

# SMART GRID E O BIG BROTHER ENERGÉTICO

Por Cyro Vicente Boccuzzi

O Ministério das Minas e Energia (MME) do Brasil acaba de criar um grupo de trabalho para avaliar as políticas públicas necessárias para a implantação de um Programa Brasileiro de Rede Elétrica Inteligente, o smart grid. O grupo é composto por representantes de diversos órgãos oficiais e centros de pesquisas e poderá contar com a contribuição de entidades setoriais e outros colaboradores.

A iniciativa envolve a Agência Nacional de Energia Elétrica (Aneel), a Empresa de Pesquisa Energética (EPE), o Centro de Pesquisas de Energia Elétrica (Cepel) e o Operador Nacional do Sistema Elétrico (ONS) como membros permanentes. A união de tantos representantes da cúpula decisória do setor elétrico nacional em torno do tema demonstra que a implantação das tecnologias de smart grid é inexorável e revela que o país está atento à necessidade de regulamentações e normas adequadas às alterações que essas novas tecnologias e inovações poderão representar no âmbito da produção e consumo de energia elétrica no país.

O advento do smart grid traz a implantação de sensores, microprocessadores e dispositivos de telecomunicação com granularidade de monitoramento nos ativos das concessionárias e nos pontos de consumo de energia, implicando na instalação de milhares de equipamentos e tornando a comunicação onipresente. Desta forma, é viabilizado um acentuado aumento do conhecimento detalhado das condições da demanda de energia pelos clientes e da situação operativa da rede elétrica. Por outro lado, deve haver maior complexidade na operação e no gerenciamento da rede.

Ao mesmo tempo em que aumenta substancialmente a capacidade de resposta das empresas responsáveis pela cadeia de suprimento de energia elétrica, essa nova plataforma incrementa substancialmente a quantidade de pontos de potenciais falhas, ataques ou erro, implicando, portanto, na necessidade de implantação de sistemas superiores de segurança.

Nesse aspecto, as principais preocupações se concentram nos seguintes pontos:

- Faturamento: necessidade de garantia da integridade e consistência dos dados medidos e da sua disponibilidade para utilitários adjacentes (infraestrutura operativa de B2B);
- Distribuição: detecção eficiente e precisa de falhas não planejadas e planejadas e do correspondente controle de carga (confiabilidade de ligar ou desligar e a correspondente execução no campo);
- Sistemas: garantia da integridade da infraestrutura de ponta a ponta e de

notificações de alteração de configuração e controle de acesso, inclusive nas redes internas dos clientes;

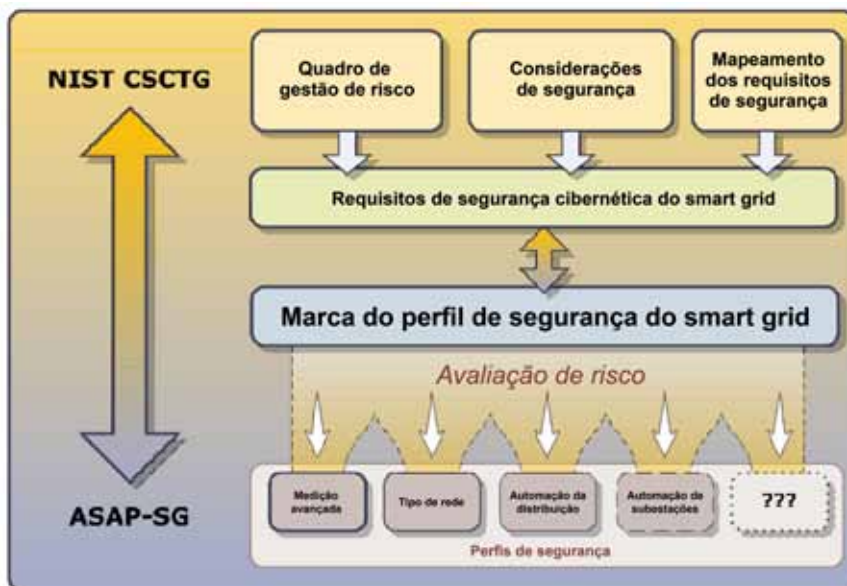
- Logística de instalação: atualização dos cadastros e garantia de atualização de firmwares de medidores e softwares operacionais de todos os equipamentos e processadores;
- Cliente: controle de acesso dos clientes na gestão de sua conta, incluindo disponibilidade de dados de pagamento, saldos de uso e privacidade de dados de identificação pessoal e de uso.

A abordagem que está sendo tomada na América do Norte, onde projetos de demonstração destes sistemas começam ter sua instalação massiva planejada, é a segurança de ponta a ponta, envolvendo uma enorme comunidade trabalhando de forma integrada. Nesses esforços, é possível destacar o papel do National Institute of Standards and Technology (NIST). O NIST está encarregado de desenvolver todas as regras de interoperabilidade das normas e padrões do smart grid de modo coordenado com as demais entidades normativas do mundo.

Na área de cyber security, o instituto norte-americano instituiu um grupo denominado Cyber Security Coordination Task Force (CSCFT), com mais de 400 membros de todo o mundo, que foca um esqueleto de requisitos básicos, em nível mais estratégico de requerimentos, abrangendo o mapeamento dos requisitos de segurança, as considerações a serem endereçadas e o quadro de referência de endereçamento e gerenciamento.

Existem também outros grupos que estão focados em nível ainda mais detalhado e operacional, fazendo uma avaliação efetiva de riscos e medidas de contenção, dos quais se destaca o Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), atuando, principalmente, nas frentes de medição eletrônica, comunicação, automação e troca automática de dados.

Toda esta preocupação com padrões e regulamentação, que somente agora começa a chegar ao Brasil, é fundamental porque o Smart Grid permite que informações bastante



detalhadas sobre o uso de energia pelos consumidores passem a ser monitoradas pelas empresas de distribuição, e isso certamente transformará o cerne das relações comerciais entre essas empresas e os clientes. De um lado, abrirá oportunidades para a prestação de novos serviços pelas empresas e, de outro, trará preocupações sobre a guarda dessas informações e sobre a privacidade dos consumidores.

Um exemplo do aspecto positivo desse conhecimento é que a introdução maciça de medidores eletrônicos permitirá às distribuidoras e aos órgãos reguladores criarem modelos de contratos semelhantes aos das operadoras de telefonia móvel, com tarifas diferenciadas em função de horários de maior e menor consumo. Isso dará aos usuários a oportunidade de reduzirem, com a ajuda da concessionária ou não, a sua demanda de energia nos períodos de pico, otimizando o uso do sistema ao longo do dia. Com isso, o consumidor terá à disposição ferramentas para administrar melhor seus gastos. As concessionárias, por sua vez, poderão atender mais consumidores com as mesmas instalações existentes. No conjunto, o processo garantirá o aproveitamento mais eficiente de toda a infraestrutura disponível, com redução de custos e benefícios para toda a sociedade.

Além disso, a tecnologia possibilitará o controle do pagamento das contas de luz e cortes de energia de forma centralizada, bem como maior precisão e celeridade na detecção de perdas, falhas e fraudes, melhorando as condições de operação das distribuidoras e reduzindo desperdícios, hoje arcados por todos os consumidores.

## SEGURANÇA E PRIVACIDADE

Entre os princípios de segurança que estão sendo estudados, destacam-se as questões de confidencialidade, disponibilidade e integridade.

A confidencialidade trata sobre como manter as informações privadas, evitando converter o smart grid em um instrumento invasivo à privacidade dos usuários. Por meio da tecnologia, será possível saber se uma casa está vazia, ou não, num dado momento; a que horas as pessoas acordam, tomam banho ou desligam seu televisor habitualmente; ou se a geladeira e a máquina de lavar já não operam com nível mínimo de eficiência, havendo oportunidade de serem trocadas por equipamentos mais modernos e eficientes.

Mesmo que esse tipo de informação não tenha, em princípio, grande utilidade para as concessionárias de distribuição, certamente existe um grande mercado comercial ávido por informações sobre tais hábitos de consumo. Seguramente, esse tipo de informação interessa a vários empreendimentos desejosos por identificar o perfil de um potencial cliente para seus produtos e serviços. A exposição do perfil e dos hábitos de consumo dos usuários da rede elétrica evoca, portanto, questões relativas à segurança das pessoas e de sua privacidade. São necessárias regras claras que abarquem o tema e protejam o consumidor do uso indevido dos seus dados de comportamento.

Além disso, essas informações estarão continuamente trafegando entre as casas e a companhia de eletricidade e poderá haver interessados na sua interceptação. Isso traz preocupações óbvias com a segurança dos sistemas de telecomunicações e de tecnologia da informação. Assim, mesmo que tais dados passem a ter uso regulado, restrito e controlado pelas empresas, deverá haver controle e garantia de que eles não poderão ser mal utilizados ou vazados por um funcionário ou prestador de serviços mal intencionado, ou então, que

sejam interceptadas e utilizadas para fins não autorizados. Por esse motivo, a segunda questão de interesse trata da disponibilidade das informações, ou seja, quais profissionais ou processos poderão ter acesso a que informações necessárias para fazer o seu trabalho.

Finalmente, uma grande preocupação é também devotada à integridade das informações, garantido que o que é medido ou monitorado seja apropriadamente reportado, que o que é enviado seja recebido, sem alterações e que o que é solicitado seja executado corretamente e com precisão. Nesse aspecto, a questão de sabotagem ou terrorismo traz à tona novas ameaças a infraestruturas críticas de serviços essenciais, hoje com potencial relativamente limitado de ser provocada à distância.

Por todos esses motivos, nos países onde se avança na implantação das redes inteligentes, da medição eletrônica e dos dispositivos de controle interno dos equipamentos das residências, esse debate já começou e está bastante aquecido, em decorrência da preocupação sobre a definição dos requisitos mínimos e precauções desses sistemas de telecomunicações e de tecnologia de informação, para evitar problemas no futuro. O foco das discussões, como apresentado, tem sido a disponibilidade, integridade e confidencialidade das informações e a clara definição dos propósitos específicos para sua utilização.

Nesse sentido, vale lembrar que, apesar de as empresas em geral (não somente de eletricidade) já possuírem, há décadas, muitas informações granulares de seus clientes, as novas tecnologias e o debate de sua implantação vem impondo que a informação coletada legalmente por uma razão específica e com uma finalidade determinada só possa ser utilizada para esse fim. Não custa lembrar que até as redes sociais, como o Facebook e outras, têm sido alvo de crescente questionamento nesses países.

Assim, a regulamentação das tecnologias vinculadas ao smart grid deve ir muito além dos parâmetros eminentemente técnicos e tecnológicos, envolvendo até mesmo questões de Direito Internacional. Isso porque, seja no Brasil ou nos Estados Unidos, uma grande parte das empresas é multinacional e terceiriza seus serviços de informática contratando empresas prestadoras de serviços situadas em outras partes do mundo, como China ou Índia, na onda da tendência da chamada cloud computing. Dessa forma, as regras referentes à segurança da informação também precisam contemplar culturas e legislações de cada país.

Como se pode perceber, as alterações da prática de distribuição de energia decorrentes do smart grid não são poucas, favorecendo o aumento da flexibilidade e a eficiência nas relações entre consumidores e distribuidoras, bem como a otimização da infraestrutura disponível com grandes benefícios para a sociedade. Mas a garantia de que a inovação tecnológica do smart grid será causa de melhorias no setor energético brasileiro depende da correta regulamentação do tema. Assim, estabelecer, desde o início, regras relativas à privacidade dos consumidores e à segurança das informações é fundamental para evitar que a rede elétrica abra as portas para uma nova modalidade do Big Brother energético. **MI**



**Sobre o autor:** Com quase 30 anos de experiência internacional no setor de energia, Cyro Vicente Boccuzzi é fundador e Presidente da ECOee. Foi vice-presidente da AES Eletropaulo, diretor-executivo da Andrade & Canellas e membro de conselho de diversas empresas, associações e entidades de pesquisa.

**Sobre a empresa:** A ECOee – Expertise, Consultoria e Ordenamento em Energia Eficiente é uma empresa de consultoria na área de energia, com foco em Gestão e Tecnologia. Com vasta experiência internacional, atua na concepção de soluções realistas e implementáveis, assistindo empreendimentos a obterem sucesso e resultados sustentáveis na implantação de inovações.

[www.ecoee.com.br](http://www.ecoee.com.br)