



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

CB/GTL/26

22 a 25 de outubro de 2017
Curitiba - PR

GRUPO -XV

**GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS
ELÉTRICOS- GTL**

SEGURANÇA DE DADOS NAS REDES DE AUTOMAÇÃO EM SUBESTAÇÕES NA CHESF

Pedro Leon B. Gomes.(*) **Marcos D Guimarães.** **Marcelo M. Rodrigues Leite.** **Ronaldo D. da Silva**
CHESF **CHESF** **CHESF** **CHESF**

RESUMO

O sistema de supervisão da CHESF compõem-se de uma grande variedade de diferentes dispositivos que aquisitam e transmitem dados de equipamentos em subestações, tornando-os acessíveis pelos operadores do sistema, seja nas próprias subestações (supervisão em N2) ou nos Centros Regionais de Operação (supervisão em N3); os quais estão localizados em diferentes capitais dos estados da região nordeste do país. Para viabilizar este sistema faz-se necessária uma vasta rede de transmissão de dados com grande diversidade de tecnologias. Com o passar dos anos, surgiu naturalmente a necessidade de buscar alguma segurança na atuação dos diversos agentes envolvidos na manutenção dos equipamentos de operação conectados nestas redes. O trabalho mostra a experiência da CHESF na implantação de uma arquitetura de segurança no acesso aos equipamentos das redes Scada localizados nas subestações na CHESF.

PALAVRAS-CHAVE

Sistemas Scada, Infraestrutura Crítica, Defesa em Profundidade, Redes de Automação, Defesa Cibernética

1.0 - INTRODUÇÃO

A necessidade de se tentar implantar segurança dos procedimentos que exigem acesso remoto via rede ethernet às máquinas que compõem o sistema SCADA teve basicamente duas motivações:

- a. A necessidade de alterar a tecnologia de distribuição de distribuição dos dados entre N2 e N3 de supervisão, de comunicação serial com modem para rede TCP/IP;
- b. O crescente aumento do número de acessos remotos realizados para máquinas do supervisório em subestações.

Além destes, recentemente tem-se feito um grande esforço dentro das empresas que operam estruturas classificadas com infraestrutura críticas, no sentido de tornar mais seguros o seus sistemas conectados em rede. Sendo geradora e transmissora de energia, a CHESF se enquadra dentro deste grupo.

O acesso remoto para manutenção das máquinas do sistema Scada utilizando a infraestrutura de rede ethernet era feita apenas por poucas equipes e por um número limitado de pessoas. Com a necessidade de se agilizar o atendimento, obtenção mais rápida de informações, reduzir custos com deslocamento, etc; cada vez mais funcionários envolvidos na manutenção dos sistemas de supervisão e controle das subestações passaram a acessar remotamente estas máquinas, representando um risco crescente de segurança. Além disso, a tecnologia de distribuição de dados entre N2 e N3 de supervisão, via canal serial com modem se tornou limitada em recursos de gerenciamento, frente às opções da rede ethernet. Além disso os modems usados pararam de ser fabricados e

(*) Rua 15 de Março nº 50, Bloco B – sala B 201- Anexo 2 – Bongi. CEP 50.761-070 Recife, PE, – Brasil
Tel: (+55 81) 3229-4225 – Fax: (+55 81) 3229-4315 – Email: pedrolg@chesf.gov.br

estava cada vez mais difícil de achá-los no mercado.

Havia ainda o problema de que muitas vezes os equipamentos (modem, terminais-server, canais serial) que compõem a rede serial com a redundância de dois canais, apresentava defeito em algum dos seus componentes e só se detectava este problema na hora em que era necessário usar a suposta redundância do canal secundário.

A idéia de passar para TCP-IP veio também como um forma de se retirar os pontos de falha entre os servidores sistema Scada em N2 e o ponto de entrega na rede de distribuição dos dados, uma vez que, com a mudança, passa-se a ter apenas um cabo ligando a placa de rede do servidor e o porta do switch. A partir dali teria-se uma rede ethernet com a redundância padrão fornecida pelos protocolos de roteamento convencionais e pela infraestrutura de rede.

Esta alteração na distribuição dos dados Scada entre N2 e N3 levou naturalmente a vários questionamentos relacionados com segurança:

- a. Muitos locais que não possuíam acesso remoto para manutenção passariam a ter acesso fácil pela rede para qualquer um dentro na rede interna da empresa;
- b. Quanto aos dados que trafegam pela rede, haveria o risco de ocorrer perda dos pacotes por limitação da capacidade de transmissão dos dados. Qual a necessidade de banda para estes tráfego?
- c. Existe uma politica de definição e atualização de senhas para acesso às máquinas?
- d. De que forma isto vai impactar na atuação das equipes de manutenção?

Baseando-se nestes tópicos e na infraestrutura disponível, o que pode ser feito para viabilizar esta mudança de arquitetura?

2.0 - METODOLOGIA

Neste ponto decidiu-se por abordar o problema da segurança usando o que havia disponível na infraestrutura de rede das subestações, somando-se a isto outras medidas que dificultassem tentativas de acesso aos equipamentos da rede Scada através da rede ethernet. Esta junção de recursos que visam mitigar acessos ou ataques à rede, se encaixa dentro da filosofia de segurança conhecida por defesa em profundidade (1). O que se buscou então foi acrescentar algumas ferramentas que não existiam e melhorar algumas já utilizadas.

3.0 - FERRAMENTAS IMPLEMENTADAS

3.1 - Hardening

O sistema operacional vem com alguns aplicativos que podem representar pontos de falha de segurança, como por exemplo protocolos de acesso remoto sem criptografia, que é o caso do serviço *telnet*, e no caso de serviços de transferência de arquivos, o *ftp*. Outros exemplos são o *nfs*, e o WebServer *Apache*. Estes serviços e outros podem ser desativados desde que se verifiquem as dependências de outros recursos com relação a estes serviços. Por exemplo, o cliente telnet ainda é necessário nas máquinas do N2, pois muitos IEDs são instalados com acesso via linha de comando pelo *telnet*, necessitando que o cliente esteja funcionando localmente nestas máquinas. Mesmo assim, o serviço do servidor, que permite acesso às próprias máquinas do N2 pode ser desativado ou desinstalado.

Outra medida importante mas nem sempre simples de relizar é a atualização do sistema operacional nas máquinas onde o supervísório se hospeda. Novos releases trazem melhorias de segurança na medida em que retiram as falha de pacotes em versões antigas. Muitas das falhas presentes em uma determinada versão do sistema operacional são de conhecimento público e representam riscos ao sistema.

3.2 - Controle de Senhas

A filosofia se usar senhas para permitir acesso às máquinas sempre foi praticada na empresa. O melhoramento se deu pelo desenvolvimento de uma ferramenta que realiza a troca das senhas remotamente, com periodicidade definida pelos mantenedores. O sistema mantém ainda um banco de dados com registros de trocas e falhas de comunicação eventualmetne registradas. A ferramenta acessa as máquinas localizadas em subestações e em centros regionais de operação e atualiza as senhas de acesso, informando os mantenedores e os interessados sobre as alterações. O nível de complexidade das senhas pode ser alterado pela quantidade de caracteres que se deseja utilizar, uso de letras maiúsculas ou minúsculas e metacaracteres.

O serviço fica hospedado em um servidor de aplicação conforme a ilustração na Figura 1.

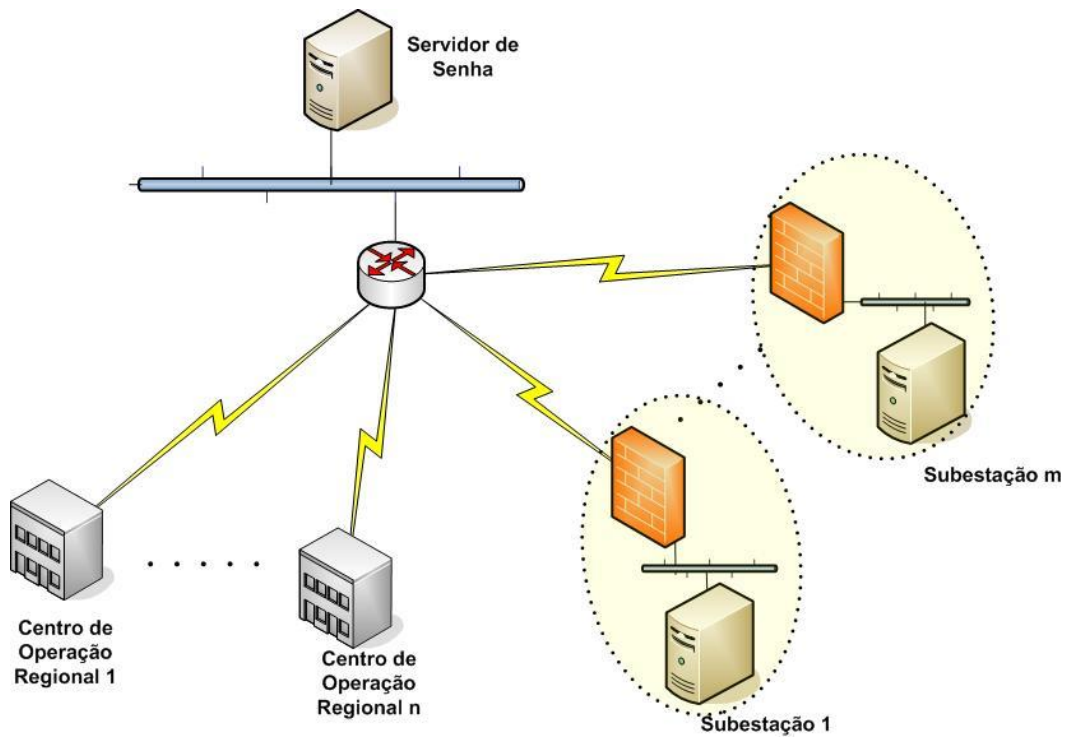


FIGURA 1 – Mudança de senhas

3.2 - Definição de parâmetros de rede

3.2.1 - Definição de Banda Necessária para Tráfego das Informações

A distribuição dos dados dentro da rede ethernet da empresa trouxe a preocupação quanto à possibilidade de aumento excessivo do tráfego, com risco de ocorrerem picos de ocupação da banda durante ocorrências no sistema elétrico, principalmente em trechos da rede onde há limitação de recursos com links de menor capacidade. Para ter idéia do que seria necessário dispor de recursos de forma a viabilizar o trabalho, foi feita uma simulação de tráfego com monitoramento de uma distribuição de dados de uma máquina em um sistema Scada em uma subestação específica (rodando a mesma base de dados instalada em uma máquina real), para uma aquisição em um centro regional. Os testes simularam situações de tráfego moderado e situações de avalanche de dados com geração de várias sinalizações e variações de medições ao mesmo tempo. Nesta simulação foi usada a ferramenta sim-tr do Sage. A montagem usada nos testes está ilustrada na Figura 2.

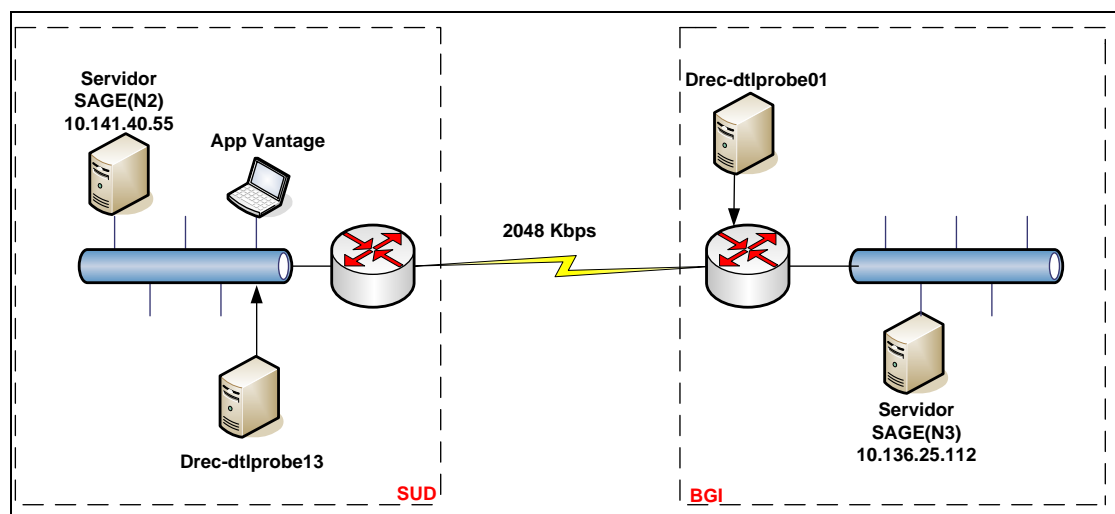


FIGURA 2 – Estrutura dos Testes

A distribuição dos dados foi feita em DNP3 sob TCP-IP. O link de conexão com a subestação era de 2048 Kbps na época dos testes. Como resultado a utilização média da banda foi de 8,5 Kbps (2).

3.2.2 - Priorização dos Pacotes de Sistema de Supervisão

Devido a importância do tráfego dos dados da supervisão em tempo real com relação aos outros dados que possam estar trafegando na rede decidiu-se utilizar o QoS (Quality of Service) para priorizar os pacotes provenientes do sistema Scada das subestações. Foi implementada a marcação dos pacotes provenientes dos servidores em N2, com um valor DSCP específico, de forma que os equipamentos de rede podem dar o tratamento diferenciado a estes pacotes.

Uma vez que o sistema supervisório predominante nos níveis N2 e N3 da CHESF é o Sage, esta funcionalidade de marcação dos pacotes no próprio sistema supervisório foi solicitada ao CEPEL, que prontamente disponibilizou o recurso em um update do SAGE.

3.3 - Restrição do Acesso a Redes Específicas

Muitas manutenções e coletas de dados são feitas pela rede acessando-se as máquinas remotamente, seja nos centros regionais ou em subestações. Como forma de reduzir os acessos realizados remotamente às máquinas do tempo real, decidiu-se restringir estes acessos com base nas redes de origem do IP acessante. Pela divisão dos IPs internos da empresa foi possível determinar quais redes são as nativas das equipes de manutenção e de acordo com a responsabilidade da manutenção de cada subestação, seleciona-se quais equipes podem acessar uma determinada subestação ou não.

Esta restrição de acesso busca evitar os acessos por indivíduos de equipes não autorizadas a trabalhar nestas máquinas e também desencorajar indivíduos mal intencionados a buscar acesso.

A arquitetura seguida busca também isolar todas as máquinas envolvidas na supervisão do tempo real, permitindo acesso apenas àquelas que trocam dados de tempo real entre si. Outras máquinas que funcionam, por exemplo, como terminal de visualização de telas, não são acessíveis pela rede. A Figura 3 ilustra a configuração seguida.

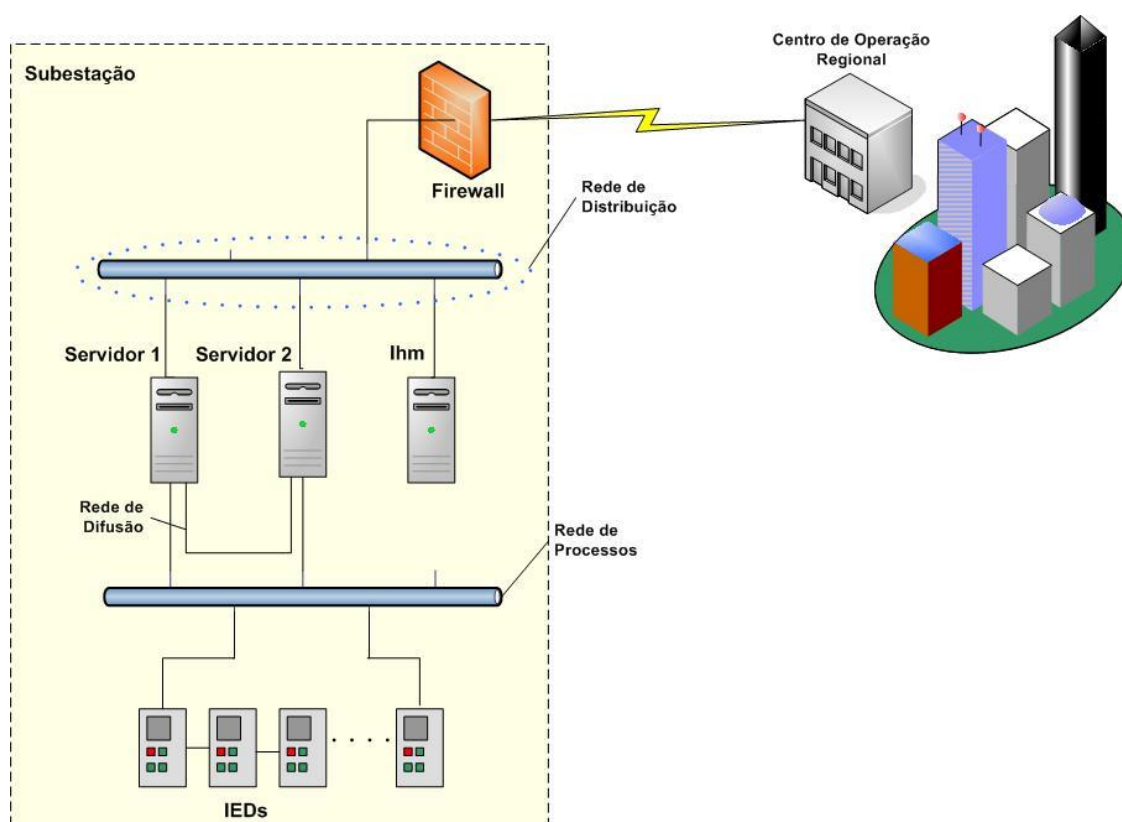


FIGURA 3 – Arquitetura da SE

4.0 - RESULTADOS

A implantação da arquitetura gerou resultados bem rápidos em termos de identificação de usuários e redução de acessos. Os resultados mais imediatos estão listados abaixo:

- a. Por meio dos logs do sistema já pode-se verificar uma redução dos acessos remotos em algumas localidades;
- b. Foi possível também ter uma ideia mais detalhada de quais pessoas acessam quais locais e os motivos, pois estas passaram a reclamar o acesso que antes possuíam. Alguns destes acessos eram feitos para obter informações que poderiam ser obtidas por outros meios, tais como ferramentas especialmente desenvolvidas para isso, que acessam dados do sistema supervisório, seja nos próprios servidores ou em bancos de dados históricos;
- c. Com a distribuição dos dados em TCP-IP trouxe a necessidade de escrever novos normativos de manutenção para as equipes envolvidas nesta atividade, no sentido de como proceder com os novos equipamentos de rede;
- d. Com a segurança em rede, que fortaleceu a ideia de mudar a distribuição dos dados entre N2 e N3 para protocolo DNP3.0 em TCP-IP, houve significativa redução de quedas de comunicação em algumas subestações que historicamente apresentavam alto índice de quedas de comunicação, seja por defeitos nos equipamentos (modems, terminais-server, etc) seja por outros motivos que ficavam indeterminados;
- e. Com esta alteração também houve uma melhora significativa no monitoramento da comunicação entre os níveis N2 e N3 por simples checagem do links. Além disso, uma vez que todos os equipamentos envolvidos estão conectados na rede ethernet, todos eles podem ser monitorados via SNMP no próprio supervisório da subestação.

Portanto vê-se que os resultados da implantação da segurança foram diretos e indiretos, uma vez que possibilitaram a continuidade de outros trabalhos que eram postergados por se achar que haveria muita exposição do sistema Scada na rede.

5.0 - CONCLUSÕES

A preocupação e as ações tomadas no sentido de tornar o sistema Scada mais seguro vieram em parte de uma reação a outros problemas, tendo sido posta em prática de uma maneira que não foi a mais correta. Mas o que se obteve até o momento foi um início de um trabalho que terá continuidade. Mesmo assim, nas atividades do dia a dia, nota-se um acréscimo de dificuldade por parte de alguns setores em acessar máquinas em subestações, gerando reclamações. Essa é uma das consequências deste tipo de trabalho, e foi um importante resultado, pois evidenciou um problema grande que não se esperava antes da implantação, pois até ser apenas uma proposta, as restrições de acesso eram vistas como sendo algo que viria naturalmente. A realidade mostrou-se diferente.

A ideia é que haja essa dificuldade ou mesmo o completo impedimento para funcionários de dentro da empresa sim, mas que os procedimentos se adaptem, permitindo que eles ainda tenham acesso às informações que forem necessárias. É uma questão de mudança de mentalidade do corpo de funcionários por uma necessidade da empresa. Essa dificuldade atuará de forma semelhante em indivíduos que queiram deliberadamente gerar danos ao sistema.

O que se implantou até o momento foi pouco frente as opções e obrigações disponíveis na literatura. Mas esse pouco já incrementa a segurança do sistema que se encontrava completamente desprotegido.

Outro benefício importante foi que este passo trouxe confiança para seguir-se em frente com outros trabalhos que, mesmo não sendo diretamente relacionados com segurança, sofriam pela falta desta.

6.0 - TRABALHOS FUTUROS

Os próximos passos para melhorar a segurança são o acréscimo de outros itens que devem estar presentes em um sistema de segurança bem implementado, a saber:

- a. Sistema de detecção de intrusão;
- b. Medidas de reação em casos de ataques cibernéticos reais;
- c. Indicação de procedimentos que ajudem a identificar danos provenientes destes ataques;
- d. Como recompor o sistema de maneira mais rápida;
- e. Capacitação dos funcionários;
- f. Investimento em segurança física (engenharia social);

Muito do que se faz no âmbito da manutenção vem de uma necessidade que normalmente tem certo grau de

urgência. Percebe-se que este procedimento prejudica em alguma medida os resultados de alguns trabalhos. Para implementação de um sistema deste tipo seria necessário preparação do corpo de funcionários e planejamento das etapas de implantação de forma que os itens acima sejam cumpridos adequadamente.

7.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) Souza, P. A., Kiefer, A., Santos, C., Videira, E., Branquinho, M. Cyber Security para Sistema de Automação de Energia – Como a Defesa em Profundidade Pode Aumentar a Segurança Cibernética em Instalações Críticas. Eletroevolução, Dezembro de 2015.
- (2) Divisão de Operação e Gerenciamento de Recursos de Telecomunicações. Relatório de Análise de Tráfego. Novembro de 2014.

8.0 - DADOS BIOGRÁFICOS



Pedro Leon Barbosa Gomes nasceu em Recife- PE em 24 de Abril de 1979. Graduiu-se em Engenharia eletrônica pela UFPE em 2003, concluiu Mestrado em Engenharia de Produção na UFPE em 2006, possui Especialização em Engenharia de Software pela UPE-POLI concluído em 2015. Trabalhou no SENAI como professor em 2005 e na UFRPE também como professor de 2004 a 2006. Atualmente trabalha na CHESF como engenheiro realizando manutenção nos equipamentos da rede de automação e melhorias nos serviços do sistema supervisão e controle, em subestações e centros regionais de operação.

Marcos Dantas Guimaraes nasceu em 17 de janeiro de 1965 em Brasília/DF. É engenheiro Eletrônico formado pela Universidade Federal da Paraíba (UFPB) - Campus II (em Campina Grande/PB, atual UFCG). Fez Curso de Especialização em Redes de Dados em 1997 pela UFPB (Campus I - João Pessoa). Trabalhou entre 1996 e 2001 como Engenheiro de Telecomunicações na TELPA - Telecomunicações da Paraíba S/A. Atualmente trabalha como Engenheiro Eletrônico na CHESF (Companhia HidroElétrica do São Francisco) desde 2006 na área de automação industrial, administrando e fazendo manutenção do SAGE (Sistema Aberto de Gerência de Energia) do CEPEL. Trabalha, também, com manutenção dos servidores e IHMs de toda a planta da CHESF, manutenção de sistemas VideoWall e é responsável pela manutenção do sincronismo de tempo do sistema SAGE.

Marcelo Marcos Rodrigues Leite, nascido em Arcoverde, PE, em 03 de junho de 1959. Analista de Sistemas, formado em Ciência da Computação (1984) pela Universidade Federal de Pernambuco; Com pós-graduação em Geoprocessamento (2011) pela Universidade Estadual da Paraíba, UEPB, PB; Tem trabalho apresentado no XX SNPTEE com o artigo "PROTOCOLO DE COMUNICAÇÃO TASE.2/ICCP – UMA INEVITÁVEL EVOLUÇÃO NA COMUNICAÇÃO ENTRE CENTROS DE CONTROLE DE GRANDE PORTE: A EXPERIÊNCIA NA CHESF"; Trabalha na Companhia Hidro Elétrica do São Francisco – CHESF, desde 1987, atuando na área de Suporte Tecnológico de Automação, principalmente em Banco de Dados para ambientes de Tempo Real e instalação e manutenção de Redes e Protocolos de Comunicação para Sistemas Supervisórios.

Ronaldo Dantas da Silva nasceu em Recife-PE em 01/12/1966. Formado como Técnico em Telecomunicações no ETFPE 1984. Graduado em Engenharia Eletrônica pela UPE-POLI em 1997. Atualmente é Engenheiro da Divisão de Operação e Manutenção de Telecomunicações na CHESF.