



**XXIV SNPTEE
SEMINÁRIO NACIONAL DE PRODUÇÃO E
TRANSMISSÃO DE ENERGIA ELÉTRICA**

CB/GTL/29

22 a 25 de outubro de 2017
Curitiba - PR

GRUPO - XV

**GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÕES PARA SISTEMAS
ELÉTRICOS – GTL**

**PROPOSTAS PARA MITIGAÇÃO DE INTRUSÃO EM SISTEMAS DE SUPERVISÃO
E CONTROLE NA ÁREA DE TRANSMISSÃO DA CEEE-GT.**

**Fernando Eduardo Covatti (*)
CEEE-GT**

**Vitor Donaduzzi
CEEE-GT**

RESUMO

Neste trabalho, será proposta uma arquitetura segura para o setor de transmissão da CEEE-GT. Esta arquitetura abrangerá a segurança de comunicação a nível de subestação e entre subestações e centros de operação, bem como o acesso e troca de dados entre redes de supervisão e a rede corporativa. Serão previstas metodologias para controle de acesso aos sistemas utilizados nos centros de operação e subestações, minimizando os riscos de intrusão. Também, serão detalhados os equipamentos e ferramentas que poderão ser utilizados no monitoramento e detecção de ataques, tais como Firewalls, Gerenciadores de Rede (Nagios) e de Logs, IDS, protocolos encapsulados em SSH, VPNs e etc. Além disso, serão detalhadas abordagens utilizadas em sistemas de supervisão baseados em Linux, como o SAGE que podem ser empregadas para torná-lo mais seguro. Por outro lado, uma abordagem com relação às experiências e políticas de cibersegurança dentro da empresa, bem como pontos de insegurança que serão sanados, poderá ser relatada.

PALAVRAS-CHAVE

Cibersegurança, mitigação de intrusão, sistemas de supervisão e controle, setor de transmissão

1.0 - INTRODUÇÃO

Sistemas de supervisão e controle (SCADA) e de gerenciamento de energia (EMS) são cruciais para o monitoramento em tempo real e operação de subestações de transmissão de energia. Com o advento de soluções utilizando redes Ethernet/IP em ampla escala nos sistemas do setor elétrico, tais como protocolos da norma IEC 61850, IEC 61850, DNP3 e IEC104, é vital que se utilizem arquiteturas seguras de modo a prevenir que tais sistemas sejam acessados por usuários não autorizados, internos ou externos à empresa ficando desta forma vulneráveis a ataques cibernéticos.

Além disso, os protocolos SCADA em geral, foram desenvolvidos sem preocupações de cibersegurança e as políticas de segurança da área de Tecnologia da Informação nem sempre consideram as características de tais sistemas.

Devido às ameaças reais, como por exemplo o caso de um ciberataque que desligou companhias de energia da Ucrânia [1], e um esforço grande de agências governamentais para proteger os sistemas de infraestrutura crítica (ICS), se verificou a necessidade de rever a arquitetura de rede e a segurança dos sistemas supervisórios na área de transmissão da CEEE-GT. Com isso, um trabalho de monitoramento de equipamentos, segmentação e modificação de arquiteturas de rede, instalação de sistemas de detecção de intrusão (IDS), implantação de políticas de segurança e uma mudança cultural na empresa se mostrou extremamente necessária.

(*) Av. Joaquim Porto Villanova, 201 – Predio F – Sala 207 – Jardim Carvalho – Porto Alegre – CEP: 91410-40, RS, – Brasil Tel: (+55 51) 33822382 – Email: fernando.covatti@ceee.com.br

2.0 - FALHAS DE SEGURANÇA COMUNS A EMPRESAS DO SETOR ELÉTRICO

2.1 Visão Geral do Setor Elétrico

No caso do sistema elétrico brasileiro [2], onde existe um regime baseado nas concessões, os vencedores de determinados leilões adquirem o direito de instalação, manutenção e operação de parte do sistema. Logo, diversas empresas existam e participem do setor elétrico. Essa divisão origina regiões de fronteira, onde por exemplo, partes de uma subestação de energia pertençam a empresas distintas. Um exemplo simples de fronteiras pode ser dado através de uma linha que chega na subestação pertencente a uma empresa, as baixas tensões a uma outra e o transformador a uma terceira. A Figura 1.1 ilustra como podem existir diversos participantes no setor e as diversas fronteiras que eles possuem.

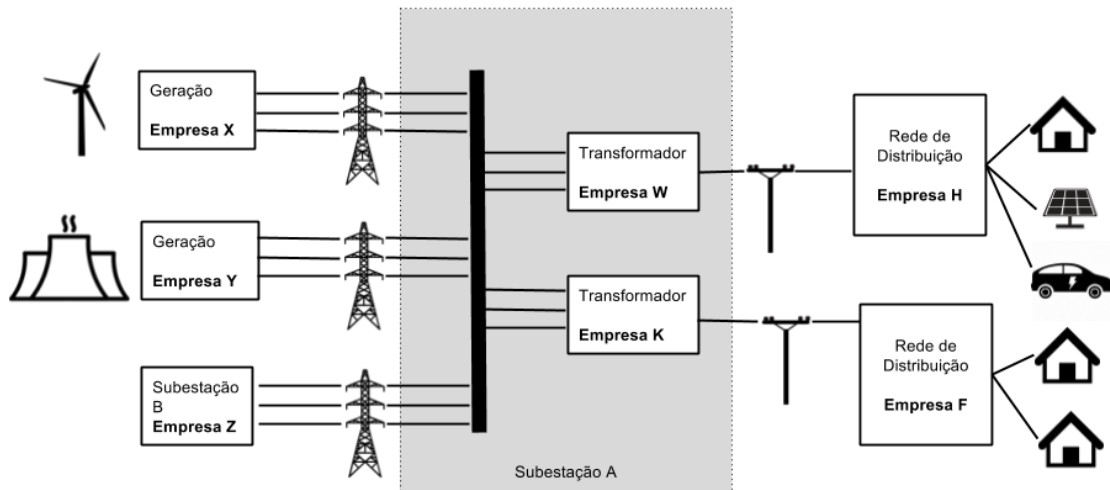


FIGURA 2.1: Diagrama simplificado das fronteiras entre empresas do setor elétrico

2.2 Sistemas de Supervisão e Controle

Apesar das diversas empresas que podem estar presentes no setor elétrico, cada uma delas é responsável pelos seus sistemas de supervisão e controle. A Figura 2.2, mostra um diagrama simplificado com a relação de alguns dispositivos que compõe o sistema bem como suas interligações de comunicação. No caso de empresas distintas que compartilham por exemplo, uma mesma subestação, os sistemas de supervisão e controle (SCADA e IEDs) se encontram nas imediações da subestação em casas de controles separadas, porém interconectadas por fibras ópticas. Logo há comunicação entre IEDs para proteção dos equipamentos da subestação. Entre sistemas SCADA para demais informações, como medições de potência e estado de outros dispositivos. E por fim, até mesmo entre sistemas EMS das diversas empresas do setor de forma a se ampliar a visibilidade do sistema elétrico e facilitar a operação do mesmo. Fora essas comunicações, também existem IHMs (suprimidas da imagem) que se comunicam com o sistema SCADA da Subestação e servem para visualização do estados dos dispositivos em diagramas unificares, bem como operação local em painéis em caso de falha de comunicação com os centros de operação.

Os IEDs que compõem esses sistemas de supervisão e controle necessitam trocar informações em tempo real numa mesma subestação de forma a garantir que uma falha física em um dispositivo, por exemplo em uma linha de transmissão, não cause um distúrbio no resto do sistema, por exemplo nas demais linhas. Além disso, dependendo do tipo de falha, podem se causar problemas de dimensões maiores ao Sistema Interligado Nacional (SIN), deixando regiões sem energia elétrica.

Para os sistemas SCADA, é necessário a troca de informações de maneira a se saber se por exemplo, todos equipamentos da subestação estão energizados ou não, para que se possa efetuar uma manutenção local. Além disso, no caso de ocorrência de uma falha elétrica, o sistema SCADA recebe todos os eventos dos IEDs e envia ao centro de operação de maneira que os operadores possam tomar uma decisão de executar algum comando remotamente ou mesmo enviar uma equipe de manutenção para averiguar a falha.

Já a troca de informações entre sistemas EMS amplia a visibilidade de uma concessionária e facilita a operação de maneira que se possa saber se uma determinada região possui uma maior carga e também se uma outra área não apresenta problemas após uma ocorrência de falha. Além disso, além das informações obtidas através dos sistemas SCADA presentes nas subestações da empresa, se pode utilizar dados de outras empresas para se estimar o estado dos dispositivos operados dentro da sua área de concessão.

Por fim, há também um envio de informações das empresas para o Operador Nacional do Sistema (NOS) [3], que é o responsável final por manter o SIN funcionando e orientar a operação das empresas do setor.

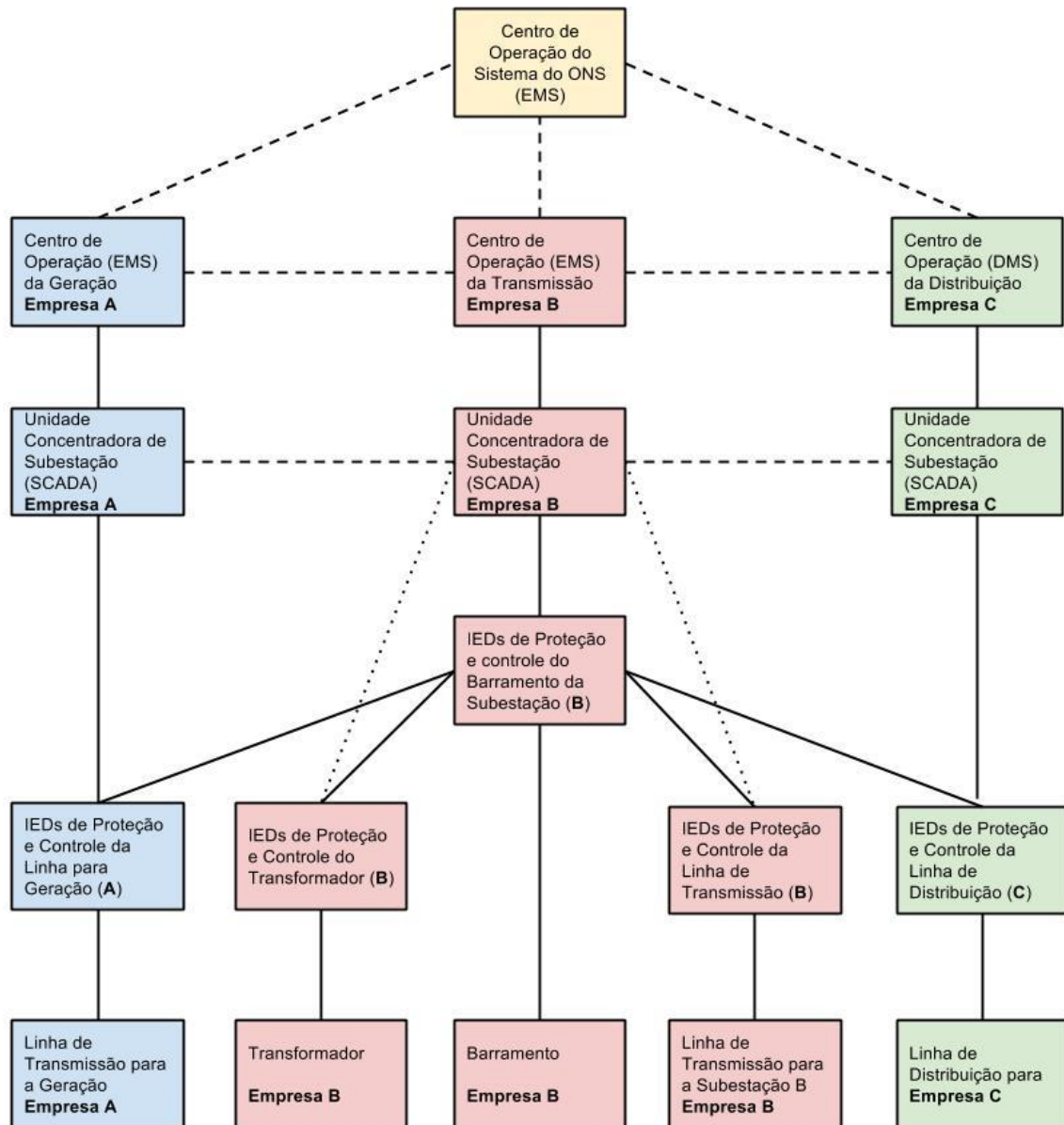


FIGURA 2.2: Diagrama simplificado de comunicação de diversas empresas

Essa grande quantidade de fronteiras e o grande número de concessionárias no setor elétrico brasileiro contribui para as preocupações com cibersegurança. Mesmo em outros sistemas elétricos, como o europeu, americano e de demais países sempre há regiões de fronteira onde essa troca de informações pode ocorrer.

2.3 Falhas de segurança em sistemas de supervisão e controle

Proteger as fronteiras de invasões ao sistema local utilizando ferramentas de detecção internas ou com troca de informações entre empresas de maneira segura é um princípio básico de segurança e algo necessário de ser realizado. Por mais que essa troca de informações seja normalmente segura, ainda existe a possibilidade de que informações trocadas entre os diversos equipamentos seja corrompida, como por exemplo através de ataque de *Man-in-the Middle*. Ademais, os equipamentos de telecomunicações utilizados para a troca de informações entre subestações e centros de operação, por vezes utiliza caminhos ou sistemas compartilhados por outras empresas do setor elétrico, ou mesmo do ramo de telecomunicações.

Já dentro de cada empresa, o uso de acesso remoto aos equipamentos pode também abrir brechas por onde um atacante possa afetar os sistemas. Além disso, sempre existe uma troca de informações entre os sistemas EMS/SCADA e a rede corporativa. É necessário um envio de informações dos sistemas para fins de histórico, análise de ocorrências, gerenciamento de carga entre outros. Porém, essa troca de informações deve ser feita sempre de maneira a não expor o sistema de tempo-real aos mesmos riscos dos sistema de TI utilizado pelos demais funcionários, minimizando assim a exposição a atacantes.

3.0 - ARQUITETURA PROPOSTA

A Figura 3.1 demonstra a arquitetura proposta para uso na CEEE-GT, considerando os sistemas legados existentes e arquitetura de centros utilizada pela operação. A parte dos sistemas de telecomunicação, como switches e multiplexadores que interligam centros de operação e subestações foi omitida para simplificação. As partes hachuradas se encontram em outras localidades, distantes da sede da empresa. As partes em verde são pertencentes a empresa e em vermelho de outras empresas.

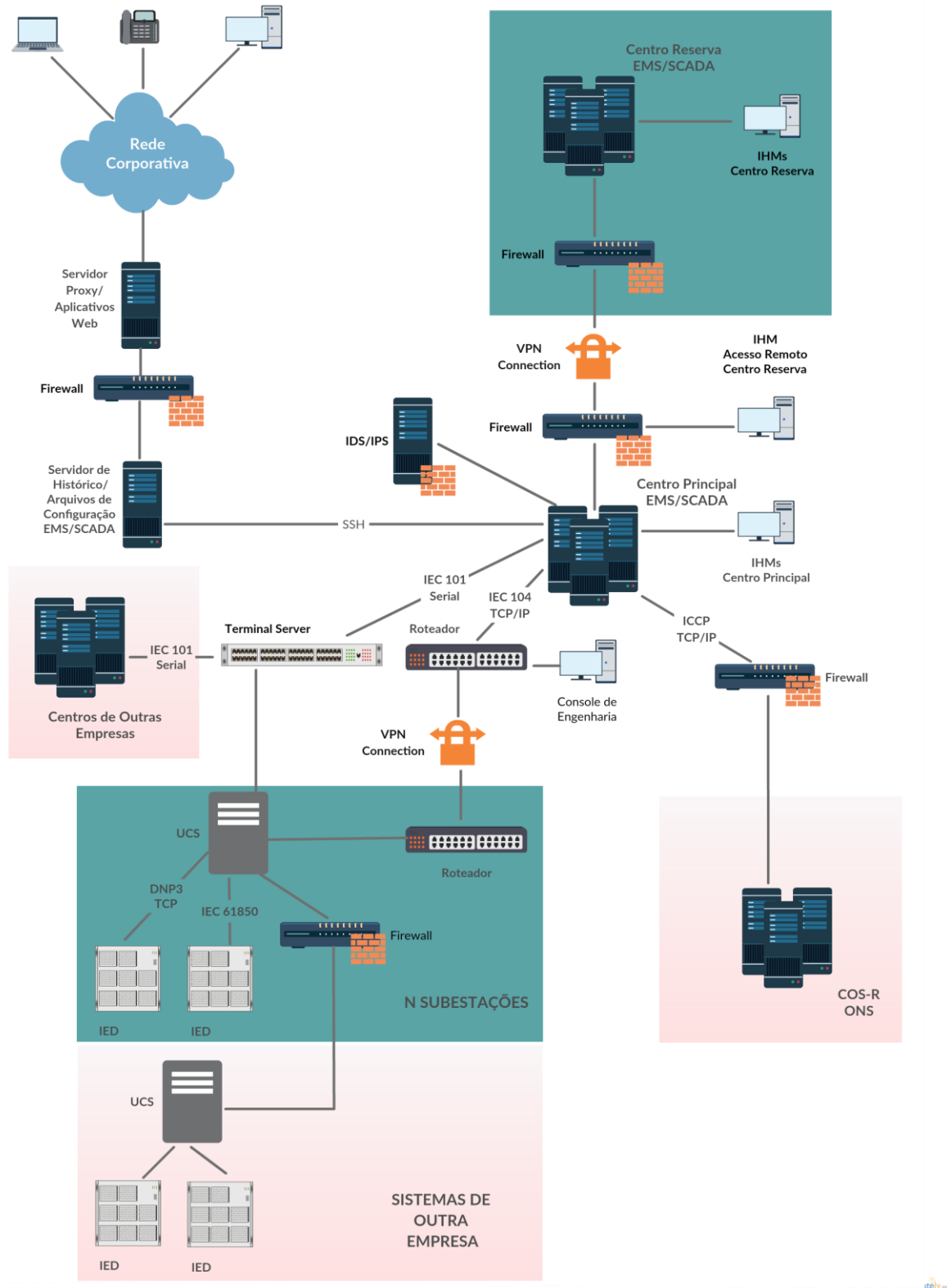


FIGURA 3.1: Arquitetura proposta para CEEE-GT

4.0 - METODOLOGIA DE SEGURANÇA E IMPLANTAÇÃO

Além de uma arquitetura segura, políticas de segurança são necessárias para que se mantenha o sistema seguro. O processo utilizado para implantar uma metodologia de segurança, bem como da arquitetura proposta foi dividido em 3 etapas. Dessa forma, atacando primeiramente as falhas de segurança mais simples de resolução.

4.1 Curto Prazo (1 a 2 anos)

- Mapeamento de vulnerabilidades de rede
- Segmentação de redes
 - Isolamento de rede de acesso remoto a equipamentos dos centros de operação e de subestações
 - Isolamento de Terminais Servers (IEC 101 serial) da rede de subestações.
 - Isolamento de rede de envio de dados ao ONS que era compartilhada com a de subestações
- Monitoração de estado de rede de dispositivos através do NAGIOS
- Instalação de firewall entre Centro Principal e Centro reserva visando proteção em caso de ataque cibernético a um deles.
- Planejamento de atividades a serem implementadas visando mitigar demais vulnerabilidades

4.1 Médio Prazo (2 a 5 anos)

- Alteração de Senhas para mais robustas
- Uso de VPNs entre Centros e Subestações
- Uso de SSH para comunicação com Terminais Servers
- Regras restritas para comunicação 101/104/ICCP nas portas no EMS/SCADA SAGE dos Centros de Operação através do iptables.
- Restrição de permissões para máquinas com chaves SSH primárias que acessam o SAGE
- Separação de equipamentos presentes na rede corporativa e rede de supervisão e controle com o uso de proxys.
- Instalação de firewalls para restrição de tráfego em todas redes.
- Servidor de Logs de tráfego para análise de ocorrências cibernéticas
- Instalação de um IDS/IPS que trabalhe em conjunto com o SAGE (Ex: Snort)
- Utilização de dispositivos de armazenamento de dados seguros

4.1 Longo Prazo (mais de 5 anos)

- Plano de incidência de ataque cibernético
- Política de senhas uniforme para demais áreas das Engenharias
- Diodo de dados entre rede corporativa e rede de supervisão e controle
- Auditoria Externa
- Migração para solução IEC 104 com TLS ou protocolos mais seguros disponibilizados no setor.

5.0 - CONCLUSÃO

Muitas vezes a segurança cibernética acaba ficando em segundo plano no setor elétrico, uma vez que, por se tratarem de sistemas críticos, a disponibilidade do sistema acaba sendo mais importante. Além disso, obras de expansão e a manutenção dos sistemas existentes são tarefas que acabam recebendo mais importância por trazerem retorno financeiro no curto prazo para as empresas.

Porém, com esse trabalho, foram detalhados os pontos vulneráveis que podem surgir na troca de dados entre os equipamentos devido as diversas fronteiras que os sistemas de supervisão e controle possuem. Com base nisso, foi proposta uma arquitetura segura e montado um plano com propostas para mitigar a intrusão dos sistemas de supervisão.

Vale destacar que existiam diversos pontos de vulnerabilidade na rede existente da empresa antes da preocupação com cibersegurança ser iniciada. Logo, foi montado um plano para sanar essas vulnerabilidades, que apesar de ter um prazo longo de adequação, consegue conciliar as demais demandas e ser cumprido de maneira gradual. Essa gradualidade de implantação também é favorável no sentido de acompanhar o desenvolvimento e maturação das tecnologias de segurança do setor.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

[1] LEE, Robert M.; ASSANTE, Michael J.; CONWAY, Tim. Analysis of the cyber attack on the Ukrainian power grid. **SANS Industrial Control Systems**, 2016.

[2] ABRAADE, Visão Geral do Setor Elétrico, Disponível em <http://www.abradee.com.br/setor-eletrico/visao-geral-do-setor> , acessado em 07/02/2017

[3] ONS, O que é o Sistema Integrado Nacional, Disponível em: http://www.ons.org.br/conheca_sistema/o_que_e_sin.aspx , Acessado em 02/03/2017.

[4] GRAINGER, J. **Power System Analysis**, McGraw-HILL, Inc , 1994.

[5] CASWELL, Jayne. Survey of Industrial Control Systems Security. **Washington University in St. Louis, St. Louis, Missouri**, 2011.

[6] STOUFFER, Keith; FALCO, Joe; SCARFONE, Karen. Guide to industrial control systems (ICS) security. **NIST special publication**, v. 800, n. 82, p. 16-16, 2011.

7.0 - DADOS BIOGRÁFICOS



Fernando Eduardo Covatti, Meng.

Nascimento: Sarandi – RS, 1984

Graduação em Engenharia Elétrica – UFRGS – Porto Alegre, 2007.

Mestrado em Automação e Controle – UFRGS – Porto Alegre, 2014.

Trabalha na CEEE-GT, na área de Engenharia de Supervisão desde 2011.

Áreas de atuação: Sistemas SCADA/EMS, Gestão de Redes de Supervisão e Controle, Monitoramento de dispositivos, Segurança Cibernética, Análise e Desenvolvimento de Protocolos de Comunicação, Administração de Sistemas Linux,



Vítor Donaduzzi, Eng.

Nascimento: Santa Maria – RS, 1984

Graduação em Engenharia Elétrica – PUCRS – Porto Alegre, 2013.

Trabalha na CEEE-GT, na área de Engenharia de Supervisão desde 2006.

Áreas de atuação: Sistemas SCADA/EMS, Interfaces IHM para controle local e remoto de subestações, Segurança Cibernética, historiadores de dados, aplicações web, sistemas de treinamentos para operadores.