Solution Brief

Intel® Product Technologies

Energy Industry

Computing Technologies for the Smart Grid

Advanced Intel® product technologies boost availability, reliability and security

Disruptive business changes and forces are driving the massive upgrade of 20th century power grids to "smart grids." Every part of the grid is open for redesign, leading equipment manufacturers to develop new platforms, merge and enhance functionality, and eliminate some legacy products. The equipment design focus has transitioned from generating new energy capacity to emphasizing availability, predictability and efficiencies, which requires more intelligent equipment, like soft PLCs and relay controllers.

Utility operators can ill-afford to build new power plants every time peak load jumps, not to mention that many governments are reluctant to grant new building licenses due to environmental concerns. Yet, demand continues to grow at a historic rate of 2.4 percent per year,[1] which is forcing utility operators to find ways to do more with their existing energy capacity, consider renewable energy sources and implement demand-side management.

These regulatory and market realities are requiring a new way of thinking for utilities. There's a greater emphasis on preventing service outages and continuing on the path of reducing "customer minutes lost," a standard measure of supply reliability. Such measures are needed to increase customer satisfaction and can be realized by deploying equipment with higher levels of availability, reliability, and security.

The equipment supporting electrical grids is truly diverse, including some that was engineered, built and deployed back in the 1950s. The global need for CO_2 reductions is a major driver for updating and retrofitting the existing electrical network, enhancements that will be partially funded by government programs. The equipment within the electrical system spans huge turbines that generate energy, control systems that distribute power and smart meters that monitor home consumption. Supporting this wide range of equipment types, Intel® processors, chipsets and advanced technologies provide many capabilities that can be applied to the regeneration of the electrical utility industry, including:

- **Increasing equipment availability** by improving remote diagnostic and repair capabilities
- **Improving software reliability** by isolating application code and preventing dangerous interactions
- **Enhancing grid security** by preventing any node from executing malicious software

The smart grid will combine power transmission and information technologies, working together to enable a bidirectional flow of energy and programs designed to optimize energy usage. Supplying the required computing resources, Intel® platforms also provide the security and networking capabilities needed to usher in a new age of efficient energy management. This solution brief discusses how technologies built into Intel® silicon components improve remote management, virtualization and security, thereby enabling equipment manufacturers to better address the requirements of next-generation power grids.

Keeping Systems Online with Remote Management

When a piece of equipment on the power grid goes down, a service interruption usually occurs, and a technician is dispatched to find, isolate and fix the problem. On-site repairs are especially costly for the energy industry, which has geographically dispersed equipment such as meters located at every customer site and equipment buried underground or attached to the top of utility poles. Alternatively, utility operators are turning to remote management solutions to diagnose, repair and get equipment online faster and at lower cost.

Today, almost every power system is connected to a data network in order to share power monitoring and switching information between utility operators, consumers and power networks. The data network can also provide the communications link for remote management terminals used for many IT support tasks, such as updating software, repairing systems and collecting inventory information. When communicating with remote management systems, many power systems use the same networking functionality (e.g., Ethernet NICs, CPU, operating system, protocol stacks) for both standard LAN and remote management communications. When equipment fails, this "in-band" approach has the drawback of relying on the continued operation of many equipment components: CPU, operating system, hard disk drive and system memory. In other words, if the system is not functioning, the only option may be to send a crew.

Providing a significant remote management breakthrough, Intel® Active Management Technology[2] (Intel® AMT) implements a special circuit in the Intel® chipset that can access and control the system, even when the system is powered off or the software is corrupted. This circuit establishes an "out-of-band" link that allows the system to communicate with a management console with-out relying on the system's standard networking functionality. Intel AMT is a cross-platform solution, meaning it can support a wide variety of devices, including energy generation equipment, control systems and home energy gateway, as shown in Figure 1.

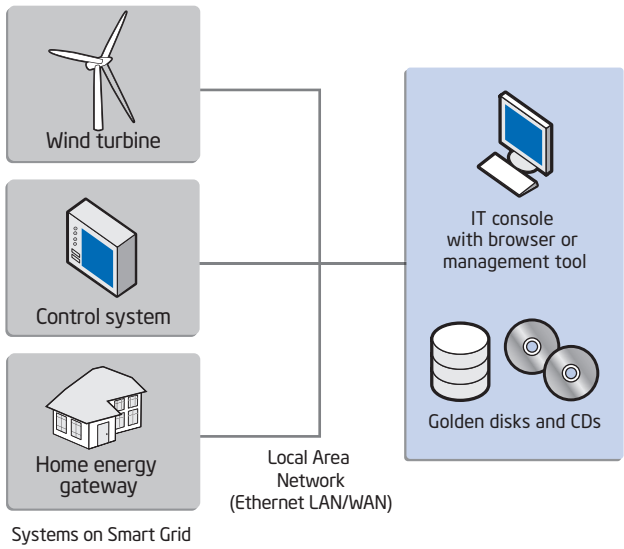

Figure 1. Remote Management Solutions for the Smart Grid

Capabilities	Results
Fix hung systems	Restore systems by cycling power, reloading software or booting from a 'gold' hard drive over the network.
Track intermittent failure modes	Access error log and event records from FLASH, accessible at all times to the remote console.
Protect against infected devices	Quarantine at-risk systems by cutting off their in-band network connection, which isolates the virus.

Table 1. Intel® Active Management Technology (Intel® AMT) Capabilities and Results

Cutting IT Support Costs

By employing Intel AMT-based management solutions, utility operators can remotely fix a wide assortment of system defects, track inventory – including warranty and software license information – and track intermittent failures, as described in Table 1. This capability reduces cost and saves time by supporting devices without requiring hands on intervention.

Reduce Onsite Repair Costs

When a power system won't boot due to corrupted software (e.g., OS, driver or critical application), the usual remedy is to send a technician on-site to reload the software image. Using Intel AMT, it's possible to remotely boot a device from a networked drive (golden disk in Figure 1) with known good software, which greatly aids troubleshooting. IT can also remotely change BIOS configuration settings, load new drivers or load a new operating system, whether or not the system is running.

Track Intermittent Failure Modes

When logging events and errors, power systems are leaving valuable clues about their health, including intermittent fail conditions that could eventually turn into a hard failure. With Intel AMT, systems can continually store this information in non-volatile memory, accessible at all times to the remote management system, regardless of the system

state. If an on-site visit is required, this capability can help identify failed components in advance, which enables technicians to arrive with the appropriate spares and fix systems faster.

Keep System Virus Signatures Up-to-Date

Power automation equipment connected to a network should be protected by the most up-to-date security software. With Intel AMT, utility operators can ensure each device has the latest virus signatures, without user assistance or the device powered-on. If a third-party contractor using an Intel AMT-enabled system connects to the network, but has out-of-date security profiles, the remote management system can quarantine the device and keep it from possibly spreading any viruses. Once the system is updated with the latest virus definitions, it is allowed to reconnect to the network.

Safeguarding Software with Virtualization

Running millions of lines of code, control systems provide the intelligence for the smart grid. Equipment developers must ensure there are no software conflicts, even though the code comes from various sources, like utility operator programmers, equipment manufacturers, legacy systems and third party vendors. Ideally, all of this software will be consolidated onto a single platform, including applications written to run on different operating systems (OS), like a utility operator's legacy customer database application. To safeguard code and improve control system reliability, developers can run safety-critical code in safe, virtualized execution environments that isolate different workloads and prevent them from interfering with one another.

Addressing Software Challenges

Today, most power systems run a single OS, typically either real-time, general purpose or homegrown. If developers want to add an application running on a different OS, they probably have to rewrite the software, which can be time-consuming and risky. Alternatively, developers can choose to run multiple OSs and their associated applications in secure partitions using virtualization. Virtualization has been around for many years, most notably used in data centers where many applications are consolidated onto a single server. Complementing software-based virtualization solutions, Intel® Virtualization Technology[3] (Intel® VT) improves their fundamental flexibility and robustness and gives software developers greater control over operating systems and applications. This capability can simplify the porting of legacy applications onto new platforms, increase the performance of time-critical functions and avoid hardware rebooting delays, as shown in Table 2 and described in the next three sections.

Simplify Software Migration

As power systems consolidate more applications, it's essential that latent defects, like software conflicts or bugs, don't crash the system. For example, a time-critical energy load monitoring application can run in its own partition, protected from unintended interactions with other applications, as shown in Figure 2. In addition, applications can run on their native OS, with little or no modification, which eases software migration and shortens development time.

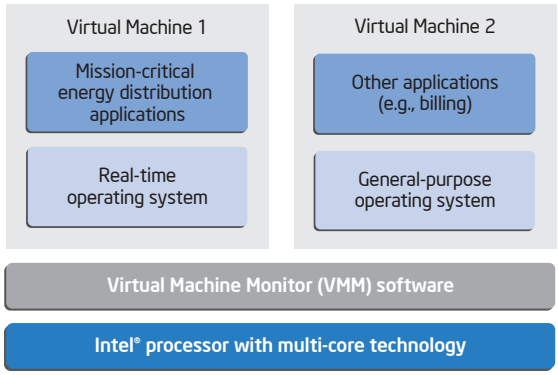

Figure 2. Virtualization Isolates Mission-Critical Code

Capabilities	Benefits
Isolates applications in secure partitions	Eases software migration and consolidation
Runs RTOS on a dedicated processor core	Improves real-time performance
Restarts applications without booting the hardware	Gets the system working faster

Table 2. Intel® Virtualization Technology Capabilities and Benefits

Improve Security of Mission-Critical Code

It's essential to secure mission-critical applications, such as "remote disconnect," which allows power companies to cut a customer's power via the network. Applications requiring a higher level of security can be isolated in secure virtual machines (VM), whose memory space is protected by hardware features in Intel processors and Intel VT. This means software running in a VM only has access to its own code and data regions, unable to page outside the memory boundaries specified by the VMM.

Avoid Rebooting the System

When an application running on a power system fails, the only solution may be a hardware reboot, which takes the system offline for a period of time. Using virtualization, developers can implement a software failover mechanism that restarts the software running in one partition without impacting the other partitions. For example, if a billing application running in a partition fails, it can be reloaded and restarted without interrupting applications running in other partitions.

Increasing Security with Hardware-Assist

When securing the smart grid, one of the biggest challenges is preventing hackers from wreaking havoc, like turning power off to consumers, perhaps cities, at will. It's possible to stop such malicious software from even executing by using hardware-based security features that are built into many of today's computing systems. This technology creates a trusted execution environment, whereby equipment manufacturers and system administrators can define a list of trusted, validated software, and only applications or device drivers on this list can be loaded.

Features	Benefits
Protected execution environment	Safeguards critical applications and data
Encrypted keys and secrets (e.g., platform configuration registers)	Eliminates potential security holes
Launch control policies	Stops compromised systems from booting
Measured launch environment	Prevents execution of untrusted software

Table 3. Features and Benefits of Intel® Trusted Execution Technology (Intel® TXT)

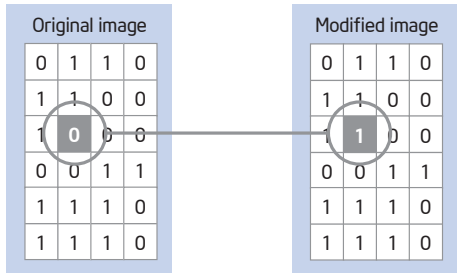

Figure 3. Hashing Detects Single-Bit Discrepancies

Designed to help protect against software-based attacks, Intel® Trusted Execution Technology[4] (Intel® TXT) integrates new security capabilities into the processor, chipset and other platform components. These hardware-based security features, unalterable by rogue software, run mission-critical applications in a safe partition, protect crucial platform data and keep malware from launching in the first place, as described in Table 3.

Protect Critical Software from Malware

In 2008, the U.S. Central Intelligence Agency confirmed that criminals had hacked into computer systems via the Internet and cut power to several cities.[5] Cybercriminals, looking to profit from attacking the power grid, seek to breach power distribution application software and databases. Using Intel TXT, OEMs can put software and data out of reach of hackers by running applications, operating systems and VMMs in the highest privilege level, permission granted only by system developers. As a result, application code and data are stored in hardware-secured memory regions, inaccessible to malware. OEMs and system administrators can define a list of trusted, validated software, and only applications or device drivers on this list can be loaded.

Stop Unauthorized Access of Data

Spoofing and phishing – when a system or program masquerades as another – are fraudulent activities used to gain access to confidential information. Helping to prevent these attacks, Intel TXT provides sealed storage in the TPM for security codes, like VPN encryption keys, which keeps perpetrators from intercepting secured communications links of power systems. Intel TXT encrypts and stores critical security codes and ensures they are only released (decrypted) to the executing environment that originally encrypted them.

Prevent Booting a Compromised System

Compromised control or home metering systems, possibly infected with a virus or connected to an illegal peripheral, need to be deactivated before they can cause harm. One solution is to stop these systems from booting whenever the software or hardware configuration differs from the trusted state. This is achievable with Intel TXT, which compares the hash (a number generated by a formula of all system software of the trusted state) with the current state and blocks system startup when differences are detected. The hashing function will detect single-bit changes, as shown in Figure 3, and prevent the system from booting.

Improving the Power Grid

Utility operators are relying on the convergence of power transmission and information technologies to support the bidirectional energy flow, while increasing availability, predictability and efficiencies. As a result, equipment manufacturers are employing Intel® product technologies that offer equipment developers new capabilities for simplifying software consolidation, managing equipment remotely and increasing system security. In addition, distributed computing architecture based on Intel technologies can help drive distributed intelligence throughout the grid and its end points, which enables optimized levels of automation and decision making at each link in the chain. These solutions can be applied across the energy network, from energy generation facilities to consumer dwellings and business sites.

For more information on Intel® energy industry embedded computing solutions, visit www.intel.com/go/energy.

For more information on Intel® Product Technologies, visit www.intel.com/technology/advanced_comm.

Additional information about Intel® embedded products can be found at www.intel.com/products/embedded/index.htm.

[1] Source: The Electricity Economy - Global Smart Energy August 2008, found at www.globalenvironmentfund.com/data/uploads/The%20Electricity%20Economy.pdf.

[2] Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/.

[3] Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[4] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). The MLE could consist of a virtual.

[5] Source: http://abcnews.go.com/Technology/PCWorld/story?id=4158869.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, visit Intel Performance Benchmark Limitations.

Printed in USA 0909/LK/OCG/XX/PDF Please Recycle 322524-001US