Segurança Cibernética para Processos Operativos em Sistemas de Energia Elétrica

Astrid Heinisch, Leonardo Leite, Bárbara Spyer, Marcos Rabello

***Resumo* – As Redes Inteligentes - *Smart Grids* –, em sua concepção, demandam a utilização de um grande número de dispositivos de sensoriamento, o emprego de tecnologias de telecomunicações sobrepostas à infraestrutura de energia e um processamento expressivo de dados coletados a partir dos pontos de automação. Essa nova infraestrutura pode aumentar significativamente a eficiência e confiabilidade da rede de distribuição de energia, mas também pode criar muitas vulnerabilidades caso não seja concebida com os controles de segurança apropriados. Este trabalho discute os principais aspectos relacionados à segurança cibernética em uma empresa distribuidora de energia e propõe o desenvolvimento de um aplicativo gestor dedicado a registrar e monitorar os parâmetros de segurança cibernética configurados nos ativos críticos de operação do sistema elétrico.**

Palavras-chave* – SCADA, Segurança Cibernética, Sistema Elétrico, *Smart Grid.

I. Introdução

Nos últimos anos, a indústria de energia elétrica tem apresentado uma preocupação crescente com o aumento de confiabilidade dos sistemas de potência, o que tem levado a questionamentos relacionados com a sua segurança, naturalmente realçados por diversas ocorrências de *cyber*-ataques em todos os tipos de instalações no mundo inteiro.

No cenário atual, a confiabilidade desses sistemas está ameaçada não só por falhas de equipamentos, condições climáticas adversas, desastres naturais, consumo crescente de energia elétrica, mas também por *cyber*-terroristas cujo objetivo é interromper o fornecimento de eletricidade através do acesso ilegal aos recursos de geração, transmissão e distribuição de energia.

A segurança cibernética na indústria de energia elétrica representa um grande desafio, pois sistemas SCADA/EMS (*Supervisory Control and Data Acquisition System / Energy Management System*) e DCS (*Distributed Control Systems*) foram projetados priorizando eficiência e confiabilidade, ao invés de segurança. Muitos destes sistemas carecem até mesmo de mecanismos básicos de segurança, especialmente se comparados com os sistemas atuais de gestão de informações corporativas.

A supervisão e o controle dos serviços de distribuição de energia elétrica passaram a utilizar, de forma mais ampla, sistemas do tipo SCADA, interligados através de uma rede de telecomunicações aos IEDs (*Intelligent Electronic Devices*) instalados em campo. Estes sistemas eram praticamente imunes a *cyber*-ataques, uma vez que utilizavam plataformas de *software* e *hardware* proprietárias e encontravam-se isolados de sistemas externos. No entanto, ao longo do ciclo evolutivo, os sistemas SCADA, os IEDs, bem como as tecnologias utilizadas para comunicação de dados, migraram para plataformas comerciais interligadas a sistemas corporativos e de gestão das concessionárias.

Eventos recentes ocorridos em plantas de energia têm mostrado que estes sistemas encontram-se vulneráveis a invasões e têm, cada vez mais, sido alvo de ataques de grupos terroristas, *hackers* profissionais e até mesmo funcionários insatisfeitos. Em junho de 2010, foi detectado um vírus denominado *Stuxnet* [1] desenvolvido especificamente para atacar o sistema de controle industrial SCADA, em instalações de enriquecimento de urânio iranianas.

Por outro lado, os sistemas SCADA/EMS estão interconectados com sistemas de gestão de informações corporativas. Essa interação é necessária para fornecer aos gestores da corporação, acesso a dados críticos sobre seus sistemas operativos, assim como para habilitar acesso remoto às redes corporativas para aqueles que estão fora da empresa, em outras instalações, em viagem, ou em visita a clientes, geralmente por meio de notebooks desprotegidos. Ao mesmo tempo, outros funcionários ou terceiros necessitam de acesso remoto aos sistemas de controle, por meio de modem, por exemplo, para manter operações em 24x7.

Infelizmente esses modos de interconexão introduzem novos pontos de vulnerabilidade, uma vez que as eventuais deficiências de segurança de uns e outros podem se reforçar mutuamente, aumentando a vulnerabilidade como um todo. Muitas vezes esse problema é reforçado pelos próprios operadores dos sistemas de controle, que adotam diversas práticas para aumentar a eficiência operativa, muitas das quais acabam também por aumentar a vulnerabilidade destes sistemas a *cyber*-ataques. Essas falhas podem permitir que um *cyber*-ataque resulte na inoculação de vírus ou de códigos maliciosos nos próprios sistemas de controle. Além disso, as exigências de operação em tempo integral dos sistemas de

Este trabalho foi desenvolvido no âmbito do Programa de Pesquisa e Desenvolvimento Tecnológico do Setor de Energia Elétrica regulado pela ANEEL e consta dos Anais do VI Congresso de Inovação Tecnológica em Energia Elétrica (VI CITENEL), realizado em Fortaleza/CE, no período de 17 a 19 de agosto de 2011.

Astrid Heinisch e Leonardo Leite trabalham na 'FITec Technologies' (e-mails: aheinisch@fitec.org.br; lleite@fitec.org.br)

Bárbara Spyer trabalha na 'Concert Technologies' (e-mail: barbara.spyer@concert.com.br)

Marcos Rabello trabalha na 'CEMIG Distribuição S.A.' (e-mail: mrabello@cemig.com.br)

controle dificultam a implementação e os testes de segurança, pois estes sistemas não podem ser apartados da rede.

Neste contexto, esse projeto propõe estabelecer diretrizes de segurança cibernética aplicado aos processos operativos de uma concessionária de distribuição de energia e implementar um software dedicado a registrar e monitorar os parâmetros de segurança cibernética configurados nos ativos da rede operativa do(s) Perímetro(s) de Segurança Eletrônica da distribuidora de energia.

O projeto, ora em execução, já apresenta resultados relacionados ao estudo, concepção e aplicação de diretrizes de segurança cibernética aplicados à concessionária de energia elétrica. Atualmente encontra-se em fase de desenvolvimento do software aplicativo que será submetido a uma prova de conceito em uma ambiente controlado.

O projeto propiciará à concessionária de energia um primeiro exercício na abordagem das questões e tecnologias envolvidas na segurança cibernética operativa, resultando em otimização de processos e de mecanismos de segurança, com reflexos na continuidade e qualidade do fornecimento de energia elétrica, beneficiando a empresa e a sociedade.

Uma vez que o Brasil ainda não dispõe de diretrizes de segurança cibernética para as concessionárias de energia elétrica, considerando-se o caráter recente dessa discussão no mercado de sistemas de potência, com o estudo, discussão e adequação de padrões internacionais às necessidades e características das empresas nacionais deste setor, objetiva-se obter um conjunto de diretrizes de segurança cibernética que atenda à CEMIG Distribuição. Através deste conjunto de diretrizes a CEMIG passará a dispor de instruções normativas de segurança cibernética capazes de orientar a implementação de ações e ferramentas que venham a consolidar as práticas de *cyber*-segurança na companhia, se estendendo para as demais empresas de geração, transmissão e distribuição do setor.

A Tabela 1 apresenta os dados gerais do projeto:

Tabela I. Dados do Projeto

Título	Gestor de Cyber Segurança Operativa
Código	D330
Ano de Início	2009
Duração	2 anos
Status	Em Execução
Entidades Executoras	FITec e Concert
Empresa de Energia	Cemig Distribuição S.A. – CEMIG D

II. Segurança Cibernética

A. Conceituação

A indústria de energia elétrica tem experimentado contínuas mudanças e avanços tecnológicos revolucionando o modo de geração, transmissão, distribuição e consumo de energia elétrica.

Assim, um esforço coordenado e focado para modernizar o sistema elétrico, em especial o ambiente de distribuição, faz-se necessário para o atendimento efetivo e de forma integrada às novas demandas. Nesse contexto, surge o *Smart Grid*, como um conceito tecnológico que propõe uma ampla arquitetura baseada em sistemas abertos, uso intensivo de sensores, redes de comunicação bidirecionais e sistemas computacionais para suportar as operações e serviços oferecidos pelas companhias de energia elétrica, abrangendo as áreas de geração, transmissão, distribuição e consumidor. Como benefícios, essa arquitetura permite novos serviços como a otimização de geração e armazenamento de energia, predição, auto-recuperação, maior eficiência na transmissão e distribuição e novas facilidades para o consumidor [2].

A aplicação do conceito *Smart Grid* preconiza o aumento da eficiência operacional e da confiabilidade do sistema de energia, novos serviços ao consumidor e um meio mais econômico e inteligente de gerar, transmitir e distribuir a energia, minimizando os impactos ambientais. Essas melhorias contam com o emprego de novas tecnologias de comunicação e um novo patamar de interconectividade construído sobre o sistema de energia, bem como a cooperação entre diferentes organizações e a análise de uma quantidade massiva de dados sensoriados. Entretanto, o emprego dessas novas tecnologias e o amplo acesso a dispositivos e dados relacionados ao sistema elétrico, torna o sistema vulnerável a potenciais ataques cibernéticos [3].

Sistemas, aplicações, redes e ambientes completamente seguros não existem e a infraestrutura *Smart Grid* não será uma exceção. Embora cada componente dessa nova infraestrutura possibilite novas facilidades operacionais, eles também introduzem novas vulnerabilidades e riscos adicionais ao sistema elétrico. Caso as questões de segurança não sejam tratadas com propriedade, pessoas e/ou sistemas mal intencionados irão explorar essas vulnerabilidades por diferentes motivações: curiosidade, benefícios financeiros, notoriedade, sabotagem e, até mesmo, como mecanismo de guerra [4].

Dessa forma, ao se implantar uma infraestrutura aderente ao conceito *Smart Grid* em uma concessionária de energia elétrica, seja de geração, transmissão ou distribuição, é necessário estabelecer um Programa de Segurança Cibernética aplicado aos processos operativos que enderece as seguintes questões:

- Identificação, classificação e avaliação de risco;
- Estabelecimento de uma política de segurança cibernética;
- Elaboração do plano de segurança cibernética;
- Análise de Contramedidas de Segurança;
- Estabelecimento de uma estrutura organizacional multidisciplinar;
- Elaboração de um plano de continuidade;
- Estabelecimento de processo de auditoria;
- Treinamento e campanhas de sensibilização;
- Adequação de perfil profissional;
- Revisão, manutenção e atualização do plano de segurança cibernética.

B. Aspectos Regulatórios

Nos Estados Unidos, as iniciativas de padronização e regulamentação de requisitos de segurança estão formalizadas coletivamente como padrões NERC CIP (*North American Electric Reliability Council's Critical Infrastructure Protection Standards*). Esses padrões substituem diretrizes adotadas em anos anteriores (NERC Standard 1200) e representam o primeiro esboço de normas de proteção contra ataques cibernéticos na indústria de energia elétrica. Lá, o atendi-

mento destas diretrizes é garantido pela ERO (*Energy Reliability Organization)*. O NERC foi designado como ERO em julho de 2006.

As diretrizes NERC/CIP identificam os requisitos mínimos para implementar e manter um programa de segurança cibernética e para proteger o patrimônio computadorizado crítico para operação confiável do sistema elétrico em larga escala. Essas diretrizes estão divididas em nove padrões [5]:

- CIP-001: Registro de Sabotagem;
- CIP-002: Identificação de Patrimônio Cibernético Crítico;
- CIP-003: Controles de Gestão de Segurança;
- CIP-004: Pessoal e Treinamento;
- CIP-005: Perímetros de Segurança Eletrônica;
- CIP-006: Segurança Física;
- CIP-007: Gestão de Segurança de Sistemas;
- CIP-008: Registro de Incidentes e Planejamento de Resposta;
- CIP-009: Planos de Recuperação para Patrimônios Computadorizados Críticos.

Complementarmente, as Normas ANSI/ISA 99.02.01 (*American National Standards Institute/ International Society of Automation*) [6] definem os elementos necessários para estabelecer um sistema de gerenciamento da segurança cibernética para sistemas de controle e automação e provêem um guia para o desenvolvimento desses elementos. São guias para segurança de sistemas de controle industrial e identificam as vulnerabilidades e ameaças comuns a estes sistemas.

Como os processos operativos das empresas de energia são essencialmente suportados por sistema de supervisão e controle (ex. SCADA - *Supervisory Control and Data Acquisition System*, OMS - *Outage Management System*, EMS - *Energy Management System*, etc.) as diretrizes dessa norma se tornam bastante aplicáveis.

Este trabalho de pesquisa e desenvolvimento propõe o estudo e aplicação dos padrões NERC-CIP e ANSI, visando a sua discussão e adequação face às necessidades e características das empresas nacionais deste setor.

III. Implementação

A metodologia utilizada para a implementação desse projeto caracterizou-se, em um primeiro momento, por pesquisas na área de conhecimento cientifico de segurança cibernética aplicada aos ambientes operacionais e gerenciais de uma concessionária de energia, com foco no estudo e aplicação dos padrões NERC/CIP e ANSI.

Em seguida, foram identificados e caracterizados os processos de automação em termos dos seus requisitos técnicos e funcionais, especificamente aqueles relacionados aos parâmetros de comunicação e fluxo de dados.

Para suportar os processos de automação foi concebida uma Rede Operativa de Dados, baseada em sistemas de comunicação convergentes para prover conectividade entre os pontos de automação e os sistemas de controle.

Foram delimitados os domínios e perímetros de segurança e seus respectivos ativos cibernéticos críticos onde as diretrizes de segurança serão aplicadas. Para cada ativo foi realizada uma análise de vulnerabilidade. Os conceitos de domínios e perímetros de segurança serão detalhados a seguir.

Por fim, propõem-se a implementação de um aplicativo gestor de segurança cibernética que coletará e classificará os parâmetros de segurança cibernética configurados nos ativos da rede operativa dos respectivos perímetros de segurança eletrônica, servindo como ferramenta de apoio à detecção e à classificação das vulnerabilidades existentes.

As seções seguintes detalham cada fase do projeto.

A. Processos de Automação

Os processos de automação do sistema elétrico são estruturados por itens referentes às funcionalidades englobadas, a informação tratada dentro do processo e a tecnologia adotada no suporte aos demais itens, fechando o ciclo do processo. Quanto às funções englobadas no processo de automação, pode-se dizer que, de forma geral, há as funções específicas voltadas à **automação de rede, automação de medição, automação de subestação e automação de serviços em campo** [7]. Para atender a essas funções de automação são necessárias tecnologias capazes de oferecer infraestrutura de telecomunicações e computacionais que tratem do transporte e manipulação das informações trocadas para a execução dessas funções. A segurança é o pré-requisito para confiabilidade e disponibilidade neste novo ambiente interconectado preconizado pelas Redes Inteligentes (*Smart Grids*).

A operacionalização de cada função de automação demanda requisitos específicos. Uma das primeiras tarefas na especificação de requisitos voltada à estratégia de segurança cibernética para *Smart Grid* é analisar as interfaces dos processos a serem automatizados. Trata-se da análise dos envolvidos revendo e revisando as interfaces lógicas, identificando os fluxos de dados, identificando as restrições e questões de segurança, e especificando os níveis de impacto da confidencialidade, integridade e disponibilidade de dados em cada interface. Para tratar as interfaces inerentes a cada função de automação, do ponto de vista da segurança da informação, adotou-se nesse trabalho, os conceitos de perímetros e domínios de se segurança, discutidos adiante.

B. Rede Operativa de Dados - ROD

Para suportar os requisitos de comunicação demandados pelas funções de automação do sistema elétrico, foi concebida a Rede Operativa de Dados – ROD [8].

Diferentemente da Rede Corporativa de Dados, utilizada pelas companhias de energia para transportar informações relacionadas a serviços corporativos (ex. intranet, e-mail, ERP – *Enterprise Resource Planning*, etc.), a ROD transporta informações relacionadas a funções operacionais demandadas pelos processos de automação descritos na seção anterior. Tais processos apresentam elevada criticidade ao se considerar os parâmetros de confidencialidade, disponibilidade, throughput, tempo de resposta e segurança da informação.

A ROD abrange o centro de operação, as redes de comunicação e os ativos da concessionária (subestações, chaves, medidores, sensores, etc.) relacionados aos seus processos operativos. Neste contexto, cada parte do sistema elétrico é visto como uma fonte de informação para a realização fim a

fim das funções operativas. Essa informação deve ser transportada por soluções convergentes de comunicação adotadas em cada processo de automação.

Por diversos motivos (ex. conectividade, capacidade de endereçamento, padronização, etc.), adotam-se tecnologias baseadas em protocolo IP (*Internet Protocol*), como forma de permitir a interação entre diversas tecnologias de acesso em uma única solução de comunicação em consonância com as tendências das redes de próxima geração. A principal característica a ser alcançada com essa arquitetura baseada em IP é a separação dos serviços e das aplicações, do transporte das informações a eles relacionadas. Ou seja, desde que o meio de transporte atenda aos requisitos especificados para aquela aplicação envolvida em um processo de automação, a tecnologia de comunicação por ele adotada se torna indiferente ao processo. Isso possibilita uma visão do sistema elétrico como uma fonte única de informação, que será transportada com qualidade de serviço. O provimento do serviço de transporte dos dados referentes às funções de automação se dará via protocolo IP, na modalidade "fim a fim", entre o ponto a ser automatizado e o centro de controle da CEMIG D.

Em se tratando especificamente da rede de comunicação, devido à dispersão e alta capilaridade dos pontos de automação, localizados em regiões urbanas, semi-urbarnas e rurais, diferentes tipos de tecnologias de telecomunicações, com e sem fio, são empregadas, conforme ilustrados na figura 1.

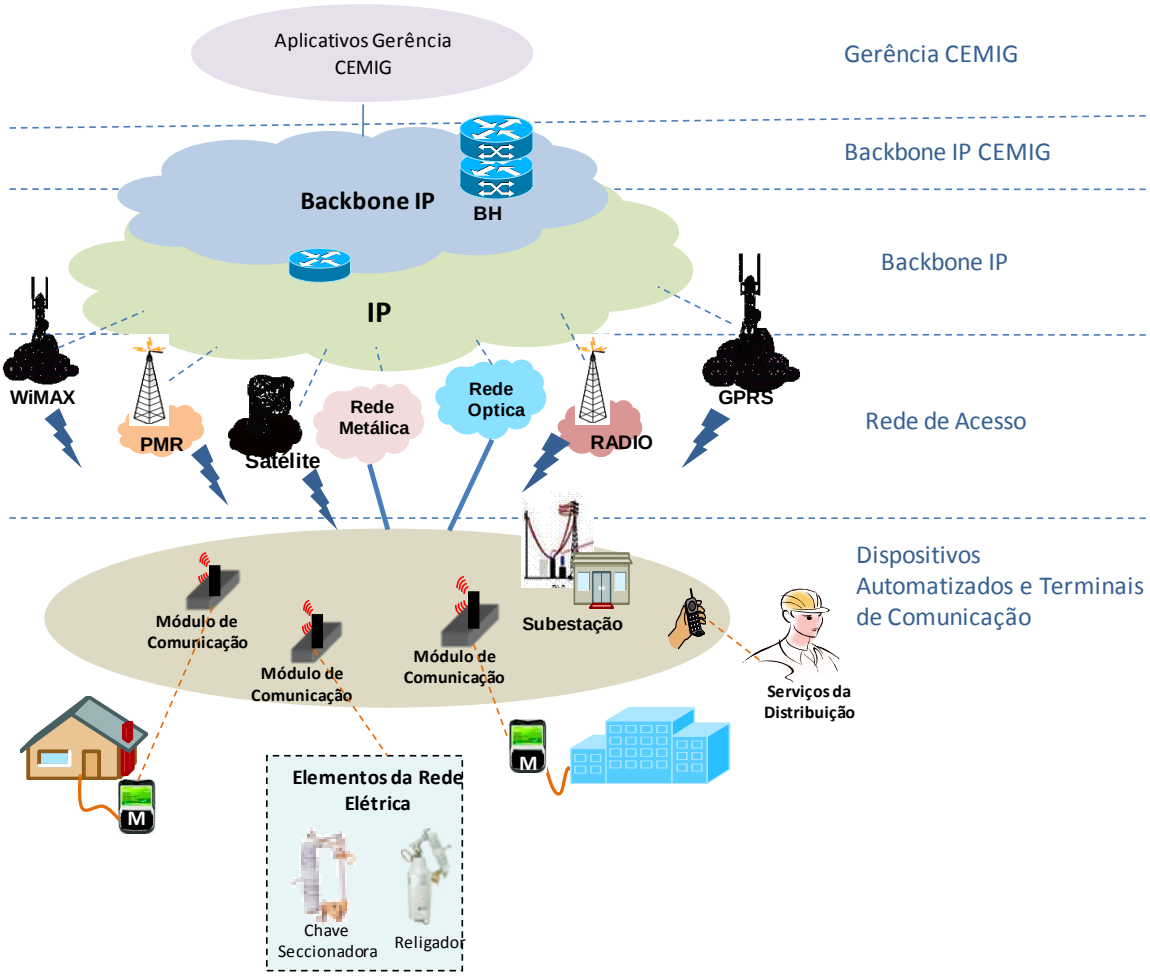

Figura 1 – Rede Operativa de Dados

C. Perímetros e Domínios da Segurança

Para melhor identificação dos requisitos e aplicação dos processos de segurança a Rede Operativa de Dados foi delineada em Perímetros e Domínios de Segurança [7]:

Perímetro da Segurança refere-se a um limite físico protegido, que compartilha um nível de segurança específico através de um elemento comum e representa um conjunto de recursos (recursos de rede, computacional e físico) que são administrados, assegurados e gerenciados através de um conjunto consistente de políticas e processos de segurança. Neste projeto, um perímetro de segurança é delimitado por pontos que permitem acesso à ROD. Cada Perímetro da Segurança é responsável por seu próprio processo de segurança geral (ativos, políticas, desenvolvimento, monitoramento e treinamento).

Domínio da Segurança refere-se a um determinado processo de automação "fim a fim", permeando um ou mais perímetros de segurança. Representa, então, um conjunto de recursos (recursos de rede, computacional e físico) que são administrados, assegurados e gerenciados através de um conjunto consistente de políticas e processos de segurança

relacionados a uma funcionalidade de automação específica. Um Domínio da Segurança provê um conjunto bem conhecido de funções de segurança que são usadas para transações seguras da informação dentro daquele domínio. No âmbito deste projeto, determinam-se Domínios de Segurança voltados à automação de elementos da rede elétrica, à automação da medição de energia e à automação de subestação.

Foram mapeados os seguintes Domínios de Segurança na ROD:

➢ Domínios de Segurança associados à Automação de Dispositivos Eletrônicos Inteligentes da Rede Elétrica (IED – *Intelligent Electronic Devices*):
- Supervisão e Controle de IEDs;
- Medição de IEDs;
- Oscilografia de IEDs;
- Proteção de IEDs.

➢ Domínios de Segurança associados à Automação de Subestações:
- Supervisão e Controle em Subestações;
- Medição em Subestações;
- Oscilografia em Subestações;
- Proteção em Subestações;
- Videomonitoramento em Subestações;
- Serviços Corporativos em Subestações.

➢ Domínios de Segurança associados à Infraestrutura de Medição Avançada de Energia (AMI – *Advanced Metering Infraestructure*):
- Acesso a Dados de Medição;
- Parametrização de Medidores;
- Acesso a Dados de Alarmes;
- Portal do Consumidor;
- Gerenciamento de Carga.

A figura 2 ilustra o conceito de perímetros e domínios de segurança da ROD.

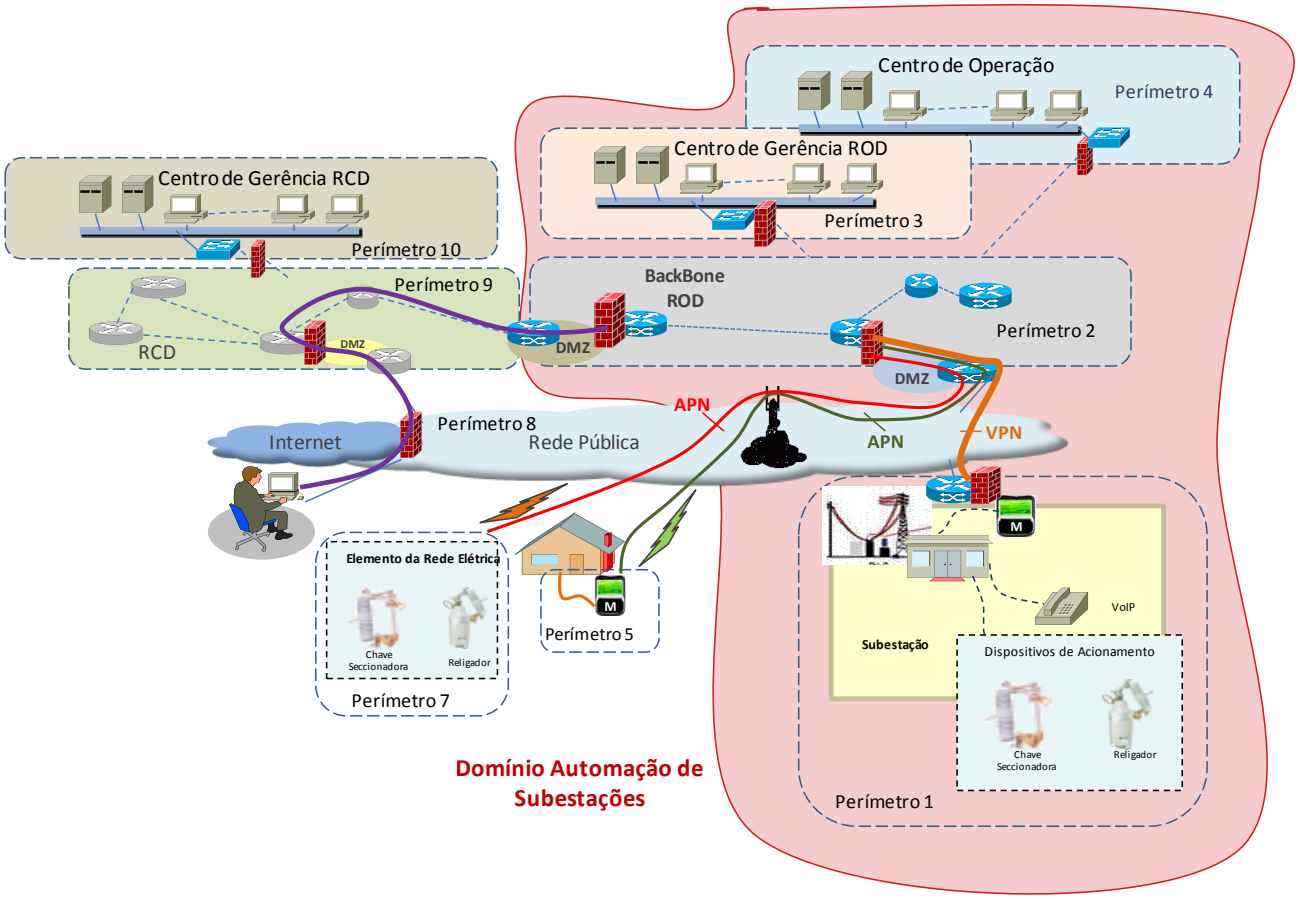

Figura 2 – Domínios e Perímetros de Segurança Cibernética

D. Análise de Vulnerabilidade de Ativos Cibernéticos Críticos

Os conceitos de confidencialidade, integridade e disponibilidade devem ser considerados em qualquer processo do negócio da organização, notadamente em processos automatizados [9].

Para a análise do impacto nos processos de automação da CEMIG D, referente aos domínios de segurança definidos anteriormente, foi verificada junto aos especialistas de cada processo operativo, o impacto da ocorrência da violação dos seguintes aspectos da segurança da informação: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade, denominada Análise CIDAL.

Para a avaliação da rapidez com que a CEMIG D deseja responder às potenciais violações, também foi levantada, junto aos mesmos especialistas, a pontuação para Gravidade, Urgência e Tendência, denominada Análise GUT.

A pontuação da sensibilidade, quanto à quebra das propriedades de segurança da informação para cada processo de automação, permite avaliar os seus impactos. Com isso, é possível entender melhor, através de pontuações atribuídas a cada processo de automação da CEMIG D, o impacto potencial nos negócios associados a tais processos, caso ocorra alguma quebra de segurança.

Como exemplo, a tabela II ilustra a análise CIDAL para as funções relacionadas ao domínio de Automação de Subestações.

Tabela II. Análise CIDAL – Funções de Automação de Subestação

Funções de Automação de Subestações	**CIDAL**				
	Confidencialidade	**Integridade**	**Disponibilidade**	**Autenticidade**	**Legalidade**
Medição	Importante	Importante	Relevante	Crítico	Não Considerável
Supervisão e Controle	Vital	Vital	Vital	Vital	Não Considerável
Oscilografia	Relevante	Crítico	Importante	Crítico	Não Considerável
Monitoramento de Ativos	Relevante	Crítico	Importante	Crítico	Não Considerável
Acesso Remoto a IEDs	Vital	Vital	Importante	Vital	Não Considerável
Vídeo Monitoramento	Relevante	Importante	Importante	Importante	Não Considerável

A análise GUT permite maior detalhamento dos processos de negócio, neste contexto, os processos de automação. Essa análise é pontuada com base na associação dos impactos CIDAL e sua Gravidade, Urgência e Tendência (GUT).

Ocorrendo a quebra de segurança de qualquer uma das propriedades da segurança da informação (CIDAL), analisa-se:

- A Gravidade para os processos de automação;
- A Urgência com que as ações para solução dos problemas encontrados serão iniciadas;
- A *Tendência* dessa situação, caso nenhuma ação de segurança seja tomada.

A tabela III apresenta a análise GUT para as funções relacionadas ao domínio de Automação de Subestações.

Tabela III - Análise CIDAL – Funções de Automação de Subestação

Funções de Automação de Subestações	**GUT**		
	Gravidade	**Urgência**	**Tendência**
Medição	Grave	Alguma	Médio Prazo
Supervisão e Controle	Muitíssimo Grave	Imediata	Rapidamente
Oscilografia	Grave	Alguma	Médio Prazo
Monitoramento de Ativos	Pouco Grave	Alguma	Médio Prazo
Acesso Remoto a IEDs	Muito Grave	Alguma	Médio Prazo
Vídeo Monitoramento	Pouco Grave	Alguma	Médio Prazo

Da mesma forma, foram realizadas as análises de impacto CIDAL e GUT para as funções dos respectivos domínios de Automação de Rede e Automação de Medição.

A consolidação da pontuação CIDAL e GUT, atribuída aos processos de automação, permitiu a classificação dos respectivos ativos cibernéticos críticos. Essa classificação possibilita determinar o nível de criticidade de um determinado ativo de acordo com a sua funcionalidade e importância para atendimento a uma determinada função dentro de um processo de automação.

A tabela IV classifica cada ativo cibernético presente na subestação de acordo com a sua importância para cada função de automação de subestação. A pontuação atribuída a cada ativo indica, de forma absoluta, o quão crítico ou importante é aquele ativo em relação aos demais para atendimento às funções de automação relacionadas.

Tabela IV – Criticidade dos Ativos Cibernéticos da Subestação

Ativos Cibernéticos -Subestação	Criticidade
Medidores	1,20
Remota de medição	1,20
Conversor Eletro Óptico - Medição	1,20
Relé de Proteção	5,50
Switch Rede de Proteção	3,85
Religadores	4,45
Conversor Eletro Óptico Religador	3,45
UCC	3,45
Concentrador Oscilografia	2,05
Sensor par Monitoração de Ativos	1,30
Computador Industrial	1,40
Câmera	0,70
Servidor (PVDR)	0,70
Switch Rede de Dados	4,90
Roteador	7,70

IV. Aplicativo Gestor de Segurança Cibernética

Na busca de uma maior segurança nos sistemas de automação e controle dos processos operativos das empresas distribuidoras de energia, o projeto busca especificar e construir um *software* dedicado a coletar e classificar os parâmetros de segurança cibernética configurados nos ativos da rede operativa dos perímetros de segurança eletrônica da concessionária, servindo como ferramenta de apoio à detecção e à classificação das vulnerabilidades existentes. Este aplicativo permitirá a integração a aplicativos GRC (*Governance, Risk Management and Compliance*), no sentido de potencializar a análise de risco das vulnerabilidades detectadas.

Definem-se seis passos para proteger a rede operativa de uma concessionária contra ameaças cibernéticas, listados na tabela V [10]. Primeiramente, é necessário compreender os requisitos da regulamentação vigente. Seminários, discussões com diferentes *players* e eventos industriais são formas interessantes para angariar as informações mais relevantes. Para o software Aplicativo Supervisor de Perímetro Eletrônico de Segurança (ASPES), objeto final do atual projeto e

atualmente em fase de desenvolvimento, os requisitos para a coleta de parâmetros de segurança cibernéticos tem sido balizada pelas normas NERC/CIP [5], ANSI/ISA 99 [6] e NIST 800-82 [11].

Tabela V - Passos para Segurança Cibernética

Passo 1	Compreender os requisitos regulatórios existentes
Passo 2	Compreender a natureza das ameaças cibernéticas
Passo 3	Identificar as áreas de não observância e de vulnerabilidade
Passo 4	Criar e reforçar procedimentos de segurança em toda empresa
Passo 5	Instalar hardware e software para assegurar a observância e proteger as vulnerabilidades
Passo 6	Monitorar continuamente a evolução das tecnologias e regulamentações

As informações relativas aos parâmetros de segurança cibernética a serem coletados são complementadas em um segundo passo que consiste em compreender a natureza dos ataques cibernéticos. Como citado previamente, os ataques cibernéticos expandiram de ataques a sistemas de tecnologia da informação de propósitos gerais realizados por amadores a ataques realizados por profissionais a plataformas específicas de hardware e software utilizados para controlar e monitorar sistemas em tempo real.

O estudo das normas juntamente com a análise da natureza dos ataques é traduzido em listas de procedimentos de segurança. Estes procedimentos de segurança foram elaborados individualmente para cada ativo cibernético crítico integrante dos perímetros de segurança da Rede Operativa de Dados da CEMIG. As listas de procedimentos de segurança são constituídas de configurações ideais para cada um destes ativos, tornando-se referência de parametrização dos mesmos.

O terceiro passo é a identificação de áreas de vulnerabilidade e de não observância. É nessa questão que o ASPES tem sua maior influência. Até o momento, auditorias são realizadas para identificar as vulnerabilidades de sistemas, porém, são limitadas às redes corporativas. O ASPES compreende a avaliação de ativos ligados a ROD permitindo a identificação de falhas de configuração em equipamentos de uso específico como medidores, religadores, relés de proteção, switches, roteadores, dentre outros.

O ASPES é composto por quatro componentes básicos, sendo eles:

- Banco de Dados;
- Containeres;
- Coletores;
- Interface Homem-Máquina.

O banco de dados e a Interface Homem-Máquina (IHM) são componentes alocados externamente ao perímetro eletrônico de segurança, como mostra a figura 3. Os Containeres e Coletores são inseridos em cada perímetro de segurança estabelecido dentro do sistema da concessionária.

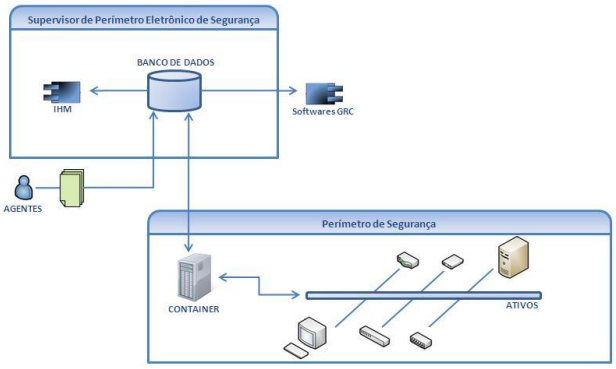

Figura 3. Componentes do ASPES

As listas de procedimentos de segurança são, portanto, traduzidas em parâmetros de segurança e inseridas no banco de dados por agentes. Esta inserção manual forma a população de tabelas com os valores ideais que são posteriormente confrontados com os dados coletados pelo ASPES. O monitoramento constante do resultado deste confronto permite a identificação das vulnerabilidades de cada ativo de cada perímetro e, conseqüentemente, da ROD.

Os agentes são responsáveis pela inserção de dados referentes às listas de procedimentos no banco de dados. O banco de dados do ASPEN pode ser acessado, consumido ou mesmo ter dados inseridos por quatro atores. A forma de conexão, que cada ator estabelece com o banco de dados, é apresentada pela figura 4.

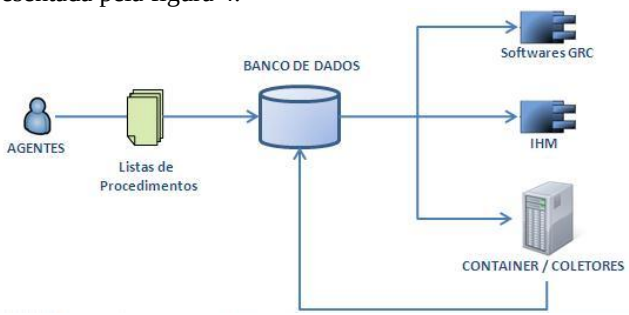

Figura 4. Formas de conexão com o Banco de Dados

A inserção dos parâmetros ideais é realizada através de três tabelas, como apresenta a figura 5. As tabelas apresentam uma relação entre o tipo do ativo, os seus modelos e as configurações ideais dos mesmos. Cada tipo de ativo é identificado por um ID, assim como cada modelo. Essa inserção de dados é extremamente importante para a conclusão do terceiro passo da Tabela V.

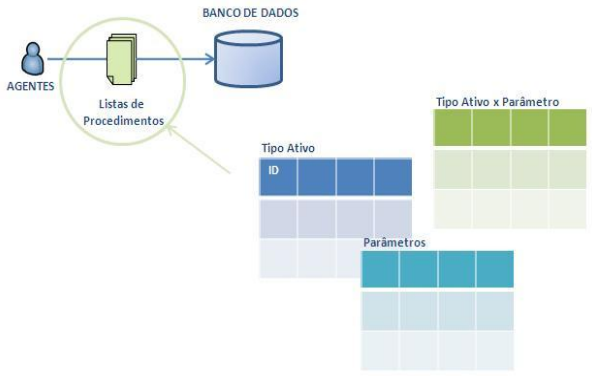

Figura 5. Inserção dos Parâmetros Ideais

A identificação das vulnerabilidades depende não somente da inserção dos dados ideais, mas também de dados coletados. Para tanto, o ASPES apresenta dois componentes responsáveis por essa função. Os Containeres são responsáveis pelo gerenciamento dos Coletores. Cada perímetro de segurança do sistema da concessionária apresenta um Container. Os Coletores, por sua vez, estão relacionados aos tipos de ativo encontrados em um perímetro. Cada Coletor representa, portanto, um tipo de ativo e não um determinado ativo. O Coletor é responsável por ativos do tipo relés de proteção ou roteadores, por exemplo. No entanto, as tabelas ideais são preenchidas com valores para um determinado modelo de ativo, por exemplo: Relé de Proteção SEL 487B ou roteador CISCO 2801. Os modelos são identificados pelo Coletor como plug-ins.

Um Coletor, portanto, conectado a um roteador irá requerer os parâmetros configurados na tabela do Tipo Ativos Roteador, como apresenta a Figura 6. Nesse momento não há preocupação com a compatibilidade dos valores extraídos com os valores ideais.

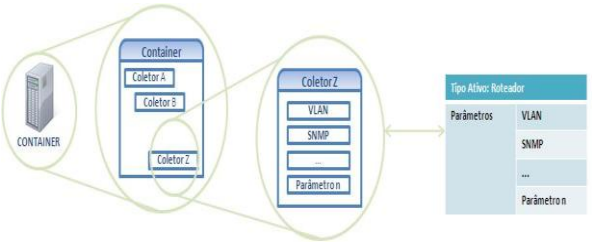

Figura 6. Relação entre Containeres, Coletores e Tipos de Ativos

Uma vez inseridos os dados ideais e coletados os valores reais de cada ativo de um determinado perímetro, é necessário visualizar as incompatibilidades identificadas pela comparação de ambos. A IHM, uma interface web, portanto, acessa o banco de dados para apresentar ao usuário final o resultado da coleta. O ASPES, portanto, é uma ferramenta que realiza todo processo de identificação das vulnerabilidades do sistema.

Existe ainda a possibilidade de integração do ASPES com *softwares* GRCs. Estes possuem a capacidade de realizar a análise de risco das vulnerabilidades dos ativos de rede. Contudo, até o momento, os *softwares* GRCs tinham acesso apenas aos dados da rede corporativa. O ASPES permite que os dados do banco sejam acessados por estes *softwares*, acrescentando uma análise estatística ao resultado das comparações dos dados coletados e inseridos. Para tanto, é necessário que estes sistemas sejam integrados via protocolo de formato aberto ao servidor de aplicação do ASPES.

A criação e a aplicação de procedimentos de segurança são o quarto passo para alcançar a segurança cibernética de uma concessionária. Uma grande porcentagem das falhas de segurança é devida a erros comuns como seleção de senhas fracas e mídias removíveis de armazenamento. Cabe, portanto, às concessionárias fazer cumprir as políticas de segurança estabelecidas. O ASPES pode auxiliar nessa questão incluindo outros parâmetros de segurança em seus Coletores para verificar se as políticas estão sendo cumpridas.

O quinto passo é a instalação de softwares e hardware que irá proteger a rede contra ataques cibernéticos. A instalação do ASPES, assim como de qualquer instrumento, físico ou lógico, deve ser acompanhado de testes exaustivos para não comprometer a integridade da rede. Essa é uma norma apontada pela ANSI/ISA 99 e NIST 800-82.

O aplicativo Supervisor de Perímetro Eletrônico de Segurança será avaliado em duas fases de teste. A primeira fase consiste em desenvolver e testar o protótipo em uma plataforma de teste contendo quatro ativos de rede distintos. Em um segundo momento, após verificado o perfeito funcionamento de todas as funçoes do aplicativo em laboratório, serão realizados testes de aceitação em campo em ambiente controlado para comprovar a sua adequabilidade aos respectivos requisitos técnicos.

Finalmente, o último passo consiste no constante monitoramento de toda a planta de segurança para manter o sistema atualizado com as tecnologias e regulamentações mais atuais. A constante evolução das tecnologias e dos métodos de invasão cibernética exige que o ASPES mantenha sempre em revisão as tabelas de valores ideais. Para tanto, a característica modular do *software* é de extrema importância para suprir essa necessidade. O ASPES permite o acoplamento de novos Coletores e parâmetros de segurança à medida que se fizerem necessários sem necessidade de alteração na arquitetura do aplicativo.

A não observância com as regulamentações e as conseqüentes vulnerabilidades a ataques cibernéticos implicam em sérios problemas que, se não tratados a tempo, terão enormes conseqüências de ordem material, humana e social para todas as concessionárias. O ASPES pretende suprir esta lacuna de segurança, ajudando a evitar que as concessionárias de energia sofram perdas com a incidência dos ataques cibernéticos. As experiências adquiridas, bem como os conceitos aplicados ao ASPES poderão servir como base para a criação de métodos e práticas de vigilância contra ameaças cibernéticas atuais e futuras em sistemas operativos.

V. Conclusões

A nova concepção de redes de energia inteligentes requer o emprego de soluções de segurança eletrônica e física em diferentes níveis. As ameaças de segurança sejam de forma inadvertida ou deliberada, dependendo da sua amplitude e abrangência, podem apresentar conseqüências devastadoras para a indústria de energia (geração, transmissão e distribuição), com grave impacto social e econômico, tanto para a

indústria como para a sociedade.

Em vez de medidas de contenção pontuais a ataques cibernéticos, desde as mais simples às formas mais avançadas, as empresas de serviços essenciais devem adotar um plano de segurança estruturado, que controle e contenha os riscos de forma automática. Somente com políticas de segurança é possível ter respostas proativas e a correta adaptação às vulnerabilidades.

Este trabalho propôs a investigação dos principais aspectos técnicos e normativos relacionados à segurança cibernética aplicada aos processos operativos de uma empresa de distribuição de energia elétrica. Para cada domínio e perímetro de segurança foram definidos os principais requisitos de segurança cibernética e realizada uma análise de vulnerabilidade dos respectivos ativos críticos. O aplicativo gestor de segurança cibernética proposto pretende ser uma ferramenta prática para a análise de vulnerabilidade de tais ativos, podendo ser aplicado em todo o ambiente de automação das concessionárias.

A próxima etapa desse trabalho é a implementação dessa ferramenta e a sua implantação em um ambiente controlado que represente as funções de automação a serem protegidas. Após a prova de conceito, pretende-se ampliá-la para todo o ambiente operativo da concessionária.

VI. AGRADECIMENTOS

Agradecemos a CEMIG Distribuição S.A., particularmente aos profissionais das superintendências TD - Superintendência de Desenvolvimento e Engenharia da Distribuição e TI - Superintendência de Tecnologia da Informação que contribuíram para realização desse trabalho.

VII. REFERÊNCIAS BIBLIOGRÁFICAS

[1] R. Millan "Siemens: Stuxnet worm hit industrial systems" Computerworld, Septemper 14, 2010.
http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142. Acessado em 01 de março de 2010.

[2] C. W. Gellings. "The *Smart Grid* – Enabling Energy Efficiency and Demand Response". Boca Raton, FL, USA. Taylor & Francis, 2009, 300 p.

[3] A. R. Metke and R. L. Ekl, Security Technology for Smart Grid Networks, IEEE Transaction on Smart Grid, Vol 1. No. 1, pp 99-105, June 2010.

[4] T. Flick, J. Morehouse. "Securing the Smart Grid – Next Generation Power Grid Security" . Burlington, MA, USA. Syngress, 2010, 290 p.

[5] NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0. NIST, September, 2009.
NERC Critical Infrastructure Protection (CIP) standards CIP-001 TO CIP-009 (http://www.nerc.com/page.php?cid=2|20).

[6] ANSI/ISA–99.02.01-2009. Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. ANSI/ISA, January, 2009.

[7] A. Heinisch, L. Leite. "Especificação de Requisitos Tecnológicos e de Segurança para a Rede Operativa". CEMIG Distribuição. Belo Horizonte, MG, Brasil. Relatório Técnico RQS-10006-GOP-V01-R01-CMG-CYBSEC-TECNOLOG-SEGURANÇA Setembro, 2010.

[8] A. Heinisch, L. Leite. "Especificação Técnica – Rede Operativa de Dados". CEMIG Distribuição. Belo Horizonte, MG, Brasil. Relatório Técnico. RQS-10005-GOP-V01-R01-CMG-CYBSEC-ESPTEC-COMUN-CONECT. Setembro, 2010.

[9] A. Bastos, R. Caubit. "Gestão de Segurança da Informação – ISO 27001 e 27002 – Uma Visão Prática". Módulo Education Center. Porto Alegre, RS, Brasil, 257 p.

[10] A. Dreher, E. Byres. "Get Smart About Electrical Grid Cyber Security". Transmission & Distribution World, December, 2010.

[11] NIST Special Publication 800-82. Guide to Industrial Control. Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf.