Cursos e Projetos de Smart Grid, Energias Renováveis e Tecnologia da Informação

Estamos prospectando novos negócios e investimentos em redes inteligentes (Smart Grid), geração de energia renovável, monitoração e automação de redes e segurança cibernética.

Nossos projetos de tecnologia são focados em agregar inteligência aos produtos e serviços, a partir de modelos de negócios inovadores. Desenvolvemos projetos de Big Data, Analytics, Internet of Things (IoT), Mobile Applications e Cloud Computing. Projetamos uma plataforma de software baseada em Hadoop para Big Data, um middleware para coletar grandes volumes de dados de dispositivos remotos usando IoT e usamos ferramentas avançadas para análise de dados. O desenvolvimento de projetos usa métodos de engenharia de software e análise de riscos a partir de protótipos para garantir a completa aderência aos modelos de negócios.

Atualmente, o foco dos trabalhos são:

- Gestão de Segurança Cibernética para Redes Inteligentes – Smart Grid (Anexo I)
- Projetos de geração de energia fotovoltaica de 1MWp (Anexo II)
- Plataforma de software para monitoração remota de sistemas baseado em Big Data, IoT e Analytics (Anexo III)
- Cursos sobre Smart Grid e Cyber Security (Anexo IV)
- Projetos de data centers para adequação de novas tecnologias (Cloud Computing, Big Data, IoT, Analytics, Aplicações Móveis, etc.) e eficiência energética da infraestrutura (Anexo V)
- Cursos e workshops sobre inovação, tecnologia e sustentabilidade (Anexo VI)

Os projetos são coordenados por Eduardo Fagundes (Anexo VII)

Anexo I

Artigo

Modelo de Maturidade de Segurança Cibernética para Redes Inteligentes de Energia Elétrica

Smart Grid Cybersecurity Capability Maturity Model

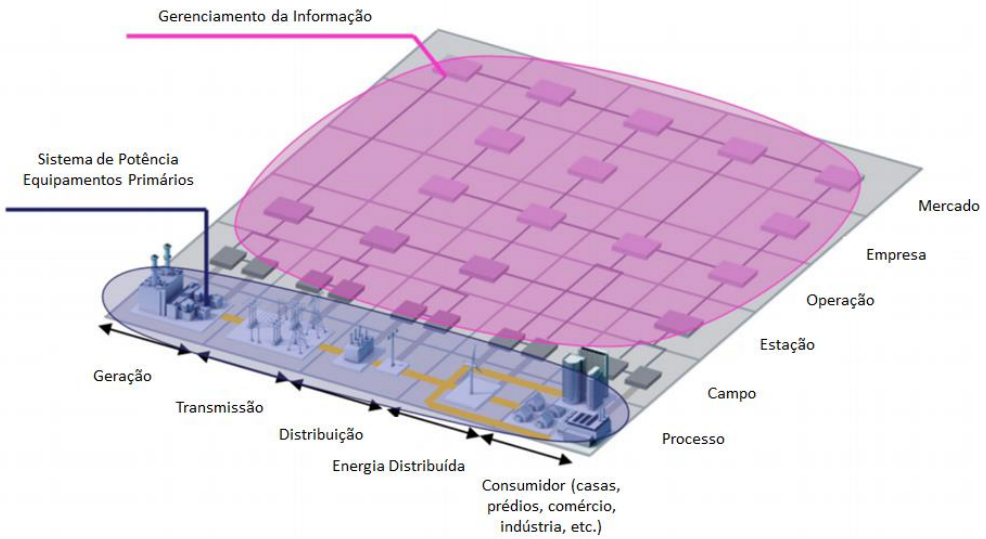
No contexto de redes inteligentes de energia elétrica, Smart Grid, a segurança cibernética tem uma forte relevância. A análise do risco e as ações para mitiga-los determinam a confiabilidade do sistema. Para comparar diferentes redes e sistemas de energia é necessária a adoção de um modelo de referência com critérios padronizados.

A partir de uma iniciativa da Casa Branca americana, liderada pelo Departamento de Energia (DOE) em parceria com o Departamento de Segurança Nacional (DHS) e com a colaboração da indústria e especialistas do setor público e privado foi desenvolvido o *Electricity Subsector Cybersecurity Capability Maturity Model* (ES-C2M2).

O objetivo do modelo é apoiar o desenvolvimento e medir os níveis de segurança no setor elétrico através de quatro objetivos:

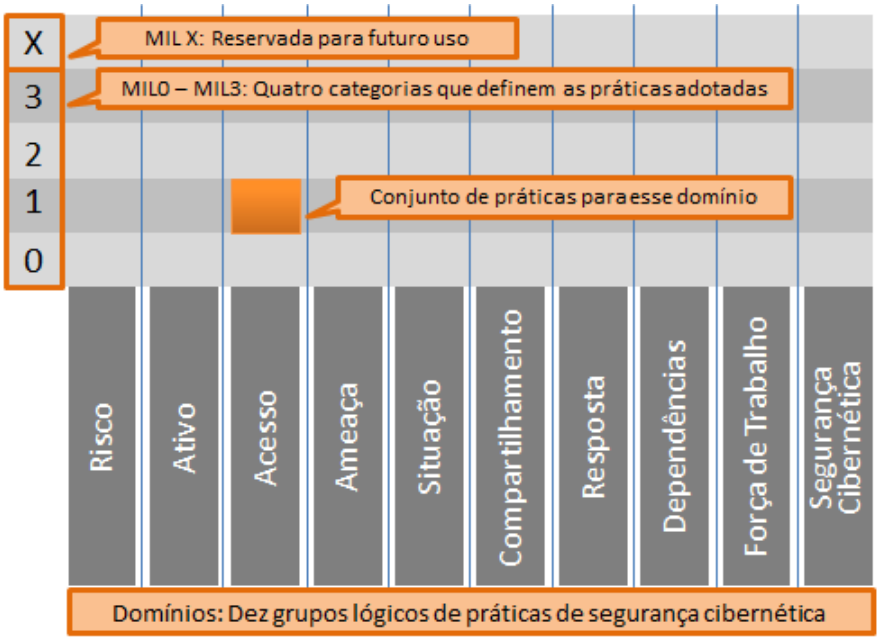
1. Reforçar as medidas de segurança cibernética do setor de eletricidade;
2. Permitir que os concessionários avaliem de forma eficaz e consistente suas ações de segurança e compará-las com outras empresas do setor;
3. Compartilhar conhecimentos, melhorar as práticas e obter referências relevantes para melhorar a segurança cibernética;
4. Permitir que as concessionárias priorizem suas ações e investimentos para melhorar a segurança cibernética.

A figura a seguir mostra uma abstração da topologia da rede do sistema elétrico. Através do modelo, a "função" é usada para descrever o conjunto de atividades que devem ser analisadas pelas concessionárias ou empresas que integram a rede de geração, transmissão, distribuição e mercados.



Arquitetura do Modelo

O modelo é organizado dentro de dez domínios e quatro indicadores de níveis de maturidade (MILs). A figura abaixo mostra a estrutura básica do modelo como uma matriz, os domínios como colunas e o MILs como linhas.



Gestão de Risco (RISCO)

Estabelecer, operar e manter um programa de gerenciamento de riscos de segurança cibernética da empresa para identificar, analisar e mitigar os riscos da organização, incluindo o seu próprio negócio, sua infraestrutura e outras partes interessadas. O domínio RISCO compreende três objetivos:

1. Estabelecer a estratégia de gestão de riscos de segurança cibernética
2. Gerenciar os riscos de segurança cibernética
3. Gerenciar as atividades de risco

Ativo, Mudança, Configuração e Gerenciamento (ATIVO)

Gerenciar as operações de tecnologia (OT) e tecnologia da informação (TI) dos ativos da organização (hardware e software) para compatibilizar os riscos da infraestrutura com os objetivos organizacionais. O domínio ATIVO é composto por quatro objetivos:

1. Gerenciar o inventário de ativos
2. Gerenciar a configuração dos ativos
3. Gerenciar as mudanças nos ativos
4. Gerenciar as atividades

Gerenciamento de Identidade e Acesso (ACESSO)

Criar e gerenciar as identidades das entidades que podem ter acesso físico ou lógico aos ativos da organização. O domínio ACESSO compreende três objetivos:

1. Estabelecer e manter as identidades das entidades
2. Controlar os acessos

3. Gerenciar as atividades

Gerenciamento das ameaças e vulnerabilidades (AMEAÇA)

Estabelecer e manter planos, procedimentos e tecnologias para detectar, identificar, analisar, gerenciar e responder as ameaças e vulnerabilidades de segurança cibernética. O domínio AMEAÇA compreende três objetivos:

1. Identificar e responder às ameaças
2. Reduzir as vulnerabilidades de segurança cibernética
3. Gerenciar as atividades

Consciência Situacional (SITUAÇÃO)

Estabelecer e manter atividades e tecnologias para coletar, analisar, detectar, usar o sistema de energia e as informações sobre segurança cibernética, incluindo a situação e as informações dos outros domínios do modelo, para formar um quadro operacional comum, compatível com o risco da infraestrutura crítica e objetivos organizacionais. O domínio SITUAÇÃO compreende quatro objetivos:

1. Fazer o registro
2. Monitorar as funções
3. Estabelecer e manter um quadro operacional comum
4. Gerenciar as atividades

Compartilhamento de Informações e Comunicações (COMPARTILHAMENTO)

Estabelecer e manter o relacionamento com entidades internas e externas para coletar e fornecer informações sobre segurança cibernética, incluindo as ameaças e vulnerabilidades, para reduzir os riscos e aumentar a resiliência operacional, compatível com o risco da infraestrutura crítica e os objetivos organizacionais. O domínio COMPARTILHAMENTO compreende dois objetivos:

1. Compartilhar as informações de segurança cibernética
2. Gerenciar as atividades

Evento e Resposta aos Incidentes, Continuidade de Operações (RESPOSTA)

Estabelecer e manter planos, procedimentos e tecnologias para detectar, analisar e responder aos eventos de segurança cibernética para apoiar as operações ao longo de um evento de segurança cibernética, proporcional ao risco da infraestrutura crítica e dos objetivos organizacionais. O domínio RESPOSTA é composto por cinco objetivos:

1. Detectar os eventos cibernéticos
2. Escalar os eventos cibernéticos
3. Responder aos eventos cibernéticos escalados
4. Plano de Continuidade
5. Gerenciar as atividades

Cadeia de fornecedores e gerenciamento das dependências externas (DEPENDÊNCIA)

Estabelecer e manter controles para gerenciar os riscos associados aos serviços de segurança cibernética e dos ativos que são dependentes de entidades externas, compatível com o risco da infraestrutura crítica e dos objetivos organizacionais. O domínio DEPENDÊNCIA compreende três objetivos:

1. Identificar as dependências
2. Gerenciar os riscos das dependências
3. Gerenciar as atividades

Gerenciamento da força de trabalho (FORÇA DE TRABALHO)

Estabelecer e manter planos, procedimento, tecnologias e controles para criar uma cultura de segurança cibernética para assegurar a adequação permanente e competência do pessoal, proporcional ao risco da infraestrutura crítica e dos objetivos organizacionais. O domínio FORÇA DE TRABALHO compreende cinco objetivos:

1. Atribuir responsabilidades à segurança cibernética
2. Controlar o ciclo de vida da força de trabalho
3. Desenvolver a força de trabalho
4. Aumentar a consciência sobre segurança cibernética
5. Gerenciar as atividades

Programa de Gestão de Segurança Cibernética (SEGURANÇA CIBERNÉTICA)

Estabelecer e manter um programa de segurança cibernética na empresa que forneça a governança, planejamento estratégico, e o patrocínio das atividades de segurança cibernética da organização de forma a alinha os objetivos de segurança cibernética com os objetivos estratégicos da organização e do risco da infraestrutura crítica. O domínio SEGURANÇA CIBERNÉTICA compreende cinco objetivos:

1. Estabelecer estratégia do programa de segurança cibernética
2. Eleger um patrocinador do programa de segurança cibernética
3. Estabelecer e manter a arquitetura de segurança cibernética
4. Desenvolver e utilizar um software seguro
5. Gerenciar as atividades

O modelo define quatro indicadores de níveis de maturidade: MIL0, incompleto; MIL1, inicial; MIL2, implantado; e, MIL3, gerenciado.

Os indicadores de níveis de maturidade são importantes para a ANEEL conhecer os riscos das infraestruturas das concessionárias e exigir iniciativas de mitigação. Para os investidores é importante conhece-los para reduzir o risco dos seus investimentos.

Artigo

Gestão de Risco em Infraestruturas de Smart Grid

Um incidente é resultado de uma sequência de falhas. Incidentes geram perdas financeiras e desgastam a imagem das organizações. Em ambientes Smart Grid que envolvem milhões de dispositivos físicos e componentes de softwares, é necessária uma nova abordagem de gestão de risco. A monitoração e a análise de risco devem ser em tempo real.

O primeiro grande desafio em sistemas complexos de Smart Grid é determinar dentro da infraestrutura quais os componentes devem ser monitorados e seu grau de criticidade, que é composto pelo tipo de ameaça, condições para iniciar uma ameaça, a probabilidade de ocorrência e o impacto nos negócios. Essa análise em sistemas complexos deve ter o apoio de softwares especializados.

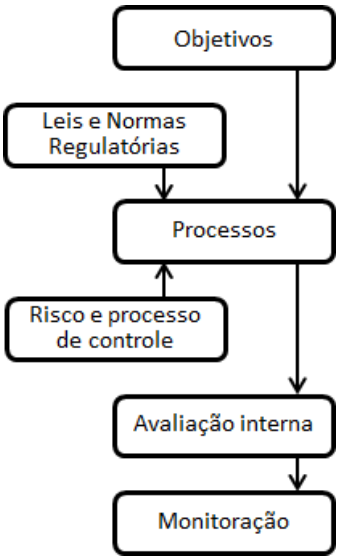
Essa análise considera os processos para o restabelecimento do serviço do componente e ações de contorno, além do tempo entre falhas e seus tempos de recuperação. Os softwares de análise não conseguem identificar processos ineficientes, sendo necessários outros estudos para determinar o processo ótimo de operação.

Todo o processo envolve risco, cabe aos gestores tornar transparente o impacto gerado por uma falha e buscar o equilíbrio financeiro para os investimentos de mitigação.

Dentro de um processo de gestão de risco temos que considerar os seguintes pontos:

- **Ambiente interno**. A cultura de risco de uma organização define como o risco será visto e tratado. Isso incluir a filosofia de gestão de risco, o apetite pelo risco, à integridade e valores éticos e o ambiente em que são operados.
- **Definição de objetivos**. Sem objetivos claramente definidos é impossível identificar os eventos que podem afetar os negócios e impedir que os objetivos organizacionais sejam alcançados.
- **Identificação de eventos**. É possível definir oportunidades e ameaças identificando eventos interno e externos que influenciam na realização de um objetivo organizacional.
- **Avaliação de risco**. Os riscos são analisados e considerados a probabilidade de ocorrência e o impacto que isso causará na organização.
- **Resposta ao risco**. Várias ações podem ser tomadas quando da ocorrência de um risco. Os riscos podem ser evitados, aceitos, reduzidos ou compartilhados. Os gestores devem selecionar que a melhor opção para a organização.
- **Controle de atividades**. Procedimentos devem ser estabelecidos e implementados para auxiliar nas respostas aos riscos. Devem existir controles para avaliar a mitigação dos riscos, as visões dos gestores, relatórios, controles físicos e controles de desempenho.
- **Monitoração**. Todos os processos e componentes devem ser monitorados para assegurar sua execução e para coletar informações para ações de melhoria contínua.
- **Informação e comunicação**. Informações relevantes devem ser identificadas e comunicadas para forma apropriada e no tempo correto para que as pessoas responsáveis possam tomar ações dentro de suas competências para evitar a ocorrência de incidentes.

A figura a seguir apresenta o fluxo de definição do processo e as etapas de avaliação de risco, avaliação interna e monitoração. A partir desse fluxo é possível definir responsáveis, alocação de recursos e ferramentas para a governança dos processos.



A definição dos objetivos está ligada as metas de negócio da organização e das unidades de negócios. As leis e normas regulatórias devem ser consideradas para a definição do processo.

As metas geram os indicadores de desempenho dos processos. Para atingir as metas estabelecidas é necessários conhecer os riscos e tomar ações para gerenciá-los (evitar, reduzir, aceitar ou compartilhar). Frequentemente, os processos devem ser submetidos a uma avaliação interna e monitorados para assegurar sua execução e coletar informações para melhoria contínua.

Uma boa prática é incluir os objetivos no modelo BSC – *Balanced Scorecard* – de gestão da estratégia.

Para desenvolvimento e gestão de processos para Smart Grid várias ferramentas e metodologias devem ser utilizadas buscando excelência operacional.

- Software de desenho e simulação de processos.
- Software de governança, gestão de risco e conformidade.
- Software de gestão de ativos.
- Software de gestão de eventos do ambiente de Smart Grid.
- Software de gestão de portfólio de projetos.
- Metodologia de melhoria contínua para processos e mitigação de riscos operacionais.
- Software de Business Intelligence e Big Data.

Resumindo, o novo ambiente de Smart Grid exige um novo modelo de gestão risco com monitoração e análises em tempo real, detectando e avaliando mudanças do comportamento do sistema para evitar ataques cibernéticos e se antecipar a incidentes que podem paralisar alguns serviços. Essa nova abordagem exige novos desenhos de processos, softwares, metodologias de desenho de processos e novas tecnologias de análise de grandes volumes de dados em tempo real (Big Data).

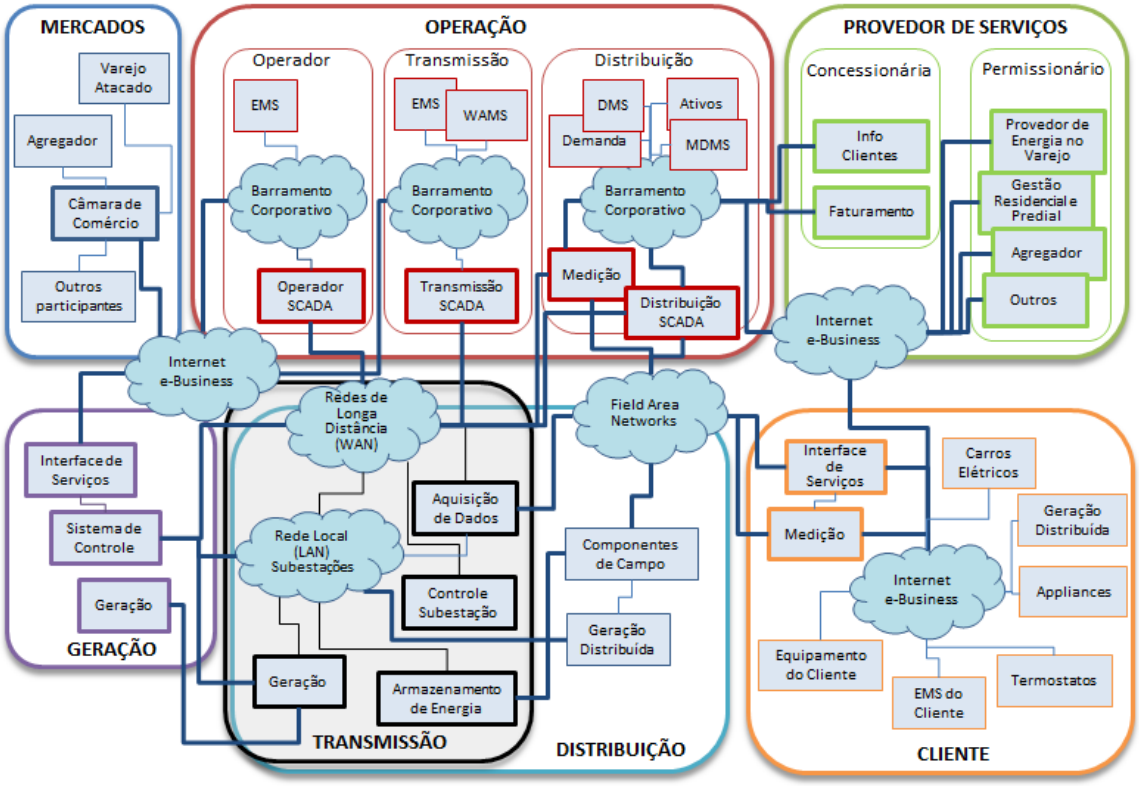
Artigo

A complexidade da troca de dados no setor elétrico gera um risco operacional

A gestão de um sistema elétrico é complexa em função da necessidade da troca intensa de dados entre os atores do sistema. Essa complexidade aumentará com a introdução de novos projetos de Smart Grid na distribuição e o aumento da micro e mini geração de energia pelos clientes. O aumento da complexidade do sistema gera um maior risco operacional. A quebra de confidencialidade e integridade dos dados ou a indisponibilidade de uma informação no momento certo pode comprometer todo o sistema e prejudicar milhões de consumidores.

O sistema elétrico é composto, basicamente, por sete domínios: geração, transmissão, distribuição, operação, provedores de serviços, mercado e clientes. Uma operação integrada requer a troca intensa de dados entre sistemas que geram ações automáticas ou manuais para o gerenciamento do sistema elétrico.

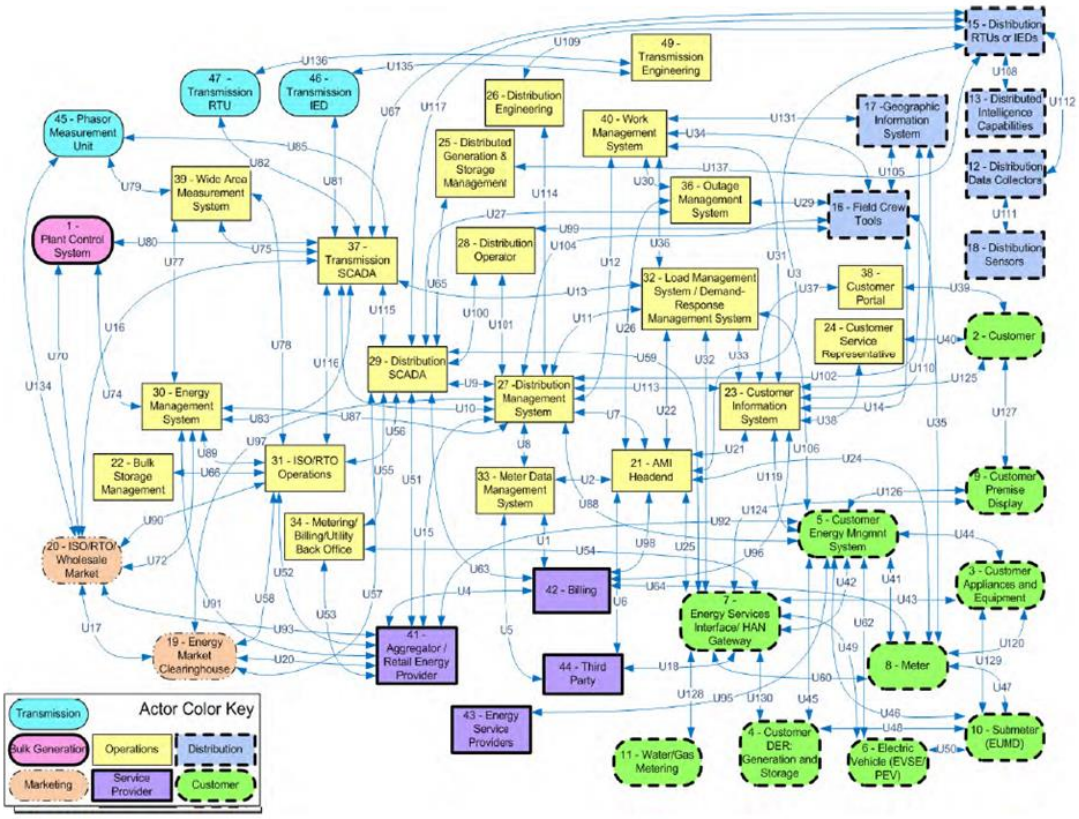
A figura a seguir mostra uma visão simplificada dos principais componentes do sistema elétrico, os softwares e a integração necessária para operar o sistema. Esse modelo se aplica a todas as empresas que compõem o sistema elétrico integrado.



O sistema envolve vários softwares e tecnologias de transmissão de dados e são definidos pelas empresas participantes do sistema. O único requisito é a padronização do formato de dados trocados e o tempo necessário de atualização. Isso requer das empresas a transformação dos formatos internos para o formato padrão, os chamados gateways.

A troca de dados entre a geração, transmissão, distribuição e operação são criticas e podem comprometer a confiabilidade do sistema. Basta um ator gerar informações falsas que todo o sistema será afetado. Se um hacker encontrar um único ponto vulnerável todo o sistema poderá ser comprometido.

A figura a seguir mostra a complexidade das interfaces de troca de dados entre os principais sistemas do setor elétrico. Cada interface deve ser padronizada, por tanto de domínio público, para garantir a confiabilidade do sistema como um todo.



É necessário garantir que todas as empresas tenham um nível de proteção e monitoração da segurança da informação que evite a ação de hackers. O desafio é grande, pois os investimentos em segurança competem com projetos de expansão e melhoria no sistema físico da rede.

Um projeto de segurança para o setor elétrico começa com a necessidade de alta disponibilidade dos computadores do Data Center da empresa. A infraestrutura do Data Center (computadores, sistema de refrigeração e energia) deve ser redundante e ter a capacidade de operar em pouquíssimo tempo em outra localidade em caso de falha do data center principal.

Os sistemas de comunicação devem dispor de no mínimo duas conexões com fornecedores, infraestrutura independente e rota física distinta entre um ponto e outro. Isso garante, por exemplo, que se um cabo de fibra em um trecho for rompido exista uma rota alternativa para o encaminhamento dos dados.

Periodicamente, o sistema deve ser submetido a um teste integrado para identificar possíveis pontos de falha. Esses testes devem ser realizados primeiro nas empresas e depois no sistema como um todo, coordenado por algum órgão regulador. Isso é necessário, pois as mudanças nos sistemas são frequentes para corrigir falhar, atualização de versão de software ou para atender a requerimentos regulatórios.

Um ponto importante nesse contexto é o gerenciamento e a proteção das interfaces de troca de dados. O gerenciamento é necessário para garantir e monitorar se os sistemas estão enviando os dados dentro dos prazos estabelecidos e a proteção é vital para evitar a quebra de confidencialidade e integridade dos dados.

No mercado livre de energia a troca de informações entre as câmaras de comércio (CCEE, Câmara de Comercialização de Energia Elétrica e o BBCE, Balcão Brasileiro de

Comercialização de Energia) e os consumidores deve ser segura e ter alta disponibilidade. Por envolver leilões de energia e trafegar informações financeiras, a confidencialidade dos dados é crítica para a confiabilidade do sistema. Por exemplo, o BBCE operar com um sistema nativo de certificado digital para garantir o não repúdio das operações, ou seja, é possível comprovar legalmente que um agente executou uma transação.

Alguns estudos indicam que o volume de dados das concessionárias de distribuição aumentará quase 3.000 vezes com a implantação de projetos de Smart Grid. Esse aumento é em função da coleta de dados frequente dos medidores eletrônicos dos consumidores. O gerenciamento desse grande volume de dados só será possível com o uso de novas tecnologias de banco de dados, como Big Data.

Resumindo, o avanço da automação no setor elétrico trará vantagens enormes para o setor, porém os gestores deverão investir em segurança da informação para manter os sistemas seguros, íntegros e disponíveis.

Artigo

Segurança nas Redes Elétricas Inteligentes

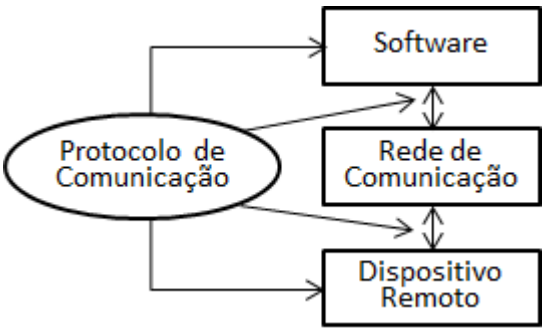
Não há dúvidas dos grandes benefícios das redes inteligentes de energia elétrica. A automação do sistema elétrico não é novidade, há anos as concessionárias de energia elétrica e grandes fábricas utilizam sistemas de gerenciamento e controle dos dispositivos de proteção, geração e transmissão. A novidade é a massificação do uso da automação na distribuição de energia elétrica chegando à casa do assinante.

Em ambientes fechados e controlados a maior preocupação era a excelência operacional do sistema SCADA (Sistema de Supervisão e Aquisição de Dados). As redes de comunicação eram fechadas com links dedicados. A segurança do sistema era entendida como adequada pela complexidade do sistema, pouquíssimas pessoas qualificadas na área e difícil acesso ao sistema.

Com a implantação do Smart Grid na distribuição cobrindo, literalmente milhões de assinantes, é necessário utilizar redes de comunicação públicas e instalar os dispositivos remotos (sensores, controladores, disjuntores e medidores eletrônicos) em postes e na casa dos assinantes. O rápido desenvolvimento da Internet criou uma legião de programadores e, infelizmente, pessoas e organizações com o objetivo de roubar informações e destruir os sistemas por várias motivações, o chamado cyber terrorismo.

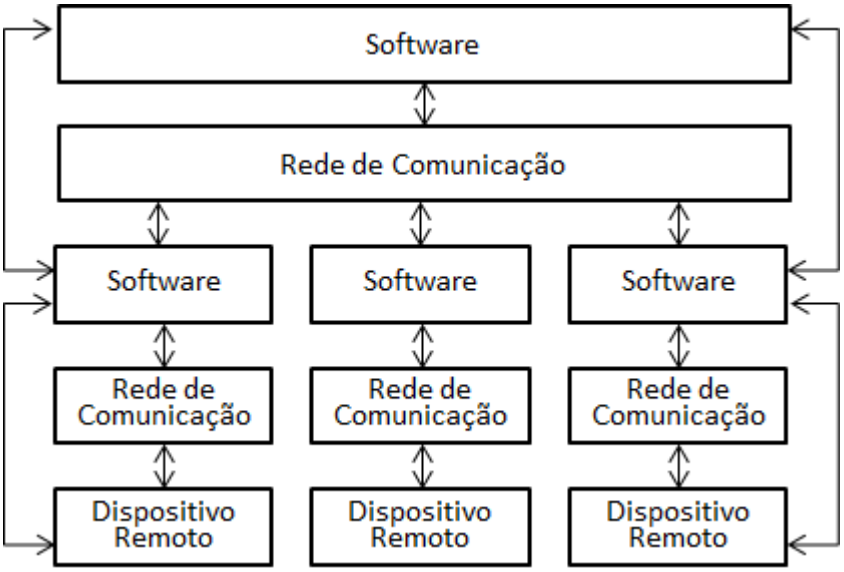
O grande desafio das concessionárias de distribuição e da indústria de equipamentos para Smart Grid é adequar a tecnologia e as questões de segurança da informação, mantendo o desempenho dos sistemas críticos com a melhor relação custo/benefício possível.

Para tornar viáveis os projetos de Smart Grid, tanto do ponto de vista financeiro como técnico, é fundamental o uso de padrões de mercado para software e processos de gestão. A utilização de padrões permite a implantação de projetos com diferentes equipamentos de fornecedores com a interoperabilidade dos seus componentes assegurada pelas normas.



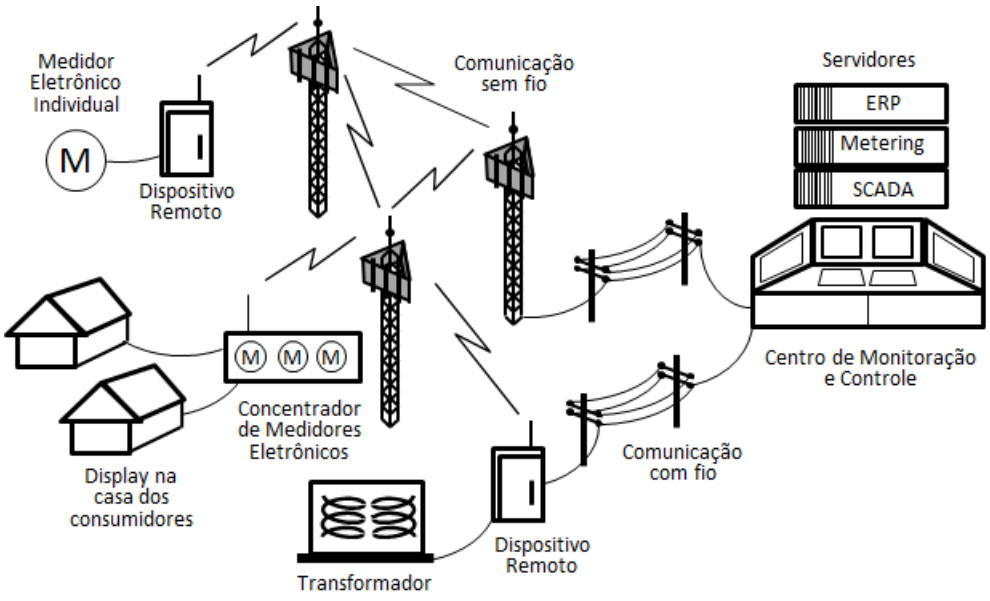
Uma visão simplificada de protocolos de redes de comunicação e computadores é apresentada na figura acima. A troca de mensagens entre o software de gerenciamento e o software no dispositivo remoto é realizada com o uso de diversos protocolos que dividem uma mensagem em pequenos pacotes de dados para transmiti-los. Usa-se o conceito de camadas de protocolo, cada camada tem uma parte da responsabilidade da transmissão de dados. O número de camadas e responsabilidades é idêntico do lado do transmissor e do receptor.

Uma rede complexa pode ter várias camadas de software com diferentes especializações dentro do conceito de hierarquia, como mostra a figura abaixo.



Uma das normas que apoia o desenho de projetos de Smart Grid é a IEC 61.850 para automação das subestações. Para a conexão de medidores eletrônicos e sensores massivamente dispersos geograficamente uma alternativa é o padrão aberto IPv6 (evolução do endereçamento IPv4 com regras de segurança), padrão de pacote seguro IPsec e a norma X.509 para segurança de mensagens.

A figura a seguir mostra uma rede de comunicação para a automação do controle de uma subestação e medidores eletrônicos, remotamente.



No exemplo, o dispositivo remoto para controle do transformador da subestação tem duas conexões de rede, com e sem fio. Essa redundância é importante para não interromper o serviço em caso de falha de uma das conexões.

A comunicação sem fio utiliza o conceito de mesh, onde cada estação base (ERB) pode se comunicar com sua adjacente de forma independente, aumentando a disponibilidade e confiabilidade da rede. Usando a rede sem fio são conectados os concentradores de medidores eletrônicos e medidores individuais.

Os displays que mostram o consumo de energia para o consumidor, exigido pela regulamentação, é feito usando comunicação de dados através da linha de energia, via PLC (Power Line Communication).

O sistema todo é controlado a partir de um Centro de Monitoração e Controle apoiado por sistemas de medição bidirecional (AMI – *Advanced Metering Infrastructure*), sistemas de supervisão e aquisição de dados (SCADA) e o sistema de gestão integrado (ERP) da empresa.

A configuração dos dispositivos é realizada por uma linguagem padronizada pela IEC 61.850 com base no XML (*Extensible Markup Language*) que define as regras de formato de um documento.

Veja na figura a seguri, um exemplo de configuração de dispositivos de controle de subestações.

```xml
<?xml version="1.0"?>
<SCL xmlns:sxy="http://www.iec.ch/61850/sclcoordinates001" xmlns="http://www.iec.ch/61850/2003/SCL">
<Header id="svc" toolID="SSI-Tool" nameStructure="IEDName" />
<Substation name="AA1" desc="Substation">
<VoltageLevel name="A1" desc="Voltage Level">
<Bay name="A01" desc="Bay" sxy:dir="horizontal">
<LNode iedName="AA1TH1" ldInst="LD0" lnClass="LPHD" lnInst="1" />
<LNode iedName="AA1TH1" ldInst="LD0" lnClass="ITCI" lnInst="1" />
<LNode iedName="AA1TH1" ldInst="LD0" lnClass="LLN0" lnInst="" />
</Bay>
</VoltageLevel>
<VoltageLevel name="C1" desc="Voltage Level">
<Voltage multiplier="k" unit="V">380</Voltage>
</VoltageLevel>
<VoltageLevel name="H1" desc="Voltage Level">
<Voltage multiplier="k" unit="V">33</Voltage>
<Bay name="Q03" desc="Trafo LV" sxy:x="54" sxy:y="33" sxy:dir="vertical">
<ConductingEquipment name="QA1" desc="Circuit Breaker" type="CBR" sxy:x="7" sxy:y="8" sxy:dir="vertical">
<Terminal connectivityNode="AA1/H1/Q03/N1" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N1" />
<Terminal connectivityNode="AA1/H1/Q03/N5" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N5" />
</ConductingEquipment>
<ConductingEquipment name="BU1" desc="Voltage Transformer 2 Sec. 3 Phase" type="VTR" sxy:x="4" sxy:y="24">
<Terminal connectivityNode="AA1/H1/Q03/N6" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N6" />
</ConductingEquipment>
<ConductingEquipment name="TrafoLV" desc="Line In/Out" type="IFL" sxy:x="7" sxy:y="26" sxy:dir="vertical">
<Terminal connectivityNode="AA1/H1/Q03/N6" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N6" />
</ConductingEquipment>
<ConductingEquipment name="BI1.2" desc="Current Transformer" type="CTR" sxy:x="7" sxy:y="12" sxy:dir="vertical">
<Terminal connectivityNode="AA1/H1/Q03/N3" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N3" />
<Terminal connectivityNode="AA1/H1/Q03/N4" substationName="AA1" voltageLevelName="H1" bayName="Q03" cNodeName="N4" />
</ConductingEquipment>
```


Como podemos observar a padronização traz grandes vantagens para a implementação de sistemas Smart Grid. Entretanto, a exposição do modelo para o público em geral cria um risco potencial de segurança.

Por exemplo, a ANATEL licenciou a frequência de 3.590MHz para o uso da tecnologia de transmissão de dados WiMax. A faixa de frequência licenciada tem largura de banda 10 MHz e potência de 2 Watts em cada antena xPol com 14 dBi de ganho e tilt típico de 4 graus. Conhecendo essas características que são públicas, um hacker pode construir um transmissor de alta potencia usando um chipsets de WiMax para interferir no sinal da rede em uma localidade. Se esse transmissor estiver em um veículo em movimento será quase impossível sua detecção e apreensão.

Outro exemplo é o acesso de um hacker aos parâmetros de configuração dos dispositivos de controle para alterar seu comportamento. O envio de comandos e a inibição de alertas de controle podem danificar um transformador e tirá-lo de operação por um longo período, comprometendo o serviço para milhares de consumidores.

Outra situação grave é a quebra de integridade dos dados de bilhetagem dos medidores eletrônicos. Se um hacker tiver acesso aos registradores (memória) do medidor, ele poderá alterar os valores de medição. Para menos, se ele quiser se beneficiar pagando valores menores. Para mais, se ele quiser comprometer a confiança da concessionária entre os órgãos públicos e consumidores.

Seja por interferência física ou lógica, os sistemas de Smart Grid são inseguros.

A alternativa para tornar o sistema mais confiável é realizar um projeto levando em conta a segurança da informação, realizar verificações de conformidade frequentes e utilizar softwares especialistas de análise de comportamento do sistema em tempo real.

Anexo II

Projeto

Geração Distribuída de Energia através de Painéis Fotovoltaicos (Planta Tipo – 1MWp)

Desenvolvemos o projeto baseado na resolução normativa nº 482, de abril de 2012 que estabelece as condições gerais para o acesso de microgeração e minigeração distribuída aos sistemas de distribuição de energia elétrica e o sistema de compensação de energia elétrica;

Especificação do Projeto

1. A Planta Tipo 1MWp será instalada no solo com layout adaptável a topologia do local;
2. A operação da planta está projetada para uma vida útil mínima de 25 anos;
3. O nível de tensão de conexão da central geradora será 13,8 ou 34,5 kV, dependendo da tensão nominal da rede de distribuição acessada;
4. O projeto prevê, inicialmente, 3.800 módulos fotovoltaicos de 270/280W com células de silício cristalino, agrupados em painéis com 24 módulos com base fixa;
5. A ligação elétrica dos módulos deve ser projetada para obter o melhor desempenho de funcionamento do inversor;
6. A distância mínima entre os painéis fotovoltaicos deve garantir a ausência de sombra, ventilação para resfriamento, limpeza e manutenção preventiva e corretiva;
7. Cada estrutura de painel fotovoltaico deve incorporar um recipiente de repelente de aves. A localização deve ser selecionada para evitar o efeito sombra;
8. A estrutura de suporte dos painéis fotovoltaicos deve ser fabricada utilizando material resistente à corrosão, assim como soldas e fechos;
9. A estrutura de suporte deve estar livre de corrosão quando instalada;
10. Os módulos fotovoltaicos devem ser fixados à estrutura de suporte do painel usando parafusos de aperto e/ou grampos metálicos. Os parafusos de aperto devem utilizar os furos de montagem fornecidos pelo fabricante do módulo.
11. Fixadores dos módulos e braçadeiras devem ser adequadamente tratados para resistir à corrosão;
12. A estrutura de suporte deve suportar cargas de vento de até 150 km/h;
13. Os módulos devem ser montados nos painéis com espaçamento adequado para melhorar a resistência ao vento;
14. As fundações para fixação dos painéis fotovoltaicos devem ser projetadas para suportar o esforço mecânico máximo dos painéis fotovoltaicos;
15. O inversor deve atender aos requisitos estabelecidos no Projeto de Norma ABNT NBR 03:082.01-003 e, posteriormente, na norma ABNT NBR a que ele der origem;
16. O inversor deve ter certificação INMETRO. Excepcionalmente, até que o processo de etiquetagem por parte do INMETRO esteja consolidado, poderão ser aceitos inversores que apresentem certificados de laboratórios internacionais acreditados pelo INMETRO, atestando que os requisitos da norma ABNT citada foram atendidos;

17. O inversor deve estar equipado com todas as proteções, tais como DC e AC, isolamento DC, proteção contra surtos e proteção anti-ilhamento. Uma placa de sincronismo, que detecta a tensão de entrada trifásica a partir do transformador de rede para sincronizar com o sistema. Deve ter função MPPT (*Maximum power point tracking*) para maximizar a geração de energia a partir dos painéis solares conectados a ele.
18. O inversor deverá exibir a tensão da matriz dos painéis fotovoltaicos DC, corrente e potência, tensão de saída AC e corrente nas três fases, AC (ativo, reativo e aparente), fator de potência e de energia AC (três fases e acumulativa). Deverá permitir o monitoramento remoto;
19. O inversor deve incluir arranjos adequados de refrigeração interna (exaustor e dutos) para operação em um ambiente não climatizado;
20. Deverá ser utilizada uma fonte auxiliar para alimentação do sistema de proteção. Para tanto deverá ser utilizado um sistema "no-break" com potência mínima de 1000 VA e autonomia de 2 horas, de forma que não haja interrupção na alimentação do sistema de proteção. Opcionalmente poderá ser instalado um conjunto de baterias para suprir uma eventual ausência do "no-break". Adicionalmente deverá ser previsto o trip capacitivo;
21. Os inversores deverão seguir as diretrizes abaixo:
    - Quando a frequência da rede assumir valores abaixo de 57,5 Hz, o sistema de geração distribuída deve cessar o fornecimento de energia à rede elétrica em até 0,2 s. O sistema somente deve voltar a fornecer energia à rede quando a frequência retornar para 59,9 Hz, respeitando um tempo de reconexão mínimo de 180 s após a retomada das condições normais de tensão e frequência da rede.
    - Quando a frequência da rede ultrapassar 60,5 Hz e permanecer abaixo de 62 Hz, o sistema de geração distribuída deve reduzir a potência ativa injetada na rede segundo a equação:

      $$\Delta P = [f_{\text{rede}} - (f_{\text{nominal}} + 0{,}5)] \times R$$

      Sendo:

      ΔP é variação da potência ativa injetada (em %) em relação à potência ativa injetada no momento em que a frequência excede 60,5 Hz (PM);

      f rede é a frequência da rede;

      f nominal é a frequência nominal da rede;

      R é a taxa de redução desejada da potência ativa injetada (em %/Hz), ajustada em - 40 %/Hz. A resolução da medição de frequência deve ser ≤ 0,01 Hz.

    - Se, após iniciado o processo de redução da potência ativa, a frequência da rede reduzir, o sistema de geração distribuída deve manter o menor valor de potência ativa atingido (PM – ΔP Máximo) durante o aumento da frequência. O sistema de geração distribuída só deve aumentar a potência ativa injetada quando a frequência da rede retornar para a faixa 60 Hz ± 0,05 Hz, por no mínimo 300 segundos. O gradiente de elevação da potência ativa injetada na rede deve ser de até 20 % de PM por minuto.
    - Quando a frequência da rede ultrapassar 62 Hz, o sistema de geração distribuída deve cessar de fornecer energia à rede elétrica em até 0,2 s. O sistema somente

deve voltar a fornecer energia à rede quando a frequência retornar para 60,1 Hz. O gradiente de elevação da potência ativa injetada na rede deve ser de até 20 % de PM por minuto.

22. Resposta às condições anormais de tensão para geração com inversores:

Tensão no ponto de conexão comum (% em relação à $V_{nominal}$)	Tempo máximo de desligamento (1)
V < 80%	0,4 s
80% ≤ V ≤ 110%	Regime normal de operação
110% < V	0,2 s

(1) O tempo máximo de desligamento refere-se ao tempo entre o evento anormal de tensão e a atuação do sistema de geração distribuída (cessar o fornecimento de energia para a rede). O sistema de geração distribuída deve permanecer conectado à rede, a fim de monitorar os parâmetros da rede e permitir a "reconexão" do sistema quando as condições normais forem restabelecidas.

23. O sistema de geração distribuída deve parar de fornecer energia à rede em 1 s se a injeção de componente c.c. na rede elétrica for superior a 0,5 % da corrente nominal do sistema de geração distribuída;
24. A tensão de saída do inversor deve apresentar a melhor relação custo/benefício para a conexão com o transformador de acoplamento;
25. O transformador de acoplamento deve ser protegido por disjuntor ou religador com função de religamento bloqueada;
26. Características básicas do transformador de acoplamento:

Potência de geração (kW)	Transformador de acoplamento				
	Potência mínima (kVA)	Lado do Acessante		Lado da Concessionária	
		Tensão nominal (V)	Conexão das bobinas	Tensão nominal (V)	Conexão das bobinas
75,1 a 100	112,5	380/222 ou 220/127	Delta	13,8 ou 34,5	Estrêla com neutro acessível e solidamente aterrado
100,1 a 128	150				
128,1 a 192	225				
192,1 a 255	300				
255,1 a 425	500				
425,1 a 638	750				
638,1 a 850	1000				

Obs: considerou-se um Fator de Potência médio de 0,85

27. O transformador de acoplamento deve sempre ter tapes fixos do lado da concessionária de distribuição com os seguintes valores (pode variar dependendo da norma da concessionária):
    - Transformador classe 15 kV - Tapes: 13.800, 13.200 e 12.600
    - Transformador classe 36 kV - Tapes: 36.200, 35.350, 34.500, 33.000 e 31.500
28. A distorção harmônica total de corrente deve ser inferior a 5 %, na potência nominal do sistema de geração distribuída;
29. A tensão no ponto de conexão em média tensão deve situar-se entre 95% e 105% da tensão nominal de operação da rede de distribuição no ponto de conexão e, ainda, coincidir com a tensão nominal de um dos terminais de derivação previamente exigido ou recomendado para o transformador;

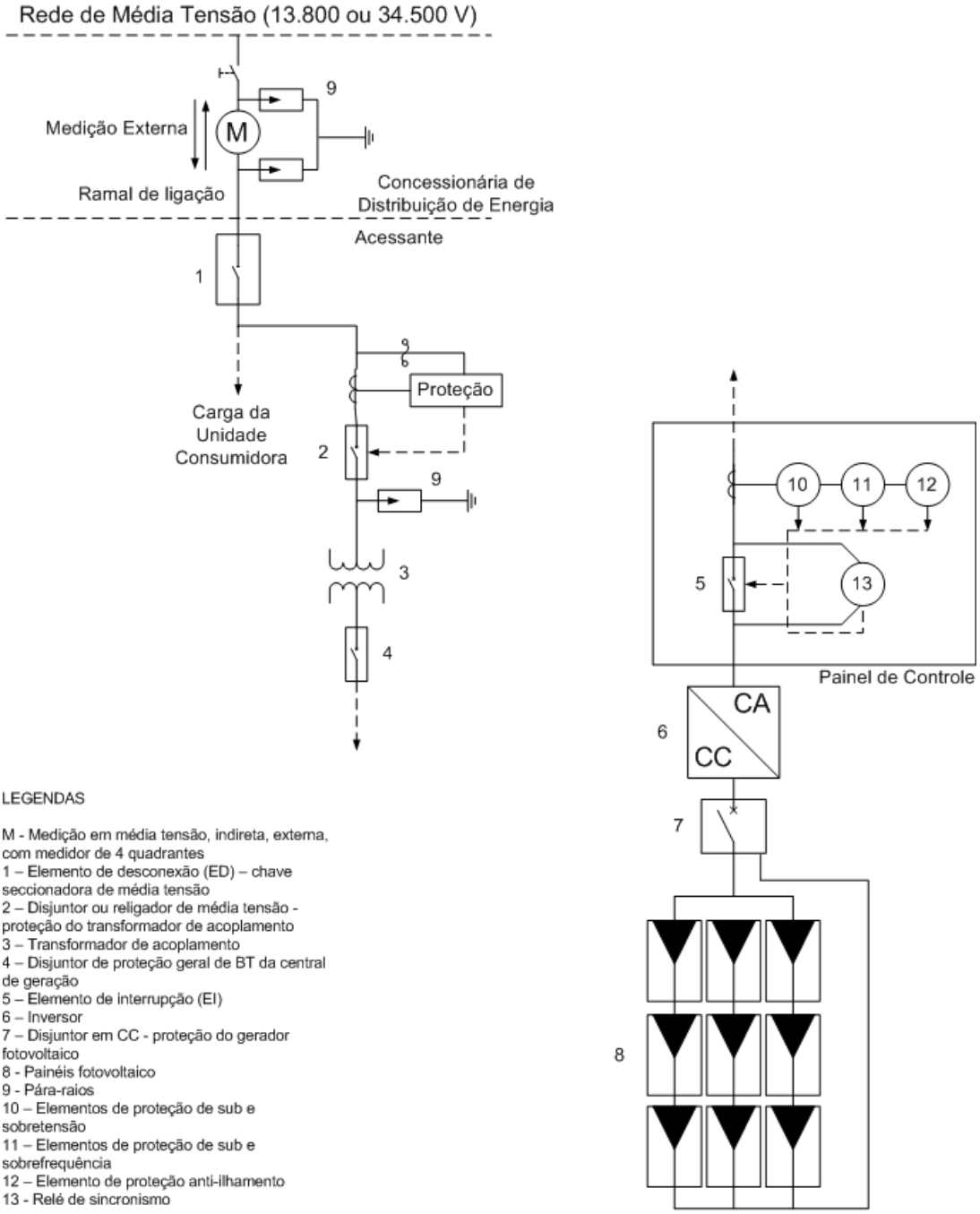
30. Limites de flutuação de tensão: devem adotar medidas para que flutuação de tensão, decorrente da operação dos equipamentos e de outros efeitos na instalação não provoque no ponto de conexão a superação dos limites individuais de Pst (*Probability Short Time*) e Plt (*Probability Long Time*) conforme tabela abaixo. Para fins de planejamento, os níveis de "flicker" na rede de distribuição devem permanecer em valores da faixa "adequado".

Valor de Referência	Pst 95% (pu)	Plt 95% (pu)
Adequado	Pst < 1,0	Plt < 0,8
Precário	1,0 ≤ Pst ≤ 2	0,8 ≤ Plt ≤ 1,6
Critico	Pst > 2,0	Plt > 1,6

31. As instalações de centrais geradoras deverão estar providas de sistemas de aterramento que garanta que em quaisquer circunstâncias não sejam geradas tensões de contato superiores aos limites estabelecidos em norma (NBR 5410).
32. Não devem ser utilizadas canalizações metálicas de água, líquidos ou gases inflamáveis como eletrodos de aterramento.
33. A matriz de painéis fotovoltaicos deve ser projetada para corresponder às especificações de entrada do inversor;
34. A matriz de painéis fotovoltaicos, equipamentos CA e CC, inversor, e fiação de distribuição devem ser aterrados, conforme necessário;
35. O aterramento deve conectar todos os componentes do sistema: recipientes de metal, caixas, quadros elétricos, chassis e painéis. O fio de ligação a terra não deve ser comutado, fundido ou interrompido;
36. O sistema de aterramento completo deve ser conectado eletricamente para fornecer retorno à terra de todo o equipamento independente de mecânica ligação;
37. Um eletrodo de aterramento separado deve ser instalado usando para teste de aterramento;
38. Os equipamentos de manobra, proteção e controle necessários para o ponto de conexão da central geradora para adesão ao sistema de compensação devem ter certificação do INMETRO, ou excepcionalmente, caso ainda não haja essa certificação, devem apresentar certificados (nacionais ou internacionais) ou declaração do fabricante que os equipamentos foram ensaiados conforme normas técnicas brasileiras, ou, na ausência, normas internacionais;
39. Se o inversor for dotado de elementos de proteção, a redundância de proteção será desnecessária;
40. Requisitos mínimos necessários para o ponto de conexão da central geradora:
    - Elemento de desconexão;
    - Elemento de interrupção;
    - Transformador de acoplamento;
    - Proteção de sub e sobrtensão;
    - Proteção de sub e sobrefrequência;
    - Proteção contra desquilíbrio de corrente;
    - Proteção contra desbalanço de tensão;
    - Proteção de sobrecorrente direcional;
    - Proteção de sobrecorrente com restrição de tensão;
    - Relé de sincronismo;
    - Proteção anti-ilhamento;
    - Estudo de curto-circuito realizado pela concessionária de distribuição;
    - Medidor de quatro quatrantes;

41. Deve ser instalado um sistema de aquisição de dados para controle e monitoramento computadorizado do sistema fotovoltaico em tempo real com armazenamento de dados para análises estatísticas. Todos os dados instantâneos serão mostrados na tela do computador.
42. Deverá ser instalado um software para acompanhamento e dados acumulativos de radiação solar da planta.

Diagrama: Conexão de geração distribuída

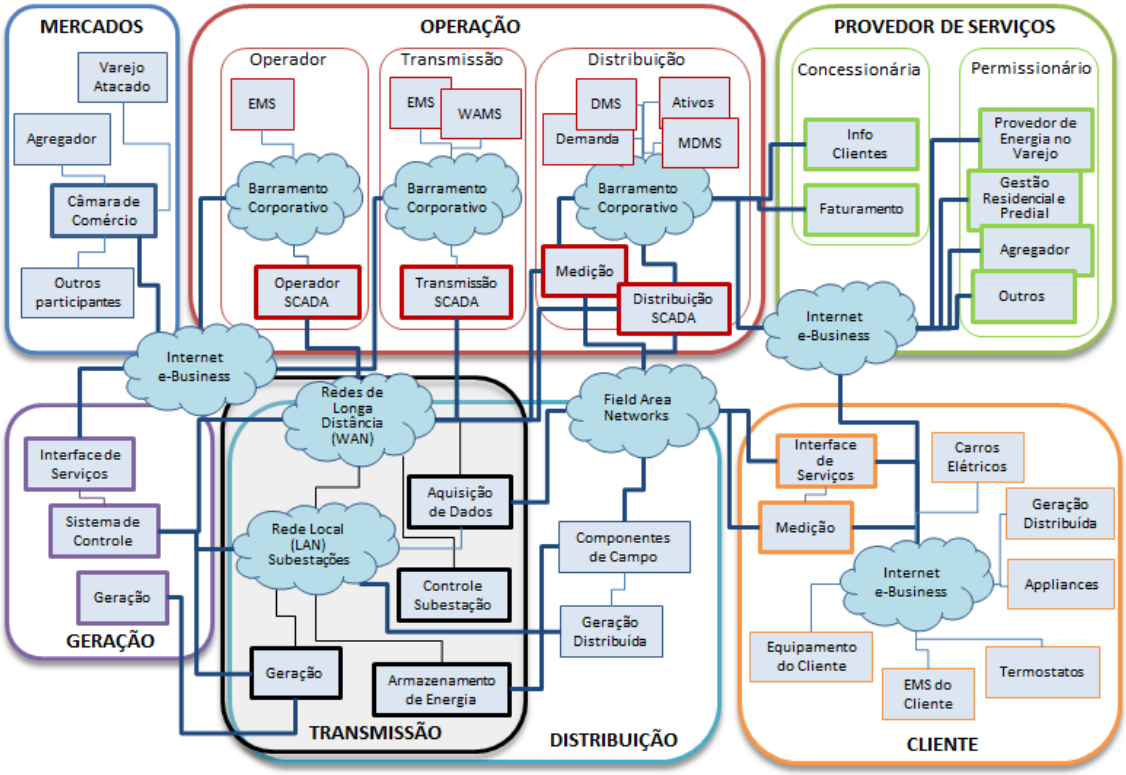


Projeto

Sistema de informação para pequenas centrais geradoras de energia elétrica

A proposta desse projeto é desenvolver um serviço na modalidade Software-as-Service (SaaS) para atender a todas as necessidades de pequenas centrais geradoras de energia elétrica. O serviço tem um grande potencial de mercado devido a adoção do conceito de geração distribuída de energia utilizando fontes renováveis, tais como solar, eólica, biomassa e de pequenas centrais hidrelétricas (PCHs). O Brasil já conta com uma regulamentação que permite que empreendedores possam investir na geração distribuída de energia até 30MW, incluindo a micro e mini geração de energia (até 1MW) com acoplamento garantido na rede de transmissão e distribuição das concessionárias. Tipicamente, cada nova planta é uma entidade jurídica independente. Cada empresa deve cumprir com todas as obrigações fiscais e trabalhistas, atender todos os requerimentos técnicos de acoplamento com a rede de transmissão e se integrar ao sistema informatizado do Operador Nacional do Sistema (ONS) para troca de dados de operação via Internet, como o despacho de carga. Uma solução SaaS nessa área é repetível e escalável, o que torna um negócio atrativo para os provedores e investidores de serviços de software.

A figura abaixo mostra os domínios de um sistema elétrico: geração, transmissão, distribuição, operação, provedor de serviços, mercados e clientes.



O serviço proposto neste projeto é atender o controle da geração e operação da planta e todo o suporte administrativo através de um ERP, considerando uma estrutura organização enxuta.

Proposta do Projeto

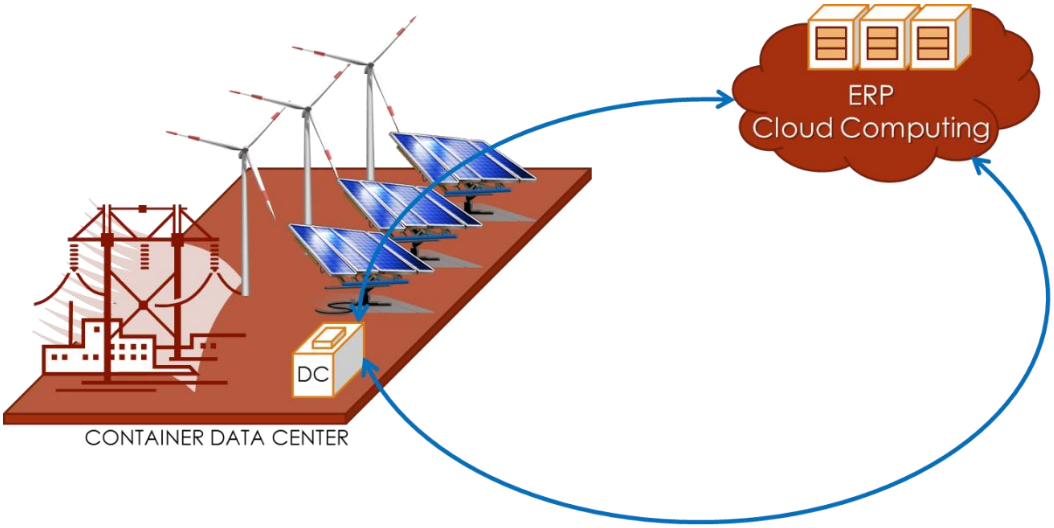
O projeto deve ser repetível e escalável, ou seja, uma mesma configuração de software deve atender a maioria das plantas de geração de energia com a menor expansão possível de

recursos de infraestrutura e pessoal. Basicamente, o projeto tem as seguintes áreas: monitoração e controle da operação da planta; integração com os sistemas do Operador Nacional do Sistema (ONS); integração com os sistemas da Câmara de Comércio de Energia Elétrica (CCEE); integração com os sistemas da concessionária de transmissão de acoplamento; e, um sistema de integrado de gestão (ERP) para os processos empresariais.

Por questões funcionais a monitoração e controle da operação na planta requer uma infraestrutura local de processamento, incluindo um data center Tier 3 de pequeno porte para instalar os servidores e sistemas de armazenamento e rede. Esse ambiente deve ter redundância de comunicação e geração de energia para contingência.

O ERP deve operar em um ambiente Cloud Computing, o que permitirá o acesso de locais diferentes e ambiente seguro de processamento.

A figura a baixo mostra uma concepção do ambiente de processamento utilizando um container data centers para minimizar os esforços de implementação.



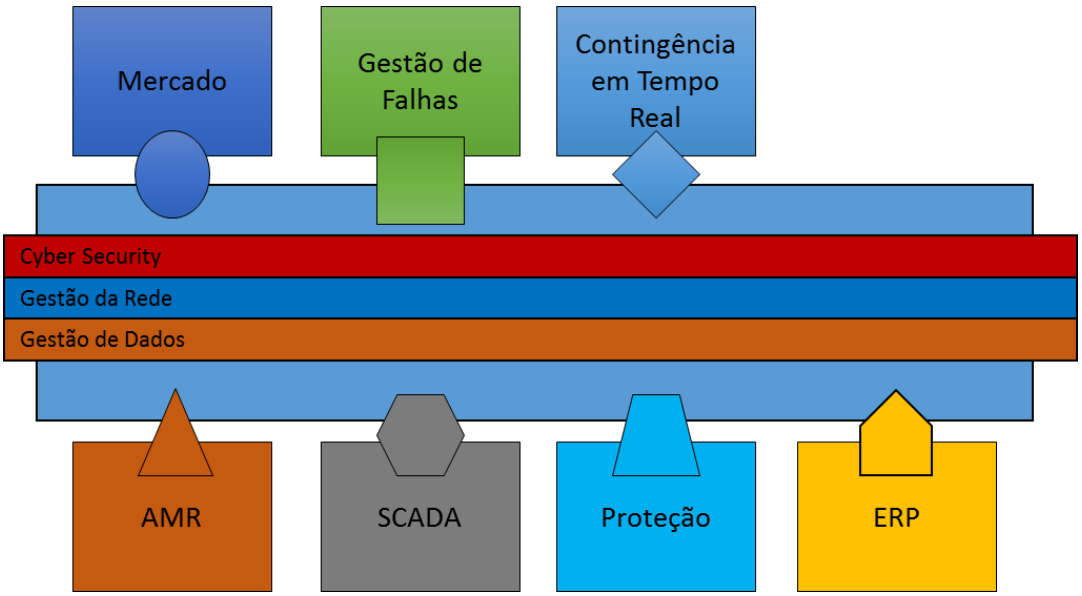
Sistema de Gerenciamento da Planta

A proposta é que o sistema de gerenciamento possua no mínimo duas camadas de software. A primeira dos sistemas proprietários dos fornecedores dos equipamentos, que variam em função do projeto técnico e equipamentos. E, a segunda camada um gerenciador padrão para orquestrar os comandos dos equipamentos e a consolidação dos dados dos diferentes equipamentos, dando uma visão única e integrada para o operador do sistema.

Essa proposta, minimiza os recursos de operação, o treinamento dos operadores, permite a centralização da operação e acelera a implantação do sistema.

A proposta é criar um dashboard para visualizar a operação de forma integrada e um sistema de operação que permita a automação dos processos de forma intuitiva e gráfica.

A figura a seguir mostra a proposta de uso um “bus” para integrar os dados dos diferentes dados da planta para a monitoração e controle centralizado.



O modelo proposto permite a conexão de qualquer software de mercado de gestão da operação e de segurança para o monitoramento e controle da planta.

O "bus" deve ter o conceito de multiplexação para o envio dos dados, ou seja, simultaneamente qualquer software pode se comunicar com o outro sem que entre em uma fila de envio. Esse requisito é importante por se tratar de uma operação de missão crítica. Por exemplo, o acionamento automático de um seccionador deve ser em ciclos de tempo (frequência) da rede elétrica. O "bus" deve suportar diferentes tecnologias de rede, tais como Ethernet e FieldBus, para atender os sistemas de controles de diferentes fornecedores.

O software AMR (*Automatic Meter Reading*) faz o controle e medição da demanda de energia despachada para a rede. O SCADA (*Supervisory Control and Data Acquisition*) é um software para monitorar e supervisionar as variáveis e os dispositivos de sistemas de controle conectados através de controladores específicos. O Sistemas de Proteção controlam os acionamento de dispositivos para interromper o fornecimento de energia em caso de anomalias no sistema.

Todos os softwares interconectados através de um "bus" devem interagir, quase que instantaneamente, e a partir de uma sequência pré-programada de ações (wokflow) garantir a integridade e proteção dos equipamentos e dos sistemas de geração e transmissão.

Planejamento de Recursos Empresariais (ERP)

O ERP deve atender a todos processos de negócios administrativos da organização e suas interações com a cadeia de fornecedores, clientes e governo. O ERP deve integrar as informações entre os processos de negócios de forma automática e em tempo real, permitindo uma melhor gestão, melhoria de processos, maior produtividade e redução de custos. Deve atender a todas as questões de conformidade das questões regulatórias e fiscais, garantindo a conformidade através de atualização no software quando houver mudanças na legislação.

O ERP deve fornecer, no mínimo, o suporte para as seguintes áreas de negócios:

- Finanças/Contabilidade: Livro Razão; Contas a Pagar; Gestão de Caixa; Ativo Fixo; Contas a Receber, Orçamento e Conciliação de Contas; etc.
- Recursos Humanos: Folha de Pagamento; Treinamento; Benefícios; Recrutamento; etc.
- Operação: Engenharia; Lista de Materiais; Ordens de Serviços; Gestão do Workflow; Controle de Qualidade; Gestão de Custos; Fluxo da Produção; Custeio; etc.
- Gestão da Cadeia de Suprimentos (Supply Chain Management): Ordens de Pagamento; Entrada de Pedidos; Compras; Especificação do Produto; Planejamento da Cadeia de Suprimentos; Programação do Fornecedor; Inspeção de Mercadorias; Processamento de Pedidos; Comissões; etc.
- Gerenciamento de Projetos: Custeio; Controle dos Investimentos e Despesas; Unidades de Desempenho; Gerenciamento de Atividades; etc.
- Gestão do Relacionamento com Clientes: Vendas e Marketing; Comissões; Atendimento ao Cliente; etc.
- Serviços Self-Services: Serviços que disponibilizam informações para uso de clientes, fornecedores e empregados.
- Controle de Acesso: Gerenciamento de acessos privilegiado e restrito para usuários do sistema de acordo com suas necessidades para exercer suas funções dentro da organização.

O ERP deve possuir os seguintes componentes:

- Banco de dados transacional;
- Portal de Internet
- Painéis de controle gerencial com suporte a gráficos e estatísticas;
- Sistemas de Business Intelligence;
- Relatórios operacionais e gerenciais personalizados;
- Suporte a EDI e Web-EDI;
- Gestão de Documentos;
- Gestão de Workflow;
- Sistema de Ajuda.

O ERP deve ser modular para que possa ser contratado ou implantado de forma seletiva.

Para atender a plantas já existentes deve existir ferramentas de migração de dados com funcionalidades de extração, transformação e carga de dados, conhecidos como ETL (*Extract, Transformation and Load*).

A premissa é que o cliente adquira o serviço com os processos padrões e que os, eventuais, ajustes possam ser feitos através de parametrização do software, evitando o desenvolvimento de códigos de programação.

A tabela a seguir mostra os principais processos para um ERP orientado para as PMEs.

Área	Processos
Finanças	Plano de contas; Lançamento contábil manual; Pré-lançamento contábil; Multimoeda; Apuração de impostos (diretos e indiretos); Multiperíodo contábil; Centro de custo; Controle de orçamento
Vendas / CRM	Cotação; Pedido de venda; Entrega; Devolução; Nota fiscal de saída; Devolução de nota fiscal; Administração de oportunidades e etapas do ciclo de vendas (pipeline); CRM
Compras	Pedido de compra; Recebimento de mercadoria; Devolução de mercadoria; Nota fiscal de entrada; Devolução de nota fiscal; Despesa de importação
Clientes/fornecedores	Administração de clientes; Fornecedores e leads; Atividades
Banco	Contas a pagar e a receber; Controle de depósitos; Cheques emitidos e recebidos; Pagamentos; Recebimentos; Sistema de pagamento; Extratos e reconciliações; Conciliação; Extrato bancário externo
Inventário	Administração de ativos; Itens alternativos; Lista de preço; Entrada em estoque; Saída de estoque; Transações de estoque; Transferência de depósito; Administração de números de série; Administração de lotes; Lista de picking
Fiscal	Nota fiscal eletrônica; SPED fiscal; SPED contábil, SPED PIS/COFINS; FCONT; SINTEGRA
Produção	Estrutura do produto; Ordem de produção; Montagem de kits; Apontamentos por código de barras; Custo industrial por absorção; Custo gerencial; Subproduto; Formação de preço de venda
Serviço	Administração de contratos de prestação de serviços; Monitoramento de clientes; Base de conhecimento (Knowledge database); Administração de ordens de serviço
Recursos Humanos	Cadastro de funcionários; Folha de pagamento; Ponto eletrônico; apontamento de horas; eSocial
Relatórios	Financeiros; Oportunidades de vendas; Vendas Compras; Parceiros de negócios; Serviços, Inventário; Produção; Recursos Humanos
Qualidade	Inspeção de entrada; Inspeção de processo; Registro de não conformidade; Laudos; Qualificação de fornecedores
Gestão de Projetos	Gestão física dos projetos (tarefas/horas); Orçamento do projeto; Apontamento de horas por projeto/tarefa; Previsto x realizado por projeto; Produção por projeto; Faturamento por projeto; Compras por projeto

Infraestrutura de Data Center e Rede de Dados

A infraestrutura dos dois data centers, local e de Cloud Computing, devem atender os requisitos mínimos de instalações Tier 3. Devem possuir capacidade de infraestrutura local redundantes com independentes meios de conexão dos servidores e dupla alimentação de energia. Devem ter uma disponibilidade de operação de 99,982%.

Deve-se considerar que algumas plantas de geração estão em locais remotos com restrições de acesso à Internet. Algumas com acesso a transmissão via satélite e comunicação através de cabos metálicos de baixa confiabilidade.

Para minimizar a questão de delay (atraso) na transmissão via satélite deve-se considerar equipamentos com compactação e otimização de transmissão.

Oportunidade de Negócios

É de domínio público que existe escassez de produção de energia renovável no país e que a atual demanda está sendo atendida por geração de energia pelas termoelétricas, que são mais caras que outras formas de geração.

Em maio de 2014, em um seminário da Frente Parlamentar em Defesa das PCHs e Fontes de Energia Renováveis, foi divulgado a existência de 800 projetos de PCHs na Aneel (Agência Nacional de Energia Elétrica) que aguardam aprovação para iniciar os projetos. Sem contar com outras plantas de energia eólica, biomassa e solar. Esses projetos têm incentivos do BNDES e são atrativas para o mercado livre de energia.

Esses dados comprovam a atratividade do negócio e o senso de urgência no desenvolvimento de uma solução completa e integrada para atender esse mercado.

Estima-se que cada empresa tenha um staff de 10 pessoas na planta em turnos de revezamento e outras 10 pessoas no back-office.

O prazo de construção e entrada em produção dessas plantas varia de 24 a 36 meses. O investimento de cada projeto de construção depende da tecnologia e local de instalação.

Anexo III

Projeto

Monitoração e Melhoria Contínua com Six-Sigma, IoT e Big Data

Contexto

As pressões do mercado por excelência em qualidade e baixo custo obrigam as empresas a adotarem sistemas de produção automatizados e imunes a falhas. Quanto mais complexo o sistema maior a automação dos processos para recuperação rápida de falhas (self-healing) para garantir a alta disponibilidade dos serviços. Há anos a metodologia Six-Sigma auxilia as empresas na identificação da causa-raiz dos problemas e na elaboração de planos e controles para reduzir o número de defeitos em processos de manufatura, logísticas e serviços.

Six-Sigma é um conjunto de técnicas e ferramentas para melhoria de processos. Tem o objetivo de melhorar a qualidade das saídas dos processos, identificando e removendo as causas dos defeitos (erros) e minimizando a variabilidade na fabricação e processos de negócios, usando um conjunto de métodos de gestão de qualidade, principalmente métodos empíricos e estatísticos. Cada projeto Six-Sigma segue uma sequência definida de passos e quantifica metas de valor, por exemplo: reduzir o ciclo de tempo do processo, reduzir a emissão de gases de efeito estufa, reduzir custos, aumentar a satisfação do cliente e aumentar os lucros. Um processo é Six-Sigma quando 99.99966% esta, estatisticamente, livres de defeitos (3,4 erros por milhão).

A monitoração e melhoria contínua usando a metodologia Six-Sigma tem o objetivo de reduzir custos operacionais, melhorar a eficiência energética e aumentar a disponibilidade dos serviços, gerando maior satisfação dos clientes e lucratividade.

Um desafio do Six-Sigma é coletar dados para as análises. Os desafios técnicos eram grandes para consolidar os registros das logs dos sistemas SCADA para fazer análises integradas dos sistemas de automação. Em alguns casos, dados eram descartados devido a limitações de armazenamento de dados. Essas restrições foram eliminadas com a infraestrutura de processamento e armazenamento escalável na nuvem (Cloud Computing).

Com a medição inteligente, tecnologias de Internet of Things (IoT) e Big Data é possível a coleta, armazenamento e análise de grandes volumes de dados com custos competitivos, quando executados em ambientes Cloud Computing.

A tecnologia Internet of Things (Internet das Coisas) é uma rede de objetos físicos ou "coisas" incorporado a produtos eletrônicos, softwares, sensores e conectividade para troca de dados com fornecedores, operadores ou outros dispositivos conectados. Estes dispositivos coletam dados úteis com a ajuda de várias tecnologias existentes e, em seguida, de forma autônoma trocam dados com outros dispositivos.

A tecnologia de Big Data e ferramentas analíticas permitem o gerenciamento e análise do grande volume de dados em tempo real produzido pelos sensores remotos, usando a

tecnologia IoT. É possível a integração de dados de sistemas proprietários e legados, como os sistemas SCADA.

Para atingir alto desempenho computacional, os sistemas de busca, classificação e análise de dados devem operar em ambientes de processamento paralelo, acessíveis para a maioria das empresas através de Cloud Computing.

Entretanto, apenas a tecnologia não é suficiente para desenvolver projetos de melhoria contínua e inovação, é fundamental uma equipe de especialistas e metodologia para alcançar os objetivos propostos.

Proposta do Projeto

O projeto de monitoração e melhoria contínua usando a metodologia Six-Sigma, tecnologias de IoT, Big Data e ferramentas analíticas tem o objetivo de reduzir custos operacionais, melhoria da eficiência energética dos sistemas de produção e alta disponibilidade dos serviços, aumentando a satisfação dos clientes e lucratividade.

Desenvolvemos uma plataforma de software em ambiente de Cloud Computing que permite a coleta remota de dados, a transformação, o armazenamento e a análise de grandes volumes de dados.

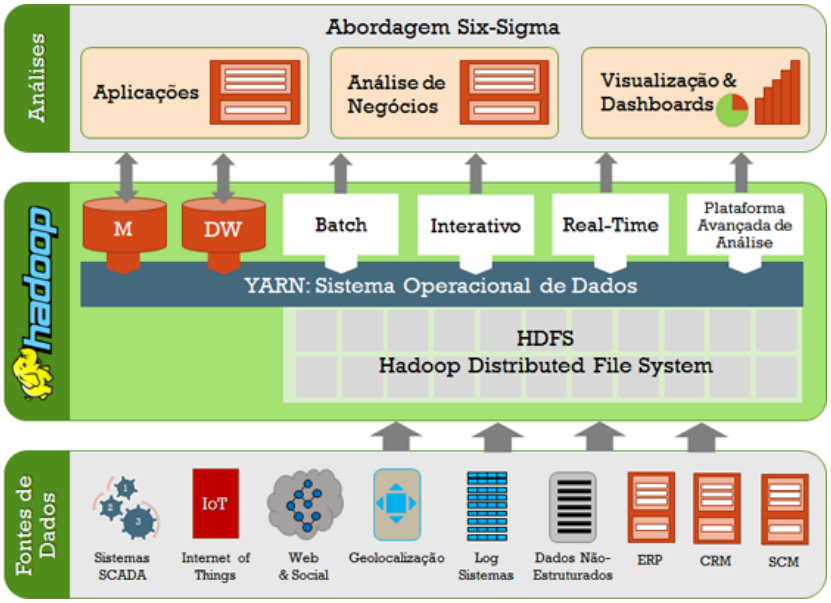


Figura 1. Plataforma de software de IoT, Big Data e Analytics com abordagem Six-Sigma

Nossa plataforma de software permite a aquisição de vários tipos de dados e fontes. Coletamos dados das logs de diferentes sistemas SCADA, independente do fabricante, transformamos para formatos compatíveis com Big Data para análises integradas de dados. Os dados dos sistemas SCADA podem ser integrados aos dados de sensores monitorados usando tecnologia Internet of Things, potencializando as análises integradas.

Ainda, é possível coletar dados do ERP e de outros sistemas legados para realizar análises mais rápidas e precisas que os sistemas de Data Warehouse e Business Intelligence (BI), devido às características de processamento paralelo do ambiente de Big Data.

Embora nossa plataforma de software permita uma ampla abordagem de assuntos de negócios, científicos, sociais e ambientais, incluindo simulações de cenários, nosso projeto

foca em monitoração de ambientes industriais, plantas de geração, transmissão e distribuição de energia, e prédios inteligentes.

A coleta de dados dos dispositivos remotos é planejada para ser através da Internet, entretanto, outros meios de comunicações podem ser utilizados dependendo da disponibilidade do serviço de Internet ou por questões de projeto.

Os resultados das análises ou conjunto de dados a serem analisados podem ser apresentados em aplicações Web.

A figura a seguir mostra as possibilidades de coletas de dados usando as logs dos sistemas SCADA em plantas industriais, em plantas de geração e transmissão de energia e em prédios inteligentes com geração de energia fotovoltaica, incluindo a monitoração de carregamento de baterias de carros elétricos.

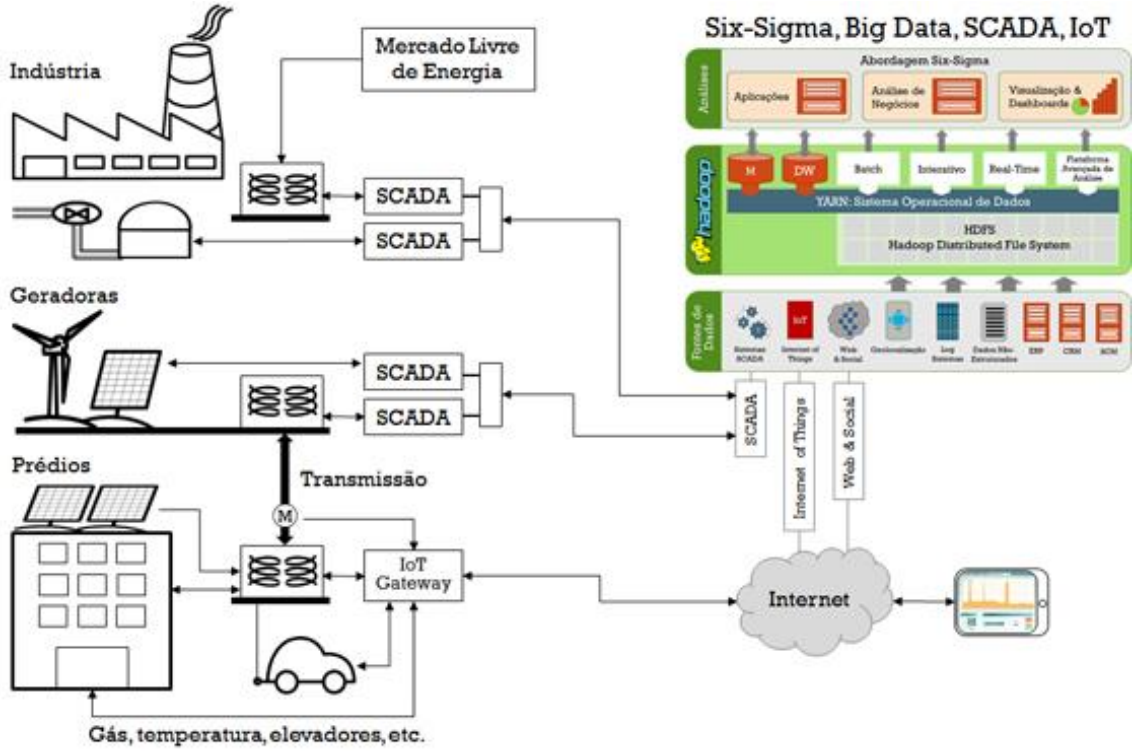


Figura 2. Coleta de dados de dispositivos remotos para monitoração e análise em Big Data

O projeto considera a utilização de todos os dispositivos digitais utilizados pelos sistemas SCADA e o uso de dispositivos de Internet of Things quando necessário.

O projeto também prevê a aquisição de dados de outros sensores, como para medição de água, temperatura, pressão, fluxo de fluídos entre outros. Essas medições são importantes para uma visão holística de toda operação e análise das correções entre diferentes parâmetros de operação. A figura 3 apresenta a conexão de um medidor inteligente utilizando uma interface RS-232 e outros sensores conectados através de uma interface HART a um conversor de protocolo. Através de um gateway de Internet of Things os dados são transmitidos para o ambiente de Cloud Computing para processamento e análises.

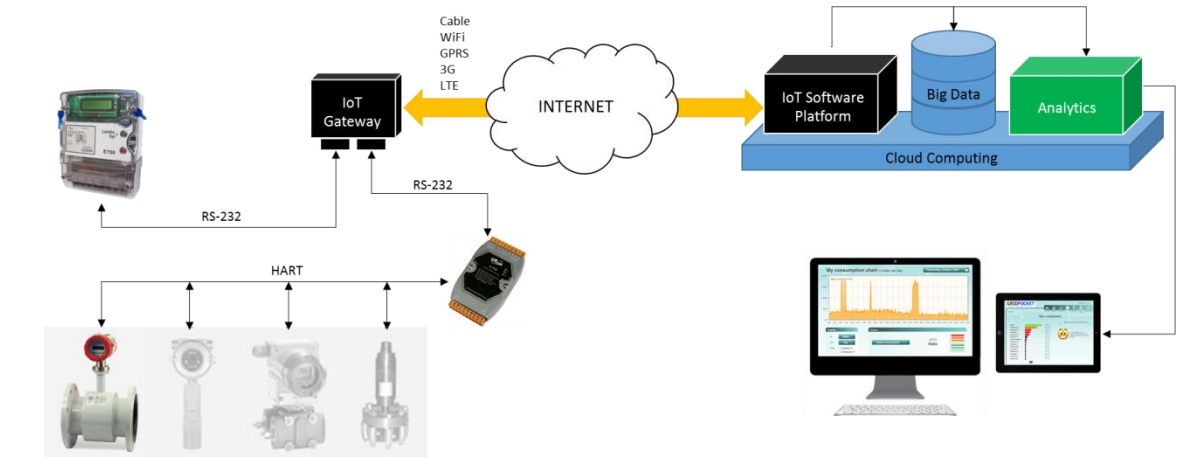


Figura 3. Configuração de rede para coleta e transmissão de dados

Todo o processamento de dados para transformação de dados, armazenamento de dados, análise avançada de dados e geração de relatórios e *dashboards* é executado em ambiente externo de Cloud Computing, gerando mínimo impacto na infraestrutura, sistemas de aplicação e recursos da área de TI da empresa.

A monitoração constante dos parâmetros do sistema permite a identificação de vulnerabilidades e ataques cibernéticos. Com a crescente automação dos processos aumenta os riscos sobre segurança cibernética – Cyber Security. Na área de energia, com as redes inteligentes – Smart Grid – o risco é enorme, pois acontecendo em uma concessionária de energia (geração, transmissão ou distribuição) existe o risco de apagão em grandes regiões, prejudicando milhões de pessoas e afetando, diretamente, a economia.

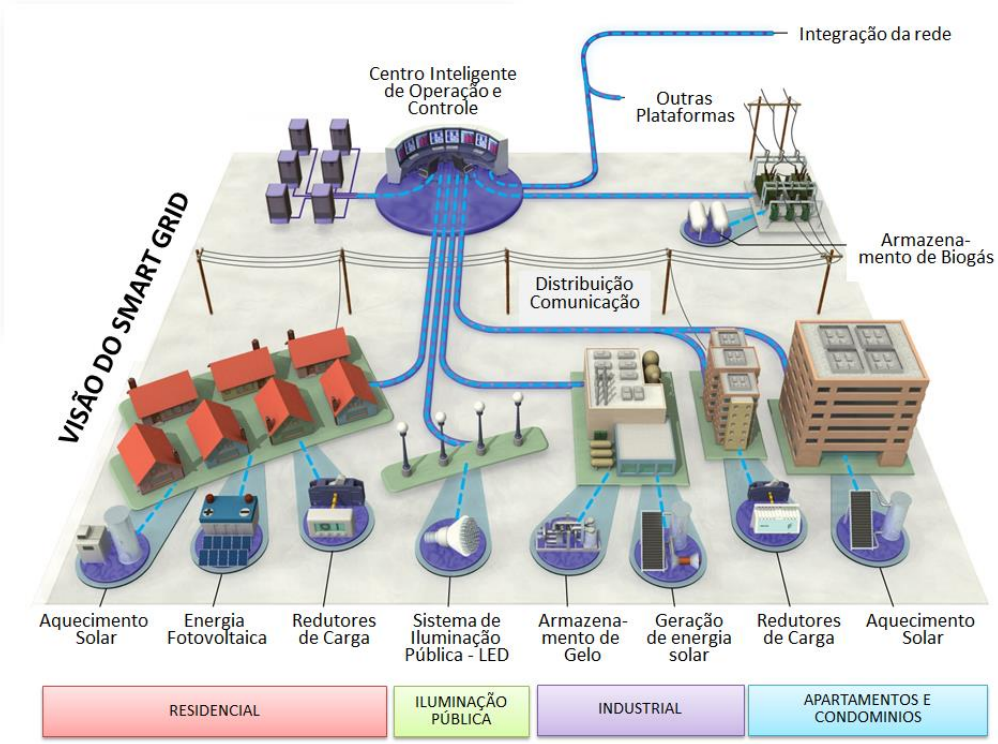
Anexo IV

Curso de Smart Grid

Apresentar os conceitos, tecnologias e tópicos para desenvolvimento de projetos de Smart-Grid, seus componentes e oportunidades de criação de novos serviços para os clientes. O programa do curso discute algumas plataformas de Smart-Grid e alternativas de técnicas de operação de redes inteligentes. Aborda a integração do Smart-Grid com os sistemas integrados de gestão das empresas e os aspectos de segurança cibernética.

Contexto

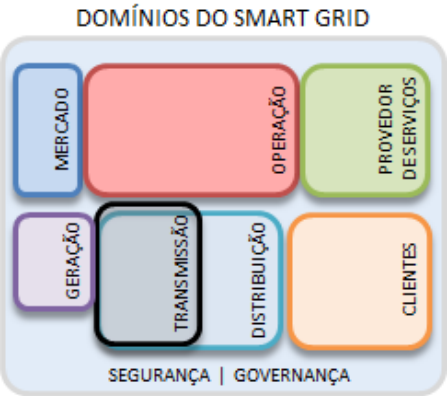
Conservação de Energia. Eficiência Energética. Go Green. Clean Tech. Smart Grid. Essas buzzwords estão no cotidiano dos executivos das empresas de geração e distribuição de energia. Como concessionárias de serviços públicos, essas empresas estão engajadas na melhoria da sustentabilidade ambiental, expansão da oferta e qualidade dos serviços. Os executivos estão sendo desafiados a projetar novos serviços de utilidade pública e se preparar para mudanças tecnológicas, mesmo desconhecendo a demanda de seus clientes. Um dos desafios é atender a demanda em horários de picos de consumo com fontes de renováveis e distribuídas, de forma eficiente e inteligente. O aumento da geração distribuída traz um impacto significativo sobre as operações de distribuição, ampliando a necessidade de automação rede de distribuição além da subestação. Outro desafio é desenvolver novos serviços para ampliar a receita e o atendimento ao cliente.



Nos últimos 20 anos, as empresas concentraram recursos consideráveis na leitura automática dos medidores para melhorar a precisão, reduzir custos e melhorar a receita com a redução das perdas não técnicas. O foco agora é desenvolver novos serviços para uma medição mais sofisticada, granular e que ajude no achatamento da curva de carga em determinados períodos, proporcionando a melhoria do fator de carga, evitando ou postergando a necessidade de novos investimentos no sistema elétrico. Esses novos serviços

criam grandes oportunidades para melhorar a receita, otimizando o uso da energia contratada, e melhorando a prestação de serviços aos clientes. Novos conceitos de distribuição podem ser adotados para introduzir novas fontes de geração de energia com preços diferenciados.

As concessionárias de energia estão desenvolvendo novas estratégias para implementar e suportar uma variedade de novas aplicações que vão além da simples medição. A compreensão dos requisitos dessas iniciativas operacionais leva a necessidade de reestruturar a infraestrutura existente para uma nova infraestrutura de rede mais avançada com um gerenciamento mais eficiente e sofisticada através de dispositivos que criam um Smart-Grid. A nova rede inteligente é composta por dispositivos inteligentes online que permite a supervisão, a avaliação, a análise, o comando e controle em tempo real do sistema de distribuição. A plataforma dessa nova rede deve ser escalável, confiável e aberta para aceitar novas tecnologias de componentes no futuro, a exemplo da rede de comunicação de dados TCP/IP da Internet.



Desta forma, é critico entender as plataformas disponíveis no mercado e selecionar aquela em que o fornecedor tenha compromisso com padrões abertos de mercado, que possua uma visão clara de mercado e capacidade de execução. O desenvolvimento de uma estratégica correta e a seleção de uma plataforma de rede para entregar o Smart Grid é fundamental para a criação de valor ao negócio.

O público alvo são executivos, engenheiros e técnicos especializados do setor elétrico de concessionárias, governo, fornecedores e instituições de pesquisa e comunidade acadêmica.

A carga horária é de 60 horas, sendo 40 horas em sala de aula e 20 horas de estudo a distância para revisão dos pré-requisitos e estudos complementares acompanhados pelos professores.

Programa do Curso

1. **ARQUITETURA E DESIGN DO SMART GRID**
   - 1.1. Redes tradicionais versus Smart Grid
   - 1.2. Inteligência Computacional
   - 1.3. Melhorias nos sistemas de potência
   - 1.4. Comunicação e padrões
   - 1.5. Visão geral do mercado de Smart Grid
   - 1.6. Funções e Papeis dos Stakehloders
     - 1.6.1. Concessionárias
     - 1.6.2. Agências Reguladoras
     - 1.6.3. Centros de Pesquisas
     - 1.6.4. Fornecedores de equipamentos
   - 1.7. Métricas de Performance do Smart Grid
   - 1.8. Funções dos Componentes do Smart Grid
     - 1.8.1. Interfaces
     - 1.8.2. Armazenamento

1.8.3. Subsistema de Transmissão
1.8.4. Tecnologias de Monitoração e Controle
1.8.5. Subsistema Inteligente de Distribuição
1.8.6. Gerenciamento da Demanda

2. TECNOLOGIAS DE COMUNICAÇÃO E MEDIÇÃO PARA SMART GRID

2.1. Comunicação e medição
2.2. Monitoração, PMU, Medidores eletrônicos, Tecnologia de Medição
2.2.1. WAMS - Wide Area Monitoring Systems
2.2.2. PMU - Phasor Measurement Units
2.2.3. Medidores Eletrônicos
2.2.4. Smart Appliances
2.2.5. Infraestrutura de Medição (AMI - *Advanced Metering Infrastructure*)
2.3. GIS e Ferramentas de Mapeamento
2.4. Comparação entre Microgrid e Smart Grid

3. FERRAMENTAS DE ANALISE DE PERFORMANCE PARA SMART GRID DESIGN

3.1. Introdução a Fluxo de Potência
3.2. Métodos para Estudo de Fluxo de Potência
3.2.1. Método de Gauss-Seidal
3.2.2. Método de Newton-Raphson
3.2.3. Método Iterativo de Gauss
3.3. Fluxo de Potência para Smart Grid
3.4. Estudos de Contingência para Smart Grid

4. FERRAMENTAS DE ANALISE DE ESTABILIDADE PARA SMART GRID

4.1. Introdução a Estabilidade
4.2. Pontos fortes e fracos das ferramentas de análise de tensão existentes
4.3. Avaliação da estabilidade de tensão
4.3.1. Estabilidade de tensão e Colapso de tensão
4.3.2. Classificação da estabilidade de tensão
4.3.3. Estabilidade estática
4.3.4. Estabilidade dinâmica
4.4. Técnicas de avaliação de estabilidade de tensão
4.5. Análise do fluxo estacionário em estudos de estabilidade de tensão
4.6. Implantação do plano de estabilidade de tensão
4.7. Otimizar a restrição de estabilidade através do controle preventivo da estabilidade de tensão
4.8. Avaliação da estabilidade de ângulo
4.9. Estimativa de estado

5. FERRAMENTAS COMPUTACIONAIS PARA SMART GRID DESIGN

5.1. Introdução às ferramentas computacionais
5.2. Ferramentas de suporte a decisão (DS)
5.3. Técnicas de otimização
5.4. Métodos de otimização clássicos
5.4.1. Programação linear
5.4.2. Programação não linear
5.4.3. Programação inteira
5.4.4. Programação dinâmica
5.4.5. Programação estocástica
5.5. Otimização Heurística
5.5.1. Redes Neurais e Inteligência Artificial

5.5.2. Sistemas Especialistas
5.6. Técnicas de programação adaptativas
5.7. Métodos de Pareto
5.8. Técnicas de otimização hibridas e aplicações para Smart Grid
5.9. Tecnologia Big Data

6. FERRAMENTAS DE SUPERVISÃO

6.1. Supervisão da rede de distribuição
6.2. Supervisão de pontos de seccionamento e manobras
6.3. Supervisão de transformadores
6.4. Supervisão de medidores e pontos de entrega
6.5. Algoritmos de defeito provável
6.6. Estratégias de operação e atendimento de emergência

7. ROTEIRO DE DESENVOLVIMENTO DE SMART GRID

7.1. Barreiras e soluções para o desenvolvimento de Smart Grid
7.2. Níveis de automação
7.2.1. Confiabilidade
7.2.2. Estabilidade
7.2.3. Despacho econômico
7.2.4. Análise de segurança
7.3. Sistema de automação da geração de energia para Smart Grid no nível da transmissão
7.3.1. Diagnóstico de falhas e estabilidade
7.3.2. Controle da energia reativa
7.4. Sistema de automação da distribuição para Smart Grid
7.4.1. Controle de tensão/Var
7.4.2. Qualidade da energia
7.4.3. Reconfiguração da rede
7.4.4. Gestão da Demanda
7.4.5. Controle da distribuição
7.5. Smart Grid para usuários finais

8. ENERGIA RENOVÁVEL E ARMAZENAMENTO

8.1. Recursos para energia renovável
8.2. Opções de energia sustentável para Smart Grid
8.2.1. Energia solar
8.2.2. Tecnologia de energia solar
8.2.3. Energia Fotovoltaica
8.2.4. Energia eólica
8.2.5. Biomassa
8.2.6. Pequenas Centrais Hidroelétricas (PCH)
8.2.7. Célula de combustível
8.2.8. Energia geotérmica
8.3. Veículos elétricos e híbridos
8.4. Tecnologia PHEV (plug-in hybrid electric vehicle)
8.5. Implicações ambientais
8.6. Tecnologias de armazenagem de energia

9. INTEROPERABILIDADE, PADRONIZAÇÃO E SEGURANÇA CIBERNÉTICA

9.1. Interoperabilidade
9.1.1. Definições
9.1.2. Conceito de Internet of Things
9.1.3. Benefícios e desafios da interoperabilidade

9.1.4. Modelo de interoperabilidade no ambiente Smart Grid
9.1.5. Interoperabilidade da rede do Smart Grid
9.1.6. Controle e interoperabilidade da rede elétrica
9.2. Padronização
9.3. Segurança Cibernética
9.3.1. Visão geral de segurança cibernética
9.3.2. Riscos
9.3.3. Preocupações de segurança associadas com o AMI (Automated Metering Infrastructure)
9.3.4. Mitigação dos riscos de segurança

Curso sobre Smart Grid Cyber Security

O curso apresenta os elementos da infraestrutura cibernética para redes inteligentes de energia elétrica (*Smart Grid Cyber Security*), estratégias de arquitetura e operação, suas vulnerabilidades e gerenciamento de risco. O curso é orientado para engenheiros, especialistas em segurança da informação e executivos do setor de energia. O curso tem carga horária de 8 horas e é apresentado sob demanda.

Contexto

Os desafios de crescimento econômico e social do Brasil exige um programa de modernização e expansão da sua infraestrutura de geração, transmissão e distribuição de energia. É imperativo que o país adote novas tecnologias de digitalização (Smart Grid) para aumentar a eficiência energética da infraestrutura, reduzir as perdas comerciais e técnicas, aumentar a produtividade de operação do sistema e oferecer novos serviços para os usuários. Um dos grandes passa pela formação de mão de obra especializada para projetar e operar as novas tecnologias de Smart Grid.

A modernização e expansão da infraestrutura de energia com o uso de tecnologias da informação traz um risco potencial de segurança cibernética. Para mitigar os riscos de blackouts e invasões que afetem a confiabilidade, integridade e disponibilidade dos dados é necessário um amplo programa de treinamento dos funcionários e prestadores de serviços das concessionárias e empresas do setor elétrico.

> *Infraestrutura Cibernética: Inclui toda a informação eletrônica, sistemas e serviços de comunicações e as informações contidas nesses sistemas e serviços. A infraestrutura é composta por todo o hardware e software para processar, armazenar e transmitir informações, ou qualquer combinação de todos estes elementos. Processamento inclui a criação, acesso, modificação e destruição de informações. Armazenamento inclui papel, magnético, eletrônico, e todos os outros tipos de mídia. Comunicações incluem o compartilhamento e distribuição de informação. Por exemplo: sistemas de computação, sistemas de controle (por exemplo, controle de supervisão e aquisição de dados, SCADA), redes, como a Internet, e serviços virtuais (por exemplo, serviços gerenciados de segurança).*

Com milhares de quilômetros de linhas de transmissão e distribuição a superfície para um ataque cibernético é vasta e crescente colocando em risco a operação do sistema. O risco se

potencializa com a ausência de um mapeamento adequado das vulnerabilidades e de uma gestão em tempo real dos ativos do sistema elétrico.

A proteção da rede inteligente rede e do núcleo de supervisão controle e dados (SCADA) requer a combinação de conhecimentos de engenharia e segurança da informação. O treinamento de engenheiros em segurança da informação e dos especialistas em segurança em elementos de engenharia elétrica é fundamental para garantir a continuidade dos serviços aos usuários e proteção dos investimentos e remuneração dos acionistas.

As organizações devem se desenvolver competências para:

1. Prepare-se para ataques externos conhecidos e pequenos incidentes internos;
2. Evitar o acesso não autorizado a informações críticas ou sensíveis;
3. Dissuadir adversários de ganhar uma posição segura dentro da infraestrutura de informações da organização;
4. Restringir o acesso a dados críticos, continuar operações críticas, minimizar danos, apesar ataques bem-sucedidos de adversários que estabeleceram uma posição;
5. Manter as operações em uma base contínua e adaptar-se às atuais e futuros ataques bem sucedidos, independentemente da sua origem.

Para atender os requisitos de competências nas organizações novas habilidades devem ser introduzidas nas equipes planejamento, controle e operação do sistema. Uma estrutura organizacional para Smart Grid Cyber Security deve reunir:

- Especialista em segurança de medidores eletrônicos
- Administrador de segurança (gerenciamento de certificados, etc.)
- Arquiteto de segurança
- Especialista em segurança de redes
- Especialista em operações de segurança
- Especialista/analista de resposta a incidentes
- Analista de Intrusão
- Analista de risco/vulnerabilidade
- Engenheiro de telecomunicações
- Técnico de engenharia reversa
- Técnico de equipamentos de campo

Essa organização deve estar apta para:

1. Desenvolver técnicas inovadoras para atender os atuais e futuros cenários de ameaças;
2. Desenvolver técnicas inovadoras para levantamento e definição de tarefas para reduzir dramaticamente o tempo de elaboração de estratégias de detecção e defesa às vulnerabilidades do sistema;
3. Desenvolver um método para produzir modelos de competência para a criação de perfis de competências inter-relacionadas para a evolução contínua da maturidade organizacional em segurança cibernética em redes inteligentes.

Programa do Curso

1. Infraestrutura cibernética

2. Estratégia para segurança cibernética de redes inteligentes (Smart Grid Cybersecurity)
3. Requerimentos de segurança
4. Criptografia e gerenciamento de chaves
5. Privacidade e fraudes
6. Vulnerabilidades da infraestrutura e operação
7. Análise de segurança
8. Pesquisa e desenvolvimento de temas sobre segurança para Smart Grid
9. Revisão de padrões e modelo de maturidade da organização
10. Casos de Uso

Anexo V

Projeto

Lean Data Center

O projeto Lean Data Center tem o objetivo de projetar, maximizar a infraestrutura, aumentar a disponibilidade dos serviços e melhorar a gestão de data centers de forma sustentável. O resultado é a melhoria da eficiência organizacional, uso pleno dos recursos tecnológicos instalados, planos de continuidade de negócios, aumento da eficiência energética e redução da emissão de gases do efeito estufa (CO_2).

Projetamos e implementamos as melhores soluções para o data center com base nas tecnologias disponíveis no mercado para empresas de todos os portes. Realizamos análises técnico/econômicas para utilização de novas tecnologias e migração para ambientes Cloud Computing.

Temos independência na seleção de fornecedores de tecnologia, garantindo a melhor solução para a sua empresa. Essa independência nos habilita a realizar o comissionamento de novos equipamentos e sistemas nos data centers.

Projetos de Data Centers

Desenvolvemos todas as fases de implantação e reestruturação de data centers, incluindo: projeto do prédio seguindo critérios de eficiência energética e sustentabilidade; projetos e implementação da infraestrutura predial (mecânica, elétrica, sistemas especialistas e sistemas de controle e automação); arquitetura tecnológica (servidores, armazenamento, redes e segurança); e, planejamento e implantação dos processos de gestão, incluindo automação e planos de continuidade de negócios.

Comissionamento de equipamento e sistemas

Coordenamos a realização dos testes de certificação dos equipamentos e sistemas para garantir sua utilização de acordo com as especificações do projeto. Adotamos as melhores práticas de comissionamento do mercado para a realização. Acompanhamento todo o processo de pré-design, design, construção e operação dos projetos.

Maximização e atualização da tecnologia

A crescente demanda por recursos computacionais e a forte pressão por redução de custos exige a adoção de novas tecnologias de processamento. O uso intensivo de virtualização e uma arquitetura unificada de operação permitem o aumento da capacidade de processamento, redução do número de equipamentos e seus custos associados, consolidação dos recursos e a ampliação da automação de processos no data center.

Melhoria dos processos de gestão

Melhoria de processos é uma atividade dinâmica e constante nas organizações. Nos data centers é fundamental que a equipe desenvolva continuamente exercícios para otimizar os processos operacionais. Com base nos incidentes e falhas operacionais devem desenvolver novas rotinas que elimine as situações que possam impactar os serviços e, consequentemente, aumentando a disponibilidade do data center e reduzindo os custos de operação.

A adoção de normas internacionais como a ISO 20.000 e ISO 27.000 são fundamentais para garantir a alta disponibilidade, segurança, confiabilidade e certificação pelas principais entidades certificadoras do mercado, tais como o UPTIME Institute e CompTIA.

Executamos projetos de melhoria contínua e treinamos o staff do data center. Utilizamos o processo Six-Sigma para análise e definição de processos para a redução do número de falhas operacionais. O Six-Sigma é um conjunto de ferramentas de gestão que determina com exatidão a causa raiz do problema e auxilia na seleção da melhor alternativa de solução.

Aumento da eficiência energética

A otimização do uso de energia é crítica nos data centers. O custo da energia é um dos principais ofensores das despesas operacionais dos data centers. Esse cenário é agravado no Brasil pelo fato que temos uma das mais caras energia do mundo. Nesse contexto o PUE – *Power Usage Efficiency* – é um parâmetro importante para medir a eficiência do data center.

Analisamos a eficiência energética dos data centers de várias formas:

- Qualidade da energia. Avaliação das harmônicas da rede elétrica, transitórios elétricos, variações de frequência e níveis de tensão que afetam os equipamentos e reduzem sua vida útil;
- Consumo dos ativos do data centers. Avaliação do consumo dos equipamentos e infraestrutura do data center para identificar oportunidades de redução. Equipamentos antigos consumem mais energia e emitem mais calor, exigindo mais do sistema de refrigeração do data center;
- Análise do contrato de fornecimento de energia. As concessionárias de energia cobram pelo consumo de energia, pela demanda garantida de energia e pela energia reativa gerada. Um contrato mal definido pode gerar custos adicionais desnecessários;
- Mercado Livre de Energia. Realizamos estudos para avaliar a migração do data center para o mercado livre de energia com o objetivo de garantir o fornecimento de energia e mitigar os aumentos de custos das concessionárias de distribuição. A migração para o mercado livre não exige mudança físicas na infraestrutura elétrica do data center, apenas a substituição do medidor;
- Cogeração de energia renovável. Desenvolvemos projetos de plantas de geração de energia solar fotovoltaica para alimentar os data centers para reduzir o consumo de eletricidade da concessionária e a emissão de gases do efeito estufa na atmosfera;
- Programa de eficiência energética da ANEEL. O contrato de concessão de distribuição de energia obriga as concessionárias a destinar um percentual da receita líquida para projetos de eficiência energética a fundo perdido. Em alguns casos, é possível avaliar com a concessionária local de distribuição de energia o uso da verba de eficiência energética para subsidiar projetos nas empresas e órgãos públicos.

Redução da emissão de gases do efeito estufa (CO2)

É cada vez maior a pressão dos governos e sociedade para que as empresas adotem soluções para reduzir a emissão de gases de efeito estufa na atmosfera. Empresas líderes de mercado estão cada vez mais aderindo, voluntariamente, aos programas mundiais de conservação do meio ambiente, como o CDP – *Carbon Disclosure Project* – e, influenciando seus fornecedores a aderem aos programas. A adesão a esses programas requer um planejamento de longo prazo com definição de metas de redução das emissões. Esse

planejamento é divulgado para a sociedade, ajudando na melhoria da reputação da empresa e aumentado as chances de novos negócios e investimentos.

Fazemos os estudos de redução da emissão de gases de efeito estufa, desenvolvemos o planejamento, registramos as iniciativas nos órgãos de controle internacionais e acompanhamos a execução do plano.

Automação da operação

A redução do número de falhas e a maximização dos recursos dos data centers está associado ao nível de automação dos seus processos. A automação permite o gerenciamento centralizado de vários data centers e a redução do staff operacional tendo como consequência a redução das despesas operacionais. No Brasil, onde a mão de obra qualificada é um desafio para as empresas, a automação reduz os riscos de falhas operacionais e falta de pessoal especializado.

Executamos projetos de automação da operação com ferramentas DCIM – *Data Center Infrastructure Management*. O DCIM é uma solução que gerencia todas as funções, ativos e recursos do data center. A solução é capaz de centralizar a monitoração e gerenciar de forma inteligente os sistemas críticos do data center.

Consolidação de data centers

Estudos mostram que a centralização do processamento reduz o custo de operação. Em outras palavras, os data centers pequenos tem um custo maior de operação comparado com os grandes. Operar em grandes complexos tem a vantagem de usufruir da redução de custos por escala e o uso de instalações robustas de fornecimento de energia, refrigeração, comunicações, segurança lógica e física entre outras. Realizamos o planejamento e a execução de planos de consolidação de data centers.

Disaster Recovery Plan (DRP)

Elaboramos e implementamos planos de recuperação de desastres (DRP) em linha com a estratégia e plano de continuidade de negócios da empresa. Realizamos uma análise detalhado dos riscos dos data centers para definir a estratégia e as atividades para a montagem e operação do DRP.

O objetivo do DRP é permitir que uma organização sobreviva a um desastre e que possa restabelecer as operações dos negócios no menor tempo possível. Para atingir esses objetivos o DRP deve atender os seguintes requisitos:

- Prover um ambiente seguro e pessoas preparadas para um desastre;
- Reduzir as perdas financeiras em casos de desastres;
- Identificar linhas de negócios críticas que requeiram suporte em situações de desastres;
- Identificar as fraquezas e executar um programa da prevenção de desastre;
- Minimizar a duração de uma paralisação das operações de negócio;
- Facilitar a coordenação eficaz de tarefas da recuperação; e,
- Reduzir a complexidade do esforço de recuperação.

Elaboração de RFP

Elaboramos e coordenamos todo o processo de aquisição e comissionamento de produtos e serviços a partir do desenvolvimento de uma Request-for-Proposal (RFP). A RFP é o convite enviado a um grupo de fornecedores para apresentarem propostas de venda de produtos ou

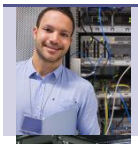
serviços. Um processo de aquisição envolvendo vários fornecedores aumenta a capacidade de negociação e o poder de compra das empresas. O documento deve conter o maior número de informações possível para que os fornecedores usem sua criatividade para oferecer a melhor solução para a empresa. Desta forma, a elaboração de uma RFP é importante para garantir a eficiência do processo de aquisição. Deve seguir uma metodologia e linguagem comum ao gerenciamento de projetos, utilizando técnicas e análise de requisitos.

Estudo de migração para Cloud Computing

Montamos vários cenários para analisar as opções de migração para um ambiente de computação em nuvem: pública, privada ou hibrida. Levamos em consideração os sistemas legados da empresa e os novos desafios planejados pela empresa. A computação em nuvem é uma realidade e vem sendo adotada cada vez mais pelos fornecedores de software, mudando o paradigma de compra de software e hardware para a contração de serviços.

Anexo VI

Cursos sobre inovação, tecnologia e sustentabilidade



Curso sobre Infraestrutura e Gestão de Data Centers
Apresenta os principais elementos para o desenvolvimento de projetos de infraestrutura, incluindo eficiência energética e Big Data, e discute alguns modelos de gestão para melhorar a segurança e níveis de serviço (SLA). CH: 8h

Workshop sobre Desenvolvimento de Negócios para Data Centers
Gera insights para identificar novas oportunidades de negócios para atender a crescente demanda de produtos e serviços para Data Centers. Desenvolvido para diretores e gerentes comerciais de diversos setores do mercado. CH: 8h

Curso sobre Governança de TI
Apresenta um roteiro para as organizações de TI revisarem seus processos e adotarem novas práticas para a gestão para melhorar sua eficiência e segurança da informação. Inclui um tópico sobre governança em Cloud Computing. CH: 8h

Curso de Fundamentos de Cloud Computing
Apresenta os principais tópicos de computação na nuvem para analistas e executivos de TI para desenvolvimento de análises técnica/econômica de migração de suas aplicações para o ambiente da nuvem. CH: 8h

Workshop sobre Governança da Inovação em TI
Discute e apresenta um modelo de governança da inovação em TI. O conteúdo inclui ferramentas de gestão da inovação e um caso prático para fixação dos conceitos. Se apresentado na modalidade "in company", discute um caso real da empresa. CH: 8h

Curso de Introdução a Big Data
Apresenta os conceitos de Big Data, migração e transformação de dados (ETL), ferramentas analíticas e a arquitetura para processamento e armazenamento, incluindo Hadoop, MapReduce e bancos de dados orientados a Big Data. CH: 8h

Curso sobre Gestão da Inovação Estratégica
Apresenta técnicas e modelos de gestão para definir metas de crescimento, estimular a criatividade, identificar novos atributos de produtos, criar insights para novos produtos e modelos de negócios e estratégias de execução. CH: 8h

Curso sobre E-Commerce
Apresenta os principais elementos para a elaboração de um plano de negócios digital. Aborda ainda, o comportamento dos consumidores e as tecnologias atuais da Internet, incluindo gestão de risco contra fraudes e Big Data. CH: 8h

Curso sobre Como Montar uma Organização de Segurança de TI
Discute vários modelos organizacionais, funções e processos para a criação de uma área de segurança, incluindo ainda: políticas, gestão de risco, testes de intrusão, teste de aplicações e computação Forense. CH: 8h

Curso sobre Smart Grid Cyber Security
Apresenta os elementos da infraestrutura cibernética para redes inteligentes de energia elétrica, estratégias de arquitetura e operação, suas vulnerabilidades e gestão de risco. Curso para engenheiros e especialistas em segurança do setor de energia. CH: 8h

Curso sobre Processos e Técnicas de Aquisição de Produtos e Serviços
Apresenta um processo para reduzir o risco operacional das compras, melhorar a satisfação dos clientes internos, melhorar o relacionamento com fornecedores, e transformar a área de suprimentos em uma organização estratégica. CH: 8h

Curso sobre Organizações Sustentáveis
Apresenta um roteiro para a adoção de práticas sustentáveis nas organizações usando conceitos de responsabilidade socioambiental. Baseado nas métricas do GRI (*Global Reporting Initiative*) e CDP (*Carbon Disclosure Project*). CH: 8h

Workshop sobre Eficiência Energética e uso Racional de Água
Apresenta o cenário do setor hídrico e elétrico brasileiro, regulamentação do setor e normas internacionais. Discute maneiras para engajamento e estimulo à criatividade dos funcionários para de redução de custos e uso eficiente de energia e água. CH: 8h

Anexo VII

Coordenador dos Projetos

Eduardo Fagundes é engenheiro eletricista, executivo de TI com experiência internacional e professor de programas de pós-graduação.

Em 1996, criou o website Efagundes.com, um portal de conteúdo e cursos online gratuitos sobre inovação, tecnologia e sustentabilidade. Hoje o portal recebe mais de 1.400 visitas diárias e tem mais de 17.000 aulas assistidas mensalmente.

Em 2008, fundou a nMentors, uma empresa de treinamento especializada em Smart Grid, energia renovável e tecnologia da informação. O objetivo da nMentors é ser a ponte entre as tecnologias utilizadas no setor de energia e as empresas de energia e consumidores, transferindo know-how para inovação e melhoria contínua de processos.

Sua experiência profissional inclui projetos na Alemanha, Argentina, Brasil, Estados Unidos, Índia, Itália e Reino Unido para a Ford Motor Company (indústria) e AES Corp. (energia). Foi gerente de TI na Ford South America Operations (incluindo a joint venture entre Ford e VW na Argentina e Brasil) e CIO na AES Brasil (AES Eletropaulo, AES Tietê e AES Uruguaiana).

Nesta jornada, trabalha com novas tecnologias, desenvolve treinamentos e plataformas de software para aumentar a produtividade, disponibilidade, segurança cibernética, monitoramento e automação. Meu portfólio inclui Big Data, IoT (Internet of Things) e Analytics (ferramentas avançadas de análise de dados).

Eduardo é graduado em Engenharia Elétrica pela PUC-RS, mestre em engenharia pela Universidade Mackenzie (SP), especialização de telecomunicações pela FAAP-SP, extensão universitária em liderança e negócios na Dardem School of Business da Universidade da Virgínia (EUA) e outros cursos de gestão na Fundação Getúlio Vargas, Universidade de São Paulo e Fundação Vanzolini. (Anexo VII)

Ministra aulas em programas de pós-graduação na Universidade Mackenzie (Big Data, Engenharia de Software e Gestão de Riscos) e no Master Business Administration (MBA) na FIAP-SP (Projetos de Responsabilidade Socioambiental).