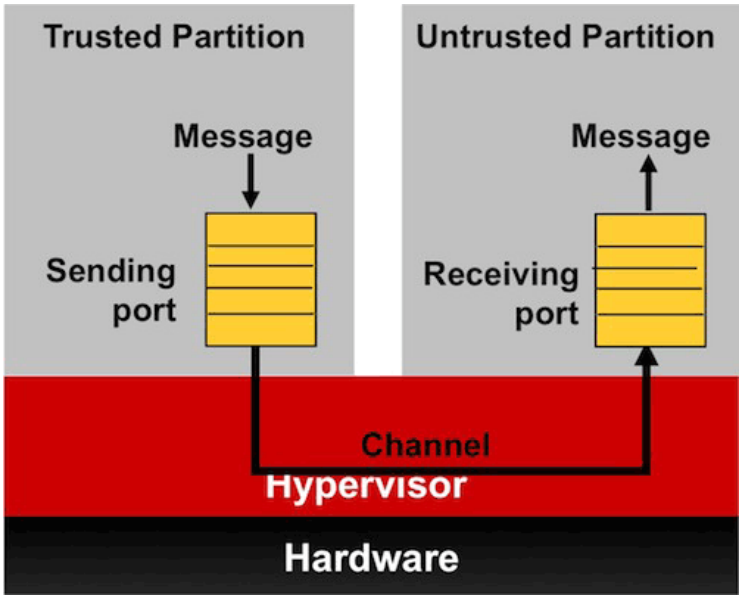

Figure 2. Secure IPC (SIPC) between partitions.

Meanwhile, a Graphical User Interface (GUI) could run on a General-Purpose OS (GPOS) in the third partition. As security becomes a more important requirement for the grid, it may become necessary to validate and certify the security characteristics of smart grid devices. Validating system security is a tedious, costly, and time-consuming task, and the effort required grows considerably for complex systems. A secure hypervisor can simplify matters by separating security-critical functions into trusted partitions and less critical software into non-trusted partitions. This separation reduces the validation workload because only the software in trusted partitions requires verification.

In order for secure partitioning to be used in smart grid devices, there must be a secure and reliable way for the trusted components to communicate with non-trusted components, and a secure way to communicate on a network of smart grid devices.

Networking, Inter-Partition Communication

Communication between partitions is a key requirement for virtualized systems since there is always a need to transfer data and control from trusted partitions to non-trusted partitions. For security reasons, the hypervisor tightly controls the allowed communication and data access amongst partitions, based on the system security policy and system configuration. One mechanism for communications is Secure Inter-Process Communication (Secure IPC or SIPC).

Figure 2 shows an example of using SIPC between partitions. SIPC uses unidirectional channels (to prevent back channels) and can provide both asynchronous and synchronous message passing.

Protected communication to the outside world—either through a dedicated private network or the public Internet—is another critical requirement for smart grid devices, as these devices must transmit sensitive billing, usage, and control information back to the grid. One approach to protecting this data is to use a high-assurance network stack that creates Multiple Single-Level (MSL) networking. This approach supports many different levels of security over the same connection, but connections at different levels of security are always kept separate. Using this approach, secure information can be kept separate from non-secure information within the smart grid device and outside in the grid communication network.

Figure 3 shows such an architecture, where a high-assurance network stack residing in a dedicated trusted partition analyzes and distributes packets to the rest of the system. Tags, such as those described by 802.1Q for virtual LANs, are used to indicate destinations of packets going in and out of the device. In this manner, secure data can be verified and isolated from general-purpose traffic.

Using a dedicated trusted partition for the network stack protects the rest of the system from network attacks and limits the covert channels available to would-be attackers. Since the network stack is isolated from the rest of the system it is easier to test, diagnose, verify, and validate the stack. Although the stack is still vulnerable to attacks from the outside world, isolation and thorough validation provides more secure communications.

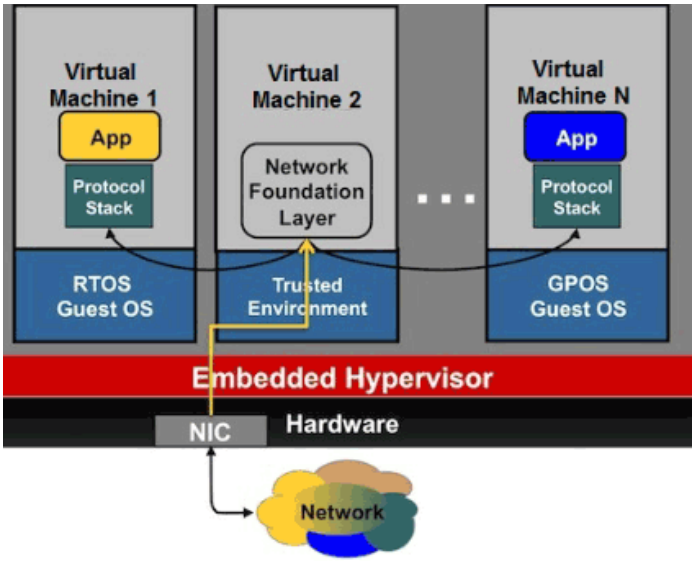

Figure 3. High Assurance Network Stack for network communication.

Leveraging Intel VT

The benefits of a secure hypervisor are significantly enhanced with Intel Virtualization Technology (Intel VT). Intel VT provides hardware assist mechanisms that improve the performance and security of a virtualized system. Key elements of Intel VT include:

Processor virtualization enhancements. Intel® Virtualization Technology for IA-32, Intel® 64, and Intel® Architecture (Intel® VT-x) speeds up the transfer of control between the hypervisor and the guest OSs. It uses hardware assist to trap and execute certain instructions for the guest OS. In addition to accelerating performance, Intel VT-x also enables implementation of certain hypervisor security features.

Memory and I/O virtualization. Intel® Virtualization Technology for Directed I/O (Intel® VT-d) enables the hypervisor to assign specific I/O devices to each guest OS. Each device is given a specific area in memory that is only accessible by the device and the designated guest OS. Once again, hardware assist accelerates performance, as the hypervisor no longer has to be involved in every I/O transaction.

Wind River Hypervisor is an example of a secure hypervisor that supports both Intel VT-x and Intel VT-d. By using Wind River Hypervisor in combination with an Intel VT-enabled processor, developers can create partitioned systems that achieve high levels of security and performance.

Partitioning is No Silver Bullet

Partitioning using hypervisor technology can enable the development of secure smart grid devices that are cost-effective to manufacture and validate. However, security is much more than just partitioning. Many other practices such as secure software design are needed to ensure security of the device as a whole. Vulnerabilities in the non-critical portions may reduce the usability of the product even if these vulnerabilities do not pose a threat to the grid. For example, corrupting the user interface of a smart grid device may render it useless or may require bothersome resets to clear the problem. To avoid such problems, proper security practices should be used in all parts of the system, both trusted and not trusted. Partitioning is a key tool, but just one part of an overall secure architecture.

Summary

Smart grid devices are susceptible to cyber attacks, especially if they are placed on public networks such as the Internet. To deal with these vulnerabilities, developers can turn to embedded virtualization using secure hypervisors and Intel VT. There are several compelling reasons to consider virtualization for smart grid devices:

Virtualization enables developers to consolidate several systems into one, which can save bill of material costs, reduce size, weight, and power, and reduce supply chain costs and complexity.

Separating secure portions of the system from non-critical parts greatly reduces the costs of verification and validation of the security of the system.

Partitioning allows smart grid devices to grow in complexity and functionality (for example, by adding GUIs and new applications) while keeping the trusted partition simpler and easier to maintain.

Secure virtualization can improve network security and reduce vulnerability to attack.

Although it does not solve every design problem, secure virtualization gives developers a critical set of tools to meet the evolving needs of this new market segment. With these tools in hand, developers have the opportunity to produce innovative designs that give them a competitive advantage. ■

The embedded industry moves fast. Keep up with the Embedded Innovator magazine that brings you cutting-edge design ideas from industry leaders. http://intel.com/design/network/ica/embeddedinnovatormag
Join the discussion at http://community.edc.intel.com
Learn more about the Intel® Embedded Alliance www.intel.com/go/embeddedalliance

Wind River is a wholly owned subsidiary of Intel Corporation and is an Associate member of the Intel® Embedded Alliance. As a world leader in embedded and mobile software, Wind River has been pioneering computing inside embedded devices since 1981. Its technology is found in more than 500 million products. Wind River is headquartered in Alameda, Calif., with offices in more than 15 countries.

WIND RIVER

intel Embedded Alliance