EXECUTIVE SUMMARY

Alstom Grid, Intel, and McAfee have joined their expertise to deliver their view on smart grid cyber security, including:

- What the smart grid is
- The smart grid cyber security landscape
- How to protect the smart grid

This initiative highlights challenges in migrating to the modern grid and different approaches to building it while addressing cyber security risks.

What Is the Smart Grid?

A Needed Evolution

According to the latest projections of the International Energy Agency, smart grid technologies have become essential to handling the radical changes expected in international energy portfolios through 2030:

- **World energy demand** is expected to increase at an annual rate of 2.2 percent, doubling the global energy demand overall.
- **Global CO2 emissions** are projected to accelerate even faster than this energy demand, leading to the first critical impact on climate change and exposing the grid to new environmental catastrophes while increasing societal awareness of environmental challenges.
- **Intermittent renewable capacity** will continue to evolve, reaching an average of 25 percent capacity by 2050 and leading some grid areas to absorb more intermittent renewable energy than their actual consumption through specific periods of the day.

The smart grid is an evolution of the electrical grid to respond to these challenges. A smart grid is an energy transmission and distribution network enhanced through digital control, monitoring, and telecommunications capabilities. It provides a real-time, two-way flow of energy and information to all stakeholders in the electricity chain, from the generation plant to the commercial, industrial, and residential end user.

This evolution is crucial for integrating both renewable and distributed energy resources and to improve the efficiency and sustainability of the electrical grid and associated services. It will also help in other ways, such as enabling:

- Smart and positive energy infrastructures
- Increased energy density management during peaks
- Real-time pricing to customers
- Integrated mobility services
- New virtual power plants
- Microgrid

Contributors

Yves Aillerie, Intel Corporation
Said Kayal, Alstom Grid
Jean-Pierre Mennella, Alstom Grid
Raj Samani, McAfee
Sylvain Sauty, Intel Corporation
Laurent Schmitt, Alstom Grid
It will also help energy customers to better manage their electricity consumption and even sell their unused home-produced electricity back to the grid. Figure 1 shows the smart grid ecosystem.

The smart grid is more than an infrastructure for smarter electricity generation, distribution, and consumption. It will have a positive impact on our modern society, with benefits for both individuals and the collective population.

The smart grid phenomenon is something like the Internet phenomenon. It is like an "Internet of watts" that can come from renewable energy sources, energy storage, electrical vehicles, or smart home appliances.

Beyond these connected smart assets, a smart grid is also about ecocitizens, efficiency, green practices, mobility, national welfare, and reliability.

Layered Architectures

Energy utilities worldwide see the need for piloting new smart grid systems, laying down a new layer of digital equipment on their existing infrastructures to interconnect all assets—from ultra-high-voltage supergrids to ultra-low-voltage micro- and pico-grids—with buildings and homes.

Smart grid technologies bring the opportunity to enhance existing power grid infrastructures (i.e., power lines, electrical substations, network control rooms) by improving real-time assessment of system conditions. New digital equipment and devices can be strategically deployed to complement existing equipment. Using a combination of centralized IT and distributed intelligence within critical system control nodes—ranging from thermal and renewable plant controls to grid and distribution utility servers to cities, commercial and industrial infrastructures, and homes—a smart grid can bring unprecedented efficiency and stability to the energy system.

Information and communication infrastructures will play an important role in connecting and optimizing the available grid layers.

Figure 2 shows the smart grid's layered architecture.
A significant challenge for these new architectures is to offer enough openness to connect historically siloed resources while matching end-user privacy regulations and mitigating new cyber security risks.

**The Smart Grid Cyber Security Landscape**

**Cyber Security Standards**
A smart grid environment relies heavily on standards, mainly to guarantee interoperability among systems. Standards also play a key role in smart grid cyber security.

Standards to develop smart grid cyber security are available today, although some enhancements and new materials will be required to reflect the evolution of the smart grid, its technologies, and threats. Some will also need to be specifically profiled for the smart grid environment.

The challenge is to maintain these standards over time at an appropriate pace. This will require substantial effort, but the benefit of supporting the deployment of smart grid infrastructures that are secure by design will make it worthwhile.

In its report, the CEN-CENELEC-ETSI SG-CG/SGIS working group chose a European electrical grid stability scenario as reference to define security levels (Table 1).²

These security level definitions help create a bridge between electrical grid operations and cyber security. They provide guidance in helping to identify critical areas where security matters most from a global electrical grid stability point of view, starting from pan-European supergrids down to microgrids in city neighborhoods.

**Fast-Changing Cyber-Threats**
The cyber threat landscape is evolving quickly. The last few years have seen an exponential growth of threats. In its fourth quarter 2012 threats reports executive summary document, McAfee says, “For the year, new malware sample discoveries increased 50 percent with more than 120 million samples now in the McAfee Labs ‘zoo.’”³ Figures 3 and 4 show total malware samples in the McAfee Labs database and new malware samples.⁴ Cyber threats are also evolving and becoming highly sophisticated. Advanced persistent threats (APT) are good illustrations of this mutation. Also, attackers are no longer amateurs, but highly skilled and organized professionals able to launch complex and coordinated attacks using sophisticated tools.

Many types of cyber threats are well known:
- Hackers
- Malware
- Zero days
- Botnets
- Denial of service (DOS)
- Distributed denial of service (DDOS)

These are all terms we have lived with for years.

Information systems have always been targeted by cyber attackers. What is relatively new is the realization that industrial control systems are also vulnerable. This was demonstrated in 2010 with Stuxnet, the first discovered malware targeting industrial control systems.⁵ Electrical grids are valuable and critical targets that need to be protected from cyber threats.

**Smart Grid Architecture**
Smart grid layers require a system of systems approach with differentiated security needs.

The smart grid includes different domains:
- Power generation
- Transmission
- Distribution
- Distributed energy resources
- Smart cities
- End consumers

It relies on a multitude of stakeholders, each with its own specific role and activity within a given domain.

---

**Table 1. M/490 SG-CG/SGIS Security Levels**

<table>
<thead>
<tr>
<th>Security Level</th>
<th>European Grid Stability Scenario Security Level Examples</th>
</tr>
</thead>
</table>
| 5 - Highly Critical | • Assets whose disruption could lead to a power loss above 10 GW  
 | |   • Pan-European incident |
| 4 - Critical | • Assets whose disruption could lead to a power loss from above 1 GW to 10 GW  
 | |   • European/country incident |
| 3 - High | • Assets whose disruption could lead to a power loss from above 100 MW to 1 GW  
 | |   • Country/regional incident |
| 2 - Medium | • Assets whose disruption could lead to a power loss from 1 MW to 100 MW  
 | |   • Regional/town incident |
| 1 - Low | • Assets whose disruption could lead to a power loss under 1 MW  
 | |   • Town/neighborhood incident |

Source: CEN-CENELEC-ETSI
A smart grid architecture is a system of systems: a large and complex system made of smaller and simpler systems distributed and interconnected. Each smaller system has a different systemic impact on the global system stability and each must be assessed.

Using the M/490 SG-CG/SGIS security levels (Table 1), Figure 5 shows how this could be transposed into a smart grid architecture.

Each smart grid subsystem and its associated assets require specific security functions and solutions. For example, the solution to secure a substation is not the same as the solution to secure demand response and home energy management systems. However, this does not mean that subsystems with "lower" criticality should not be secured. The security measures for each level must be sufficient to mitigate the risks. All subsystems would not necessarily need to align to the subsystem having the highest security requirements to efficiently protect the whole system, since they have their own role to play in the global smart grid ecosystem.

Smart grid stakeholders need to analyze security levels from the perspective of a global risk assessment of each smart grid use case and subsystem considered in the end-to-end architecture.

Smart Grid Cyber Security Specificities

The European Commission has expressed concern about measures to ensure a high common level of network and information security across the Union. The U.S. White House has also expressed concern about cyber security and protecting critical infrastructures.

As a large system of distributed and interconnected systems, the smart grid offers an exceptionally large attack surface. Every asset of the smart grid (i.e., home gateways, smart meters, substations, control room) is a potential target for a cyber attack. An attack over a critical node may jeopardize the grid security and lead a cascade effect to a whole system blackout.

The smart grid cyber security challenge is about protecting the ever-growing number of smart grid assets and their communication channels from fast-growing and continuously evolving cyber threats.

Protecting the End-to-End Architecture

No Silver Bullet

To maintain the stability of the whole system, most smart grid subsystems need to keep operating under all circumstances—even if one or more assets is breached or under attack.

Usual cyber security technologies and best practices—such as antivirus, firewalls, intrusion prevention systems, network security design, defense in depth, and system hardening—are necessary to protect the smart grid. However, history showed us they are only part of the solution.

Countering evolved and highly sophisticated threats such as advanced persistent threats (APT) requires advanced cyber security technologies including security information and event management (SIEM) systems, application whitelisting, and security features embedded at the processor level, among others.
Securing the smart grid requires a combination of standard and advanced cyber security technologies.

**Security by Design**

Since threats are constantly evolving, protection demands advanced cyber security technologies.

By providing comprehensive, real-time threat intelligence, cyber security solutions can protect systems against cyber threats across multiple vectors. Intended to collect information from devices, networks and applications, security information and event management (SIEM) systems are often focused on security events to identify risks and threats based on analysis of both internal and external data. Such systems are deployed within secure and isolated facilities, or in broadly distributed zones, which is critical for obtaining situational awareness across zones. SIEM systems collect and aggregate information from cyber systems and then provide information about risks and threats through an automated process supporting decision-making.

Application whitelisting can complement traditional malware protection technologies like anti-virus and is a valuable alternative when such traditional technologies cannot be deployed. Application whitelisting through a list of authorized files ensures that only allowed files are executed. Non-authorized software (e.g., malware) cannot be executed on systems that have this technology deployed. Whitelisting technologies are particularly suited for environment where systems used are quite stable.

Finally, Hardware-assisted security makes systems more resilient and helps decrease the time needed to return to normal service in case of incident or attack (Figure 6).
Specific secure chipsets allow secure system remote control and maintenance (operating system, BIOS, application patches) over extra-secure networks. Such platforms can also detect if the system has been physically manipulated by logging any important action that has been performed on it and by detecting any change in the hardware components.

Hardware enforced virtualization can isolate execution environments and separate memory access, effectively containing an attack to the limit of a virtual machine. Virtual machines can easily be reloaded from their latest known stable snapshot.

An embedded trusted and secure boot process verifies the platform integrity before mounting the hypervisor and the virtual machines.

Cryptographic chips provide robust and fast encryption features (such as Advanced Encryption Standard [AES]) and random generators that can be used for communication and storage encryption. Cryptographic chips also provide a secure storage for cryptographic keys.

To be truly efficient, all these advanced technologies need to be adapted to smart-grid-specific models. These are necessary steps to build inherently secure-by-design smart grid end-to-end architectures.

**Conclusion**

First experiences on smart grid demonstrations reveal that new architectures develop as combinations of new use cases and actors, to be expanded on the top of existing grid infrastructures. This requires interconnecting existing subsystems with new ones.

This inherently implies an enlargement of the grid attack surface, and so requires taking new risk mitigation measures. This must be done by taking into consideration the potential impact of an attack to the end-to-end electrical system stability for each use case considered. This requires new approaches to manage cyber contingencies in a consistent way with other traditional grid contingencies and expand grid operators’ situational awareness through cyber attacks.

Only by understanding the smart grid, its strengths and weaknesses, and the threats it has to face will it be possible to build secure-by-design smart grid end-to-end architectures.

As military strategist Sun Tzu (544 to 496 BC) stated, “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.”

Cyber security is a growing concern and a key success factor for smart grid deployment. Alstom Grid, Intel, and McAfee have teamed up to move on smart grid opportunities in a secure and effective way.

---