XX Seminário Nacional de Distribuição de Energia Elétrica
SENDI 2012 - 22 a 26 de outubro
Rio de Janeiro - RJ - Brasil

Leonardo Henrique de Melo Leite	Daniel Correa Ramos	Astrid Maria Carneiro Heinisch
Fundação para Inovações Tecnologicas	Concert Technologies SA	Fundação para Inovações Tecnologicas
lleite@fitec.org.br	daniel@concert.com.br	aheinisch@fitec.org.br

Marcos da Silva Rabello	Ariana Silva
Companhia Energética de Minas Gerais	Concert Technologies SA
mrabello@cemig.com.br	ariana.silva@concert.com.br

Segurança Cibernética em Sistemas de Distribuição de Energia Elétrica

Palavras-chave

Rede Operativa de Dados
Redes de Energia Inteligentes - Smart Grids
Segurança Cibernética
Sistema Elétrico de Potência

Resumo

As Redes de Energia Inteligentes - *Smart Grids* –, em sua concepção, vêm ampliar o uso de novos sistemas de comunicação, sensoriamento e controle em todos os níveis da rede de energia elétrica, demandando o emprego extensivo de tecnologias da informação e comunicação. Essa nova infraestrutura, embora possa aumentar significativamente a eficiência e confiabilidade da rede de distribuição de energia, pode criar novas vulnerabilidades, aumentando a probabilidade de sucesso de ataques cibernéticos. Este trabalho apresenta os aspectos relativos à segurança cibernética aplicada aos processos voltados à automação da distribuição de energia elétrica e resultados práticos de análise de vulnerabilidade de ativos cibernéticos críticos em uma subestação de distribuição.

1. Introdução

Dentre as novas ameaças trazidas à tona pela modernização da rede elétrica, destacam-se os ataques remotos

e o comprometimento dessa nova infraestrutura devido ao aumento da interconectividade das redes de comunicação de dados que controlam e monitoram as atividades da rede. Neste cenário, a confiabilidade dos sistemas elétricos de potência está ameaçada não só por falhas de equipamentos, condições climáticas adversas e desastres naturais, 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 supervisão e o controle dos serviços de distribuição de energia elétrica passaram a utilizar, de forma mais ampla, sistemas do tipo SCADA (*Supervisory Control and Data Acquisition*), 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 proprietárias e encontravam-se isolados de sistemas externos. Ao longo do ciclo evolutivo, os sistemas SCADA, os IEDs, bem como os sistemas de TIC (Tecnologia da Informação e Comunicação), migraram para plataformas comerciais interligadas a sistemas corporativos. Eventos recentes ocorridos em plantas de energia vêm confirmar que estes sistemas encontram-se vulneráveis a invasões e que têm sido alvo de ataques de grupos terroristas, hackers profissionais e até mesmo funcionários insatisfeitos (MILLAN,2010, p.1-3).

É neste contexto que a Cemig Distribuição, a Concert Technologies e a FITec desenvolveram um projeto de Pesquisa e Desenvolvimento (P&D) dentro do Programa de Pesquisa e Desenvolvimento Tecnológico do Setor de Energia Elétrica da ANEEL (Agência Nacional de Energia Elétrica) intitulado ***GESTOR DE CYBER SEGURANÇA OPERATIVA / Aplicativo Supervisor de Perímetro Eletrônico de Segurança.*** **Desenvolveu-se e** implementou-se no âmbito deste projeto, um Aplicativo Supervisor de Perímetro Eletrônico de Segurança (ASPES) dedicado a registrar e reportar os parâmetros de segurança configurados nos ativos cibernéticos críticos dos perímetros de segurança eletrônica da rede operativa. Desenvolveu-se neste contexto um estudo que culminou na definição de um conjunto de diretrizes de segurança cibernética baseadas nos padrões NERC CIP (*North American Electric Reliability Council's Critical Infrastructure Protection Standards*) aplicadas aos processos de automação.

Os resultados desse projeto propiciam à concessionária uma abordagem para tratamento de questões e tecnologias relacionadas à segurança cibernética voltada à automação. Aliada aos resultados tem-se a melhoria de processos e de mecanismos de segurança que refletem diretamente na qualidade do fornecimento de energia elétrica, beneficiando a empresa e a sociedade.

Esse artigo apresenta a seguinte estruturação: A seção I apresenta aspectos gerais sobre Segurança Cibernética aplicada à indústria de energia elétrica. A seção II apresenta a metodologia utilizada para a implementação da análise de vulnerabilidade em ativos cibernéticos críticos. A seção III apresenta a arquitetura e o princípio de funcionamento do software ASPES, desenvolvido para suportar a parametrização dos ativos e análise de vulnerabilidade dos domínios de segurança. A seção IV apresenta os resultados dos testes de vulnerabilidade em laboratório e em uma subestação de energia elétrica em operação. Por fim, são apresentadas as conclusões.

2. Desenvolvimento

I. Segurança Cibernética

I.I. 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, fez-

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 (GELLINGS, 2009, p. 300).

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 (METKE & EKL, 2010, p. 99-105).

Pode-se afirmar que 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 (FLICK & MOREHOUSE, 2010, p. 290).

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.

I.II. Aspectos Regulatórios

Nos Estados Unidos, as iniciativas de padronização e regulamentação de requisitos de segurança estão formalizadas coletivamente através do conjunto de normas 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 atendimento 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 distribuídas em nove normas (NIST, 2009, p. 145): 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* - (ANSI, 2009, p. 167) 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 automação e 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, OMS - *Outage Management System*, EMS - *Energy Management System*, etc.) as diretrizes dessa norma se tornam bastante aplicáveis.

Este trabalho de P&D baseou-se estudo e aplicação dos padrões NERC-CIP e ANSIISA 99, visando a sua discussão e adequação face às necessidades e características das empresas concessionárias de energia nacionais.

II. 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 ISA.

Em seguida, foram identificados e caracterizados os processos de automação em termos dos seus requisitos técnicos e funcionais, mais especificamente aqueles relacionados aos parâmetros de comunicação e fluxo de dados. Para suportar os processos de automação, do ponto de vista de comunicação, 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 se aplicam. Para cada ativo foi realizada uma análise sobre as possíveis vulnerabilidades e parâmetros de configuração desses ativos que se relacionam com a segurança cibernética.

Por fim, foi implementado um aplicativo gestor de segurança cibernética capaz de coletar e classificar 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 desenvolvida no decorrer do projeto.

II.I. 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** (HEINISCH & LEITE, 2011, p. 154). 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 pode ser vista como 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* foi analisar as interfaces dos elementos envolvidos nos processos a serem automatizados, bem como o tipo de informação trocada através delas. 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.

II.II. 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 (HEINISCH & LEITE, 2010, p. 39). Diferentemente da Rede Corporativa de Dados, utilizada pelas companhias de energia para transportar informações relacionadas a serviços corporativo-administrativos (ex. intranet, e-mail, ERP – *Enterprise Resource Planning*, etc.), a ROD – Rede Operativa de Dados - transporta informações relacionadas a funções operacionais demandadas pelos processos de automação. 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 críticos da concessionária (subestações, religadores, medidores, sensores, etc.) relacionados aos seus processos operativos. Neste contexto, cada parte do sistema elétrico é vista como uma fonte de informação para a realização fim a fim das funções operativas. Essa informação deve ser transportada por soluções convergentes de comunicação que atenda aos requisitos técnicos de 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 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.

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, podem ser empregadas, conforme ilustrados na Figura 1.

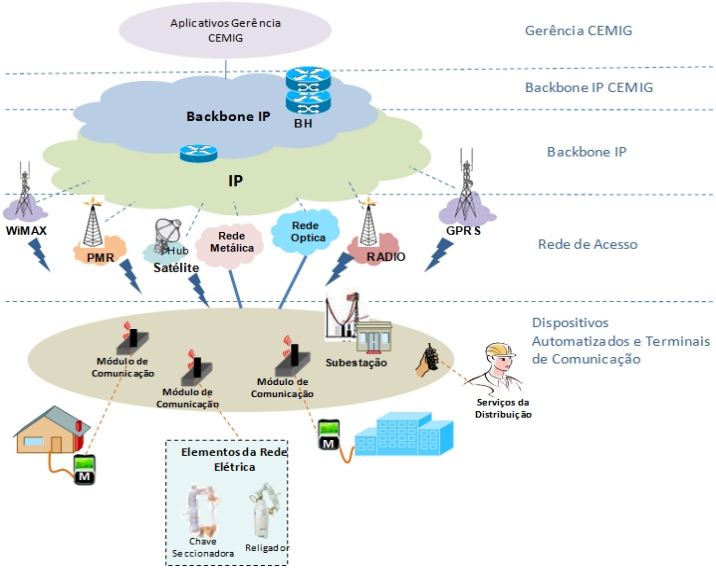

Figura 1: Rede Operativa de Dados

II.III. Perímetros e Domínios da Segurança

Para melhor identificação dos requisitos e das questões voltadas à segurança cibernética, a Rede Operativa de Dados foi delineada em Perímetros e Domínios de Segurança (HEINISCH & LEITE, 2011, p. 154):

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; Domínios de Segurança associados à Automação de Subestações e Domínios de Segurança associados à Infraestrutura de Medição Avançada de Energia (AMI – *Advanced Metering Infraestructure*). A Figura 2 ilustra o conceito de perímetros e domínios de segurança da ROD.

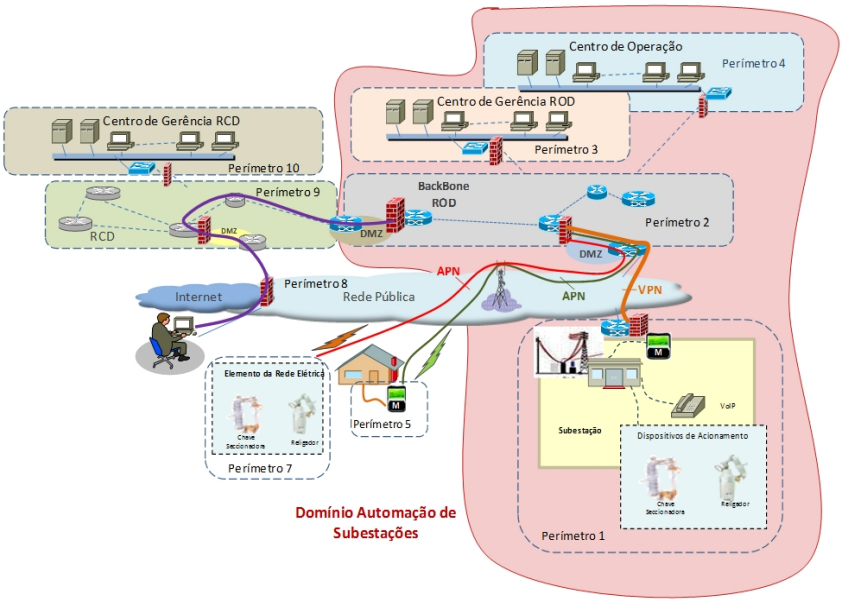

Figura 2: Domínios e Perímetros de Segurança Cibernética

II.IV. 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(BASTOS & CAUBIT, 2010, p. 257). Para a análise do impacto nos processos de automação da CEMIG, 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 necessária na resposta 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 da 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 1 ilustra a análise CIDAL para as funções relacionadas ao domínio de Automação de Subestações elaborada em função das análises dos especialistas.

Tabela 1. 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 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 e a *Tendência* dessa situação, caso nenhuma ação de segurança seja tomada. A Tabela 2 apresenta a análise GUT para as funções relacionadas ao domínio de Automação de Subestações, também com base na análise dos especialistas.

Tabela 2 - Análise GUT – 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 ativos cibernéticos em relação a sua

criticidade. Essa classificação possibilita determinar o nível de relevância 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 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.

III. Aplicativo Supervisor de Perímetro Eletrônico de Segurança - ASPES

III.I. Arquitetura

O aplicativo ASPES é composto por uma base de dados de parâmetros de segurança construída com base em um estudo prévio dos equipamentos que compõem os perímetros eletrônicos de segurança envolvidos nos processos de automação e nas diretrizes de segurança cibernética relacionadas aos processos operativos.

Através de varreduras programadas realizadas em pontos estratégicos da ROD, esse aplicativo é capaz de avaliar os parâmetros de segurança cibernética configurados em ativos cibernéticos cadastrados em sua base de dados e associar um índice de vulnerabilidade aos respectivos ativos, perímetros e domínios eletrônicos de segurança. A contabilização dos diversos índices associados aos ativos cibernéticos possibilita uma avaliação do nível de aderência dos parâmetros de segurança às diretrizes pré-estabelecidas.

O ASPES é composto por quatro componentes básicos: Banco de Dados; Containeres; Coletores e Interface Homem-Máquina. O banco de dados e a Interface Homem-Máquina (IHM) são componentes alocados externamente ao perímetro eletrônico de segurança. Já, os Containeres e Coletores são inseridos em cada perímetro de segurança estabelecido dentro do sistema da concessionária.

As listas de procedimentos de segurança são 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, consequentemente, da ROD.

A identificação das vulnerabilidades depende da inserção dos dados ideais e dos 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.

A IHM, uma interface web, acessa o banco de dados para apresentar ao usuário final o resultado da coleta de parâmetro dos ativos e a análise de vulnerabilidade.

III.II. Funcionamento

O ASPES basicamente se divide em dois módulos operacionais: Gestão e Status. No módulo de gestão são realizados e gerenciados os cadastros de usuários, cadastros de ativos, cadastros de parâmetros de ativos, cadastro de perímetros e cadastro de domínios de segurança. No módulo Status são realizadas as operações de coleta de dados dos ativos cibernéticos e realizado o cálculo de análise de vulnerabilidade dos ativos e dos respectivos domínios de segurança.

A partir da IHM, o usuário configura todos os parâmetros de segurança dos ativos cadastrados. Tais parâmetros são considerados “parâmetros ideais”, isto é, parâmetros cujos valores asseguram a proteção contra ataques cibernéticos daquele ativo. Após uma requisição de coleta, de forma automática ou manual, é realizada uma comparação entre os parâmetros dos ativos coletados e os parâmetros ideais. Caso haja alguma não conformidade em algum parâmetro, o ativo é considerado vulnerável. A soma da vulnerabilidade de cada ativo acarretará na vulnerabilidade total do domínio de segurança, de acordo com a relevância do ativo e da probabilidade de ocorrência da vulnerabilidade.

Essa análise pode ocorrer automaticamente, conforme a periodicidade configurada no ASPES ou sob demanda do usuário, de acordo com a política de segurança de cada empresa. E possível, a partir do ASPES, emitir relatórios com o histórico de todas as coletas e verificar a evolução do índice de vulnerabilidade de cada domínio de segurança.

IV. Teses de Vulnerabilidade em uma Subestação

Os IEDs envolvidos no processo de automação de subestação, bem como os equipamentos de rede de comunicação de dados da ROD foram cadastrados via interface de usuário no ASPES: Relés de Proteção, Medidores, Religadores, IHM de subestação, Switches e Roteadores, todos previamente estudados no âmbito do projeto, do ponto de vista dos parâmetros e diretrizes de segurança cibernética aplicada naquele domínio de segurança eletrônica, e adotados para o desenvolvimento da base de conhecimento do ASPES para permitir que ele execute o cálculo do percentual de vulnerabilidade.

Para os testes em ambiente de subestação, optou-se pela subestação Serra Verde, localizada em Belo Horizonte. Esta indicação se deveu ao fato de a subestação Serra Verde ser equipada com dispositivos IEDs escolhidos para serem suportados na base de conhecimento do software gestor ASPES. Neste cenário, o perímetro de segurança de rede de comunicação é representado pela infraestrutura de comunicação que interliga a subestação escolhida à rede CEMIG e o perímetro de segurança de controle e operação representado pela rede interna da TI da CEMIG Sede, onde se instalou o servidor do ASPES bem como a aplicação cliente do mesmo. A Figura 3 ilustra a configuração adotada para os testes em ambiente de subestação.

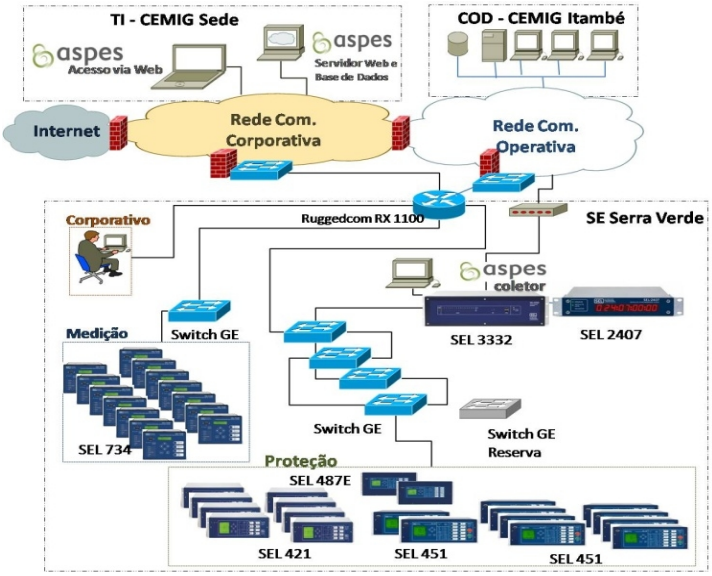

Figura 3: Configuração da Rede - Subestação

Nessa configuração apresentada tem-se a Interface Homem Máquina (acesso via Web), o Banco de Dados e o Servidor Web alocados na Sede da CEMIG, na área de TI; o coletor é alocado na SE Serra Verde

(perímetro de segurança eletrônico que contém os ativos, foco dos testes).

Em um primeiro momento foi feita toda a configuração do sistema: Cadastro de Usuário/Operador, Cadastro de Ativos, Cadastro de Domínios, Cadastro de Perímetros, Cadastro de Parâmetros de Ativos. Em seguida, procedeu-se com os testes aplicados aos domínios de segurança voltados aos processos de automação de subestação contemplados: Domínio de Segurança de Medição; Domínio de Segurança de Proteção e Domínio de Segurança de Serviços Corporativos.

Configurou-se no ASPES os valores esperados (valores ideais) para cada parâmetro em cada tipo de ativo cadastrado, bem como a relevância desses ativos, a severidade e a probabilidade de ocorrência dos parâmetros, executando-se, em seguida, um procedimento de coleta automática para o domínio de segurança, para verificar a compatibilidade da configuração dos ativos com os valores esperados. Os valores esperados tiveram como referência as diretrizes de segurança cibernética trabalhadas no projeto com base nas normas NERC CIP.

Depois de finalizada a coleta, o ASPES apresenta o percentual de vulnerabilidade dos ativos e, consequentemente, do domínio de segurança a que pertencem e ao qual foram atrelados no cadastro que o usuário procedeu previamente. O cálculo do percentual de vulnerabilidade ocorre tomando como base o valor do parâmetro coletado, sua severidade e probabilidade e a relevância do ativo.

Em seguida, alteraram-se parâmetros esperados de forma a certificar a funcionalidade do ASPES diante da variação do percentual de vulnerabilidade em função dos parâmetros de segurança de ativos de subestação. Neste mesmo sentido, alteraram-se os parâmetros de configuração de equipamentos, especificamente do roteador, tornando-o menos vulnerável do ponto de vista de segurança cibernética, solicitando-se em seguida uma nova coleta para o roteador e verificando-se então essa ocorrência. Verificou-se uma redução do percentual de vulnerabilidade no ativo e consequentemente no domínio de segurança de subestação ao qual este ativo estava atrelado.

A Figura 4 ilustra a tela do ASPES no momento da primeira coleta dos parâmetros do roteador e a apresentação do percentual de vulnerabilidade desse ativo. Neste instante o ativo apresentava uma vulnerabilidade de 30%.

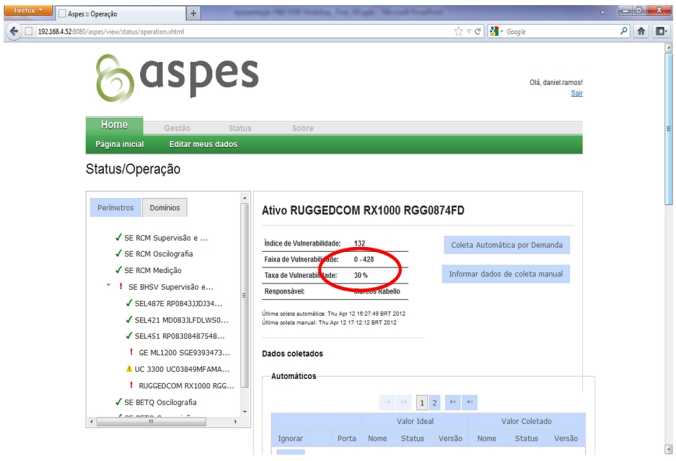

Figura 4: ASPES - Primeira Coleta de Parâmetros

A Figura 5 ilustra a tela do ASPES no momento da segunda coleta dos parâmetros do roteador, depois de alterada a configuração, desabilitando a função *Telnet*. O percentual de vulnerabilidade desse ativo foi reduzido em relação ao estado anterior. Após a alteração do parâmetro, o ativo apresentou uma vulnerabilidade de 28%.

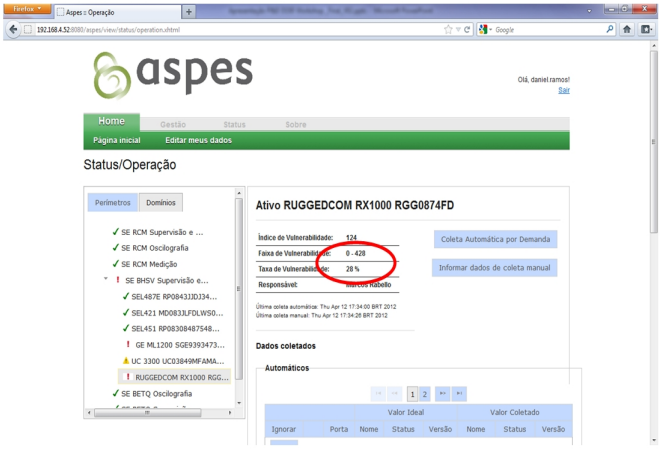

Figura 5: ASPES - Segunda Coleta de Parâmetros

Na subestação Serra Verde, foram executados testes similares verificando o percentual de vulnerabilidade dessa subestação e certificando os impactos da adoção do ASPES nesse ambiente em operação. A execução do ASPES não provocou alteração no funcionamento dos ativos e nem degradou o desempenho da Rede de Comunicação. Embora satisfatório, esse desempenho deve ser avaliado em um teste de larga escala, envolvendo múltiplas subestações.

3. 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. Com base nos testes realizados em laboratório e na subestação de Serra Verde, o aplicativo gestor de segurança cibernética desenvolvido mostrou-se ser uma ferramenta prática para a análise de vulnerabilidade de tais ativos, podendo ser aplicado em todo o ambiente de automação das concessionárias.

4. Referências bibliográficas

[1] MILLAN, R. Siemens: Stuxnet worm hit industrial systems. Computerworld, Septemper 14, 2010, p. 1-3. Acesso em 01/03/2012, disponível em: http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyN
.

[2] GELLINGS, W. The Smart Grid – Enabling Energy Efficiency and Demand Response. Boca Raton, FL,

USA. Taylor & Francis, 2009, p. 300.

[3] METKE, A. R. & ELK, R. L. Security Technology for Smart Grid Networks, IEEE Transaction on Smart Grid, Vol 1. No. 1, June 2010, p. 99-105

[4] FLICK, T. & MOREHOUSE, J. Securing the Smart Grid – Next Generation Power Grid Security. Burlington, MA, USA. Syngress, 2010, 290 p.

[5] NIST - National Institute of Standardas and Technology. Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0. NERC Critical Infrastructure Protection (CIP) standards CIP-001 TO CIP-009- NIST, September, 2009, p. 175.

[6] ANSI - American National Standards Institute. 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, p. 167

[7] HEINISCH, A. & LEITE, L. 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, 2011, p. 154.

[8] HEINISCH, A. & LEITE, L. Especificação Técnica – Rede Operativa de Dados". CEMIG Distribuição. Belo Horizonte, MG, Brasil. Relatório Técnico. RQS-10005-GOP-V01-R01-CMG-CYBSEC-ESPTEC-COMUN-CONECT. Julho, 2010, p. 39.

[9] BASTOS, A. & CAUBIT, R. Gestão de Segurança da Informação – ISO 27001 e 27002 – Uma Visão Prática. Módulo Education Center. Porto Alegre, RS, Brasil, 2010, p. 257