BUILDING A SMARTER SMART GRID: COUNTERACTING CYBER-THREATS IN ENERGY DISTRIBUTION
EXECUTIVE SUMMARY

Energy providers have arrived at a new frontier. Behind them lies the existing energy delivery infrastructure, some 70% of which is more than 30 years old, making it stress prone, labor intensive, and environmentally risky. Ahead lies the promise and potential of the smart grid, the path to more efficient, less costly, cleaner, and safer energy distribution. This new path poses a dual challenge: to retrofit and modernize the existing grid and to design tomorrow’s energy grid with even more built-in intelligence, communication, and the flexibility to adapt to the future—all at an acceptable cost and without undue complexity.

Technology exists today to help providers meet these challenges. Unfortunately, the complexity and sheer number of smart devices required to connect seamlessly and provide the intelligence that makes the grid smarter also make energy systems vulnerable to sabotage by hackers and malware. Energy systems operators, engineers, regulators, and financiers are acutely aware that the modernization of the grid and incorporation of clean technologies cannot move forward without a comprehensive and effective approach to security.

As a leading provider of secure embedded technology solutions to the energy industry, Wind River® is actively engaged with energy production and distribution operators worldwide to help meet these critical challenges. This paper explores the technology products and practices that are being deployed to address vulnerabilities in a more interconnected energy grid. It also sets forth a six-point process for enhancing security in devices and applications on which the delivery of energy is increasingly reliant.

TABLE OF CONTENTS

Executive Summary ................................................................. 2
Renewable Energy Altering the Grid Landscape ............................. 3
Increased Complexity, Increased Vulnerability ............................. 3
Workload Consolidation .......................................................... 3
Secure Partitioning ................................................................. 4
Framework for End-to-End System Security ................................. 4
  1. Threat Assessment ............................................................ 4
  2. Security-Optimized Design ................................................. 4
  3. Secure Run-Time Selection ................................................. 4
  4. Application Protection ....................................................... 4
  5. Development Life Cycle and Tools ...................................... 5
Conclusion .............................................................................. 5
RENEWABLE ENERGY ALTERING THE GRID LANDSCAPE

There is little disagreement that the ways in which the world has traditionally produced, distributed, and consumed energy must improve, for both environmental and economic reasons. While fossil fuels still account for more than 80% of global energy production, renewable sources are gaining ground year after year, prompting providers to rethink how they manage energy. Increasingly, the distribution system will need to be able to accommodate energy from an array of intermittent sources—wind, solar, hydro, wave, and geothermal—in addition to coal-fired generators. Moreover, energy from natural processes is subject to the whims of nature, and providers will need to be able to plan for variability of supply from such sources as wind, water, and the sun.

A key characteristic of the smart grid is dynamically reconfigured multidirectional energy flow, managed in a cloud-based network of connected systems that need to communicate with each other and with central control systems. While maintenance can be centralized in a distributed cloud-based deployment, the endpoints as well as the central facilities could become targets of various types of attacks.

In the smart grid, operators will expect to have complete transparency and visibility to monitor, analyze, and control energy systems. They will need to know how much energy is being created and how much is consumed, where it is coming from and where it is going. And they will need to be able to communicate with and control the various systems deployed in the cloud-based network to ensure efficiency in the flow. Decisions must be made based on real-time data generated by the system constantly instead of historical data, as is more often the case today.

INCREASED COMPLEXITY, INCREASED VULNERABILITY

Achieving this level of automation, communication, and connectivity will call for technology and integration of unprecedented sophistication and complexity, with a vast array of applications performing an equally wide variety of functions. Operators will be challenged to minimize complexity while managing the cost of development, implementation, and maintenance.

An equally demanding and arguably more critical challenge, however, will be reducing security vulnerability. Highly interconnected systems and cloud-based networks make the energy infrastructure more vulnerable to external (and sometimes internal) threats with more points of potential intrusion—with potentially disastrous results. Whether the work of disgruntled employees, hostile foreign entities, or simply individuals with destructive hobbies, hacking and malware could wreak havoc on a scale ranging from disconnecting individual meters or systems to taking control of a section of grid and immobilizing entire cities or regions. For any country, energy security is a national security issue.

For designers responsible for retrofitting existing substations or laying the foundation for the smart grid, the security issue requires a holistic view and comprehensive approach encompassing the hardware, operating system, and software requirements with adequate planning and investment before actual deployment. Designers must be sure their equipment meets stringent regulatory compliance and standards for security, such as NERC CIP in North America or the international IEC 62443 and IEC 62351, all of which focus on supervisory control, data acquisition, energy management, distribution, and automation. They must also ensure that the software solutions are upgradeable because the nature of threats will evolve over time in ways that cannot be anticipated.

WORKLOAD CONSOLIDATION

A smarter energy distribution system will rely on distributed embedded systems performing interrelated and interdependent tasks simultaneously. Historically, the conventional approach to security in a multisystem environment has been to physically separate functions and have each system run on its piece of operational or computing hardware. But this practice has proven unsustainable for a variety of reasons, including implementation, certification, and maintenance costs, the amount of real estate multiple devices take up, and the amount of energy they consume.

A more practical approach is workload consolidation through multi-core processing technology. Creating a “system of systems” enables a virtualized computing environment comprising multiple
operating systems and applications that provide multiple distinct end-user platforms. Today’s multi-core technologies make it possible to deploy integrated systems that are more energy efficient and have greater application scalability compared to multiple single-core systems. They also help protect software investments by allowing installation of hardware capable of meeting increased processing needs in the future.

SECURE PARTITIONING
Security can be further enhanced by adding safe and secure partitioning and virtualization with Wind River Hypervisor, allowing multiple operating environments and applications to run securely and independently without interference from one another. Partitioning and workload consolidation also allow the addition of a software appliance to the system that can provide a fully managed firewall from the Wind River embedded ecosystem rather than relying on one main firewall for the entire security perimeter, in which a breach could give an intruder access to the whole system. The isolation and protection between virtual boards prevent a fault in one from affecting another. If a problem occurs in a less critical human-machine interface (HMI) application, it will not affect another application supporting critical automated system tasks.

In the event of an attack, the time and space separation of functions, based on the unique option to isolate cores, prevents the spread of malware among different systems. If one of the applications is compromised by an intrusion, the others will continue to perform unaffected. The affected partition can be disinfected and rebooted while other virtual boards continue to run.

FRAMEWORK FOR END-TO-END SYSTEM SECURITY
Withstanding cyber-threats of unpredictable patterns in an energy distribution system, where many embedded systems have limited human interfacing, is a massive challenge. Wind River has established an end-to-end framework for identifying security needs, developing the right solutions, and monitoring and managing system security on an ongoing basis.

1. Threat Assessment
What potential threats, attacks, and propagation methods must the system be guarded against? An upfront threat assessment is essential to inform the design, run-time, middleware, and application component selection and provide a benchmark for validation during integration and system testing.

2. Security-Optimized Design
Based on the threat assessment, developing a design that combines robust performance with security is critical. The design stage should incorporate such best practices as componentization and secure system partitioning. Through virtualization, designers can isolate key areas of the system that could be prone to attack, allowing the system to filter, manage, and control attack points and limit the likelihood of a successful attack. The system’s design must also include the ability to periodically upgrade its security profile in anticipation of emerging threats.

3. Secure Run-Time Selection
Based on the design requirements as well as certification and regulatory standards, the appropriate system components must be selected with care, including the underlying run-time platform, operating environment, hypervisor technology, and middleware. Perpetual device ownership depends on the design of the system at deployment time. Including a hardware root of trust (such as the Trusted Platform Module or a SIM card) can enable security features over the lifespan of the device.

4. Application Protection
At this point, the designer determines the appropriate security technologies to be incorporated into the device, based on the threat assessment and relative critical nature of each component. There is a range of security options, including trusted or verified boot of firmware images, antivirus and anti-malware software, advanced data encryption, firewalls, and “whitelisting,” which enables devices to receive communications only from recognized external applications.
Wind River offers solutions such as VxWorks®, Wind River Linux, and Android, secure run-time environments that can limit exposure to uncontrolled software. On Linux-based systems, features such as grsecurity can control resources available to certain applications. Using integrity management architecture, only applications that have been signed to run on the device can be loaded into memory or installed on the file system.

5. Development Life Cycle and Tools
As the system is developed, it is subjected to validation and testing using a variety of tools, including code analysis, security tests, and “what-if” vulnerability analysis. An integration of vulnerability certification equipment with white-box diagnostics and testing technology such as Wind River Test Management is vital to keep the test-diagnose-fix cycles short and efficient.

Development tools are available that will enable application service providers or carriers to create applications or updates that can be deployed within the security framework in the deployed devices.

Once a device has been configured and deployed, it needs to be actively managed to maintain adherence to evolving security requirements and policies. Systems in an energy deployment may need an active update capability, often without user intervention. Secure remote attestation is necessary so devices in the field can be securely identified remotely.

There are constraints on how, and how frequently, deeply embedded devices can receive new firmware or patches. Wind River offers the expertise, technologies, and service capabilities to support the entire secure design life cycle. We have experience in employing specific processes to identify vulnerabilities in the pre-design phase and address them in the design. Wind River also offers tools for validation and testing, including “white box” testing to simulate malicious penetration, complex system simulation, and vulnerability testing. The company is experienced in retrofit scenarios as well as cost-optimized, flexible designs for the future. We are actively working with energy providers and their equipment suppliers to address the challenges of machine-to-machine communication, including manageability, connectivity, and security.

CONCLUSION
A smarter, more efficient energy distribution system is in the long-term best interests of the planet and everyone who lives on it. Leveraging advanced automation technologies will benefit energy producers, distributors, and consumers alike, potentially reducing the costs of delivery while increasing control at every level. The benefits far outweigh the risks posed by those who would exploit opportunities to tamper with the system.

Those risks are nonetheless real, and it is incumbent upon energy providers to protect the grid at every point of vulnerability. Performance cannot come at the price of security—and fortunately does not have to. The expertise and technologies already available will enable energy providers to secure their systems today while providing the flexibility to adapt to as-yet-unknown threats that may be looming on the horizon.