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

Gustavo C. Merighi
Empresa Energética do Mato Grosso do Sul S.A.
gustavo.merighi@enersul.com.br

Estrategia de Seguranca na Rede de Dados do Sistema SCADA.

Palavras-chave

SCADA
informa?es
opera??o
protocolo
rede
seguran?a

Resumo

Este trabalho tem como objetivo destacar a importância da segurança da rede de dados no ambiente SCADA que utilizam o protocolo de comunicação TCP/IP (Transport Controle Protocol/Internet Protocol), de forma a sugerir algumas diretrizes as demais concessionárias do setor elétrico presentes neste Seminário, com o fim de evitar falhas no ambiente SCADA e garantir a disponibilidade da operação do sistema elétrico. A Enersul esta em fase de implementação de procedimentos e políticas de segurança na rede operativa em virtude da necessidade da interação com redes menos seguras. O sistema SCADA precisa compartilhar informações com outras áreas da empresa (comercial, medição, ONS, CCEE, administrativa, etc.), e isto pode ser feito de maneira segura atendendo as recomendações do NIST-National Institute of Standards and Technology, da Cisco Systems e da NSA-National Security Agency.

1. Introdução

A Enersul[1] , desde o início da implantação da rede operativa, possui um sistema próprio de telecomunicações a fim de viabilizar a comunicação entre o COS (Centro de Operação do Sistema Elétrico) e as demais localidades (Figura-1), salvo aquelas que estão impossibilitadas em decorrência das características geográficas, onde se utiliza canais de comunicação das operadoras de telefonia.

Figura-1 - Mapa do sistema de Telecomunicações (rede de dados) da Enersul.

Em face do atual nível de dependência da supervisão automatizada em que a Enersul vivencia, onde as subestações são integralmente desassistidas, torna-se necessário uma alta disponibilidade do sistema SCADA para sua adequada operação, onde a segurança da informação é um fator crítico de sucesso na operação do sistema elétrico (automação e supervisão de religadores e unidades remotas, subestações, repetidoras, teleproteção de linhas de transmissão, comunicação com equipes de campo e todo o serviço de transmissão de voz e dados).

A área de Automação e Telecomunicações da Enersul implementou uma arquitetura de redundância das rotas de comunicação entre os Centros de Operação e as subestações para atender os requisitos de alta disponibilidade e resiliência2. Assim, destacamos que o COS da Enersul possui um site principal (localizado na sede administrativa) e um de contingência (instalado em uma subestação localizada a dezesseis quilômetros do principal), interligados através de fibra óptica redundante (Figura-2). Para aumentar o grau de disponibilidade da supervisão das subestações e, aproveitando as arquiteturas dos sistemas, estamos implementando procedimentos e políticas de segurança no ambiente SCADA, que vai desde o acesso físico ao nivel de informação.

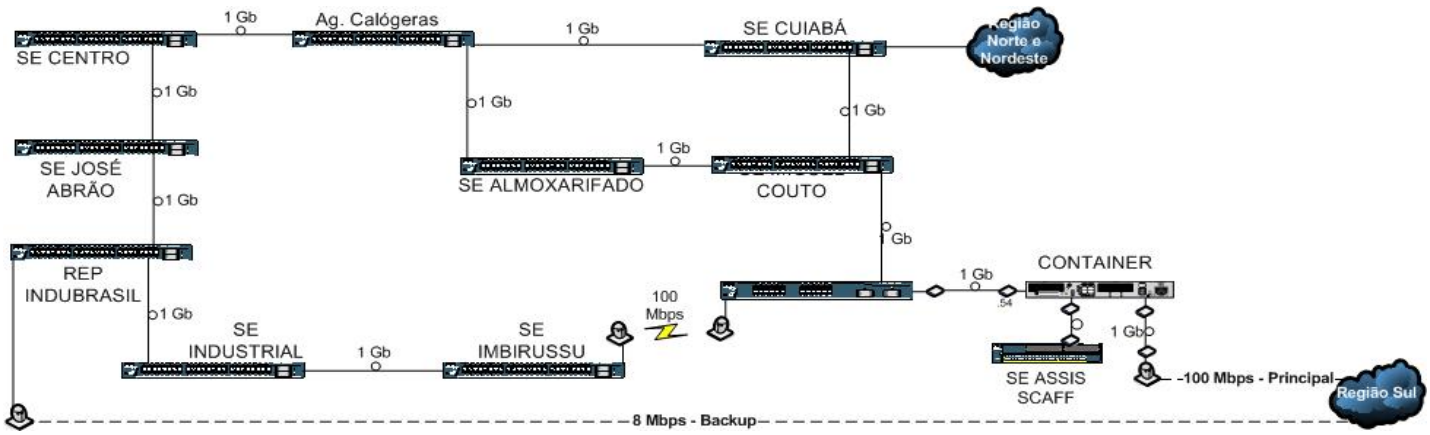


Figura-2 - Diagrama da rede operativa da Enersul na Capital (Campo Grande).

Portanto, com essa característica do sistema, podemos tornar o processo de supervisão das subestações da área de concessão da Enersul com um alto nível de disponibilidade para a Operação, sem haver interrupção da comunicação resultando em uma grande confiabilidade no monitoramento do sistema elétrico. Mas somente isso não basta, pois, se faz necessário primar pela questão da segurança que pode ocasionar uma indisponibilidade do SCADA.

2. Desenvolvimento

1. Identificando as vulnerabilidades do sistema SCADA.

No início da automação das subestações, os sistemas se comunicavam por meio de interfaces seriais, que utilizavam protocolos do padrão elétrico RS232 (distancia maxima de 12m) ou RS485 (até 1200m), necessitando, além disto, a comunicação entre o controlador de campo e o COS (Figura-3). Não bastava apenas o meio físico, mas também o protocolo de comunicação para este tipo de interface. Como a comunicação era feita através de interface serial, não havia muita preocupacão com a questão da segurança da informação, uma porque os protocolos eram específicos e não havia possibilidade de invasão do sistema sem ter acesso ao ambiente físico.

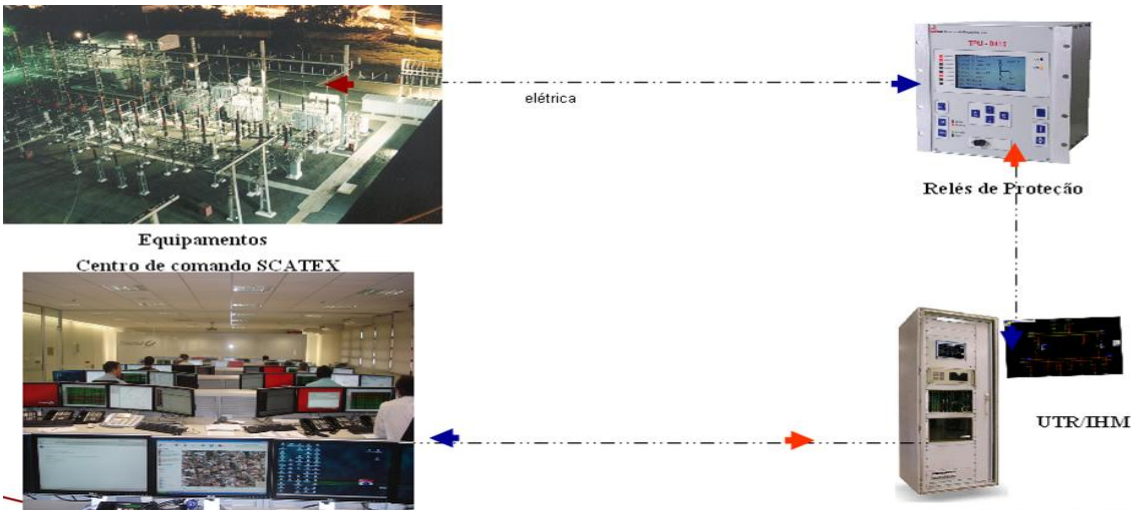


Figura-3 - Sistema de comunicação através de interface serial.

Com a modernização dos equipamentos utilizados no sistema SCADA e, consequentemente, a adoção de interfaces padrão Ethernet e protocolo de rede TCP/IP, aliado ainda com a necessidade de troca de

informação entre a rede operativa com redes menos seguradas (integração); o quesito “segurança” ganhou destaque e se tornou um motivo de preocupação. No caso de uma concessionária de distribuição de energia elétrica ter sua rede administrativa invadida por algum vírus e alguns serviços ficarem indisponíveis (email, internet, servidor de arquivos, etc.), o impacto não será tão grande. Agora, se a rede operativa ficar inoperante em decorrência de uma invasão, o sistema SCADA perderá toda a supervisão do sistema elétrico (alimentador, religador, transformador, medidores, reles de proteção, etc.), o que acarretará em vultosas multas aplicadas pelos órgãos reguladores e uma possível diminuição da receita caso algum alimentador para de fornecer energia a um determinado segmento de consumidores, sem falar dos indicadores.

Considerando que a disponibilidade do sistema SCADA é vital para a operação do sistema elétrico de toda concessionária de energia elétrica, faz-se necessário identificar as vulnerabilidades do ambiente e as possíveis ameaças que podem afetar o seu funcionamento, criando e implementando “boas práticas” de segurança para mitigar e neutralizar os riscos de invasão e sua consequente indisponibilidade.

1.1 Comparando a rede administrativa com o ambiente SCADA.

Com o avanco da tecnologia, todos os dispositivos da rede operativa passaram a ter uma interface ethernet para propiciar a comunicação através do protocolo TCP/IP. Mas nem tudo que se encontra nesta condição deve ficar sob a gestão da área de TI. São ambientes, embora análogos quando aos dispositivos (firewalls, switches, roteadores, servidores, etc.), distintos quanto a sua funcionalidade. Se a rede administrativa ficar indisponível, em regra não haverá perda de receita. E ainda, alguns serviços podem esperar para serem restabelecidos, conforme preceitua as normas de ITIL e Cobit. Na rede operativa o sistema não pode esperar, pois se trata de um ambiente com operação em tempo real, motivo pelo qual deve haver redundância. Vale a pena ressaltar que os investimentos, respeitado o limite da empresa-referência, podem ser repassados para a tarifa.

1.2 Ameaças.

As ameaças ao ambientes do SCADA não se restringem somente a questão da comunicação (vírus, cavalos de tróia, trojans, backdoor, etc.), mas sim ao acesso físico dos equipamentos. Restringir o acesso físico faz parte das políticas de segurança a operação do sistema elétrico. Acesso a base de dados e aos servidores, roteadores, switches, além dos equipamentos como relés de proteção, devem ser restritos e controlados. Portanto, todas as vulnerabilidades em potencial que possam ameaçar a disponibilidade do SCADA devem ser evitadas.

1.3 Políticas e Procedimentos contra vulnerabilidades.

Fatores de risco, como as vulnerabilidades de todos os equipamentos que compõem o ambiente SCADA devem ser analisadas constantemente. Análise do tráfego da rede IP é primordial para se monitorar e identificar possíveis vulnerabilidades como forma de manutenção pró-ativa. Estabelecer uma política e os procedimentos para manter a rede operativa disponível não e uma tarefa fácil, necessita de tempo, planejamento e de recursos humanos e materiais. São vários os planos para elaboração de políticas e procedimentos, porém, o esquema abaixo (Figura-4) representa, de maneira macro, as principais etapas para se implementar a segurança no ambiente SCADA.

Figura-4 - Guia para elaboração das políticas e procedimentos para implantação de segurança na rede IP.

Veja que o esquema propõe a constante avaliação das politicas, procedimentos e padrões adotados pela empresa. Primeiro deve-se analisar os risco e em seguida, desenhar a arquiterura proposta para neutralizar os riscos. Uma vez avaliada e escolhida a solução que atende a necessidade da empresa, partimos para a aquisição e treinamento, ou seja, todos aqueles envolvidos no processo devem ser capacitados para intervir quando for necessário. Uma vez implementada a solução, deve-se monitorar o ambiente e responder quando algo de errado ocorrer.

1.4 Compartilhamento das informações do sistema elétrico.

O SCADA fornece informações para outras areas da empresa e isto necessita ser feito de forma segura. Atualmente existem várias maneiras de compartilhar estas informações: através de VPN (rede privada virtual), serviço de FTP (file transfer protocol), Proxy-Reverso, Firewall, etc (Figura-5). Além da segurança, é importante destacar que o processo de troca das informações deve ser feita de maneira automatizada (via aplicação). Não deve ser usado procedimentos manuais que dependem da intervenção humana, como por exemplo o uso de pen-drives ou planilhas eletrônicas.

Figura-4 - Diagrama contendo integração entre redes distintas.

1.5 Vislumbrar possíveis cenários de incidentes.

O ambiente SCADA pode ficar indisponível por vários fatores que precisam ser identificados, devendo elaborar um plano de distater-recovery para cada situação elencada. A Figura-6 mostra um esquema contínuo de avaliação do ciclo de segurança proposto pela Empresa Cisco Systems.

Figura-6 - Esquema do ciclo de vida dos serviços de segurança.

Para cada cenário deve-se utilizar este esquema que no centro prevê cinco fases: 1) planejar uma estratégia para a indisponibilidade; 2) desenvolver (desenhar) a solução vislumbrada; 3) implementar; 4) torná-la operacional; 5) por fim, otimizar a solução. Este planejamento propiciará fazer uma manutenção preventiva e fazer com que a equipe envolvida possa se antecipar à indisponibilidade.

1.6 Padroniação de equipamentos.

A padronização de equipamentos possui vantagens (padrão de configuração/manutenção e baixo custo em treinamento) e desvantagens (relativa dependência de um único fabricante), devendo em cada caso concreto avaliar a escolha. No caso da Enersul, em decorrência de inúmeros fatores, optou-se em padronizar alguns equipamentos. Relés e UTR's: Schweitzer; roteadores e switches de borda: Cisco; switches IEC61850: Moxa; Rádios: Harris; Firewall e IPS/IDS: Cisco; Servidores e estações de trabalho: HP; VPN: Cisco, etc.

1.7 Documentação dos Incidentes.

A gestao da rede operativa deve registrar todos os incidentes que causam a indisponibilidade do SCADA, com o fim de atuar no problema evitando que o mesmo se repita. Além das estatísticas, esta documentação servirá como guia para a elaboração de planos para aprimorar a segurança da rede. Outro fator importante é a confecção de documentos que possam viabilizar a intervenção na ausência de um analista. Neste caso podemos citar o conhecido POP (procedimento operacional padrão), documento que descreve o que deve ser feito para restabelecer a comunicação quando ocorrer um incidente.

2. Desenvolvendo e implantando um programa de segurança.

2.1 Segurança x Negócio.

Embora a segurança do ambiente SCADA seja de suma importância, isto não pode inviabilizar a msisão da

empresa. Em outras palavras, a segurança não pode servir como desculpa para não atender nas necessidades do negócio.

2.1.1 Benefícios x Consequências.

Investir em segurança trará certos benefícios à empresa: minimizará o tempo de indisponibilidade do sistema SCADA, o que evitará possíveis sanções dos órgãos regulatórios; e o valor investido poderá ser repassado à tarifa. Caso não haja a implementação de segurança na rede do SCADA, o sismtea pode ficar indisponível.

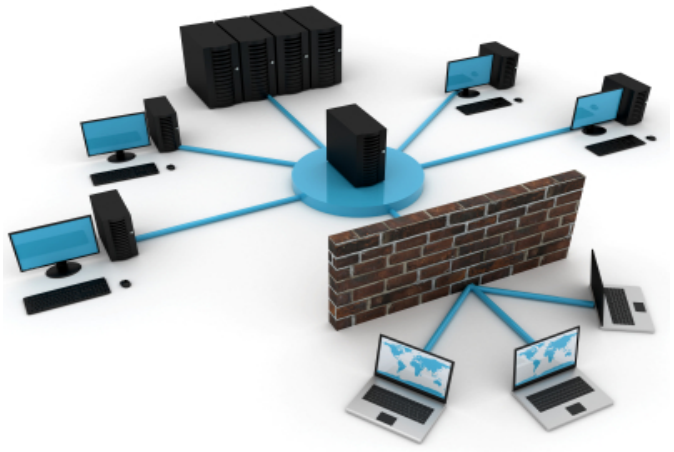
2.1.2 Aprovação da Diretoria.

Ao apresentar um programa de desenvolvimento para implantação de segurança no ambiente SCADA, não basta explorar apenas o aspecto técnico, mas demonstar com números que o investimento é uma solução viável em todos os aspectos (político-social, financeiro, regulamentar, etc.).

3. Arquitetura de rede.

3.1 Firewalls.

Este equipamento deve ser utilizado para separa (segmentar) a rede operativa de redes menos seguras. Na Enersul por exemplo, este dispositivo de segurança possui 4 segmentos: Rede Operativa (mais seguro), segmento DMZ (menos seguro), Internet (segurança zero), e rede corporativa (menos segura). Através do Firewall pode configurar qual tipo de tráfego será permitido ou proibido entre os segmentos de rede conectados nele (Figura-7).



3.2 Redundância de equipamentos.

Todas as estações de trabalho e os servidores da Enersul possuem 2 placas de rede, sendo que a primeira está conectada no switch primário e as secundárias no swich de backup. Isto é muito importante em sistemas SACADA pela característica de "real time", pois em caso de falha do principal, o secundário assume e a equipe de manutenção terá tempo para trabalhar.

3.3 Domain Name System (DNS).

O uso do serviço de DNS deve ser evitado na rede, salvo nos casos de acesso à internet. Além de causar um certo 'delay' para a resolução do nome, este serviço possui muitas vulnerabilidades.

3.4 Comunicação com protocolos de criptografia.

Todos os equipamentos da rede operativa não devem fazer a comunicação com protocolos comuns (HTTP, FTP, Telnet, etc.), onde a informação contida no pacote IP pode ser 'visto' na rede. Devem suportar protocolos de comunicação com criptografia (HTTPS, SSH, SFTP, etc.). Desta forma, mesmo que um pacote seja capturado na rede, o mesmo estará modificado (criptografado).

3.5 Simple Network Management Protocol (SNMP).

O Protocolo SNMP é usado para gerenciar redes TCP/IP complexas, onde os administradores podem gerenciar e configurar equipamentos da rede, utilizado para monitorar o desempenho da rede, detectar problemas e acompanhar quem usa a rede e como ela é usada. A Enersul utiliza 03 softwares gratuitos para fazer o gerenciamento do ambiente SCADA: Cacti, Nagios e NTOP.

3.6 Network Address Translation (NAT)

Também conhecido como *masquerading* é uma técnica que consiste em reescrever os endereços IP de origem de um pacote que passam por um *router* ou *firewall* de maneira que um computador de uma rede interna tenha acesso ao exterior ou Rede Mundial de Computadores(rede pública).

3.7 Controle de acesso.

A Enersul implantou um sistema de controle de acesso nas subestações mais importantes. Somente será permitida a entrada com a autorização antecipadado COS.

3.8 Switches.

Segundo as recomendações de vários guias de obas práticas de segurança, seria altamente recomendável a adoção de alguns recursos nos switches da rede operativa. Dente eles podemos destacar o acesso somente via protocolo SSH, alterar o valor da velocidade da porta de console, atribuir os endereços MAC à determinada porta, desenergizar as portas não-utilizadas, VLANs.

3.9 Roteadores.

Implementar recursos em camada 3 (MLPS , VRF) e camada 2 (VLANs) e desabilitar funções que não serão utilizadas. Dependendo da situação, a configuração de listas de acesso (ACLs) também é indicada.

3.10 Servidores e estações de trabalho.

Inicialmente, a Enersul tinha servidores HP-UX (Unix) e estações de trabalho com sistema operacional Windows. Agora migramos para o ambiente virtualizado com VMware com redundância. Ambientes tradicionais baseados em Windows acarreta em algumas desvantagens como: constantes atualizações do sistema operacional; correta configuração dos privilégios do usuário, serviços desnecessários habilitados, dificuldade no procedimento de backup, ambiente virtual incipiente e insipiente, etc.

3.11 Backup.

Embora seja um procedimento aparentemente dispensável e cansativo, o backup faz-se necessário em virtude da restauração do ambiente em caso de falha. No que diz respeito à virtualização, o backup se torna muito mais fácil e rápido. Quanto aos equipamentos de rede (firewall, switch, roteador, etc.) seria possível

fazer o backup de forma automatizada com o software gratuito Rancid, desde que o equipamento tenha suporte à linha de comando. Quando se fala em backup não se pode esquecer dos equipamentos sobressalentes, cuja necessidade indicará o seu percentual.

3.12 Sistema de detecção/prevenção de intrusão.

São sistemas (hadware/software) que tem por função detectar e prevenir os acessos não autorizados às redes ou hosts de uma ou mais redes, sendo portanto grandes aliados dos(as) administradores(as) de redes na manutenção da segurança dos ambientes por eles(as) controlados.

3. Conclusões

Para propiciar a interação com redes menos seguras, a Enersul está implementando as melhoras práticas de segurança na rede operativa (sistema SCADA) conforme as recomendações do NIST (National Institute of Standards and Technology) através do “Guide to Industrial Control Systems (ICS) Security”, além das orientações contidas nos guias da Cisco Systems e da NSA/CSS (National Security Agency/Central Security Service).

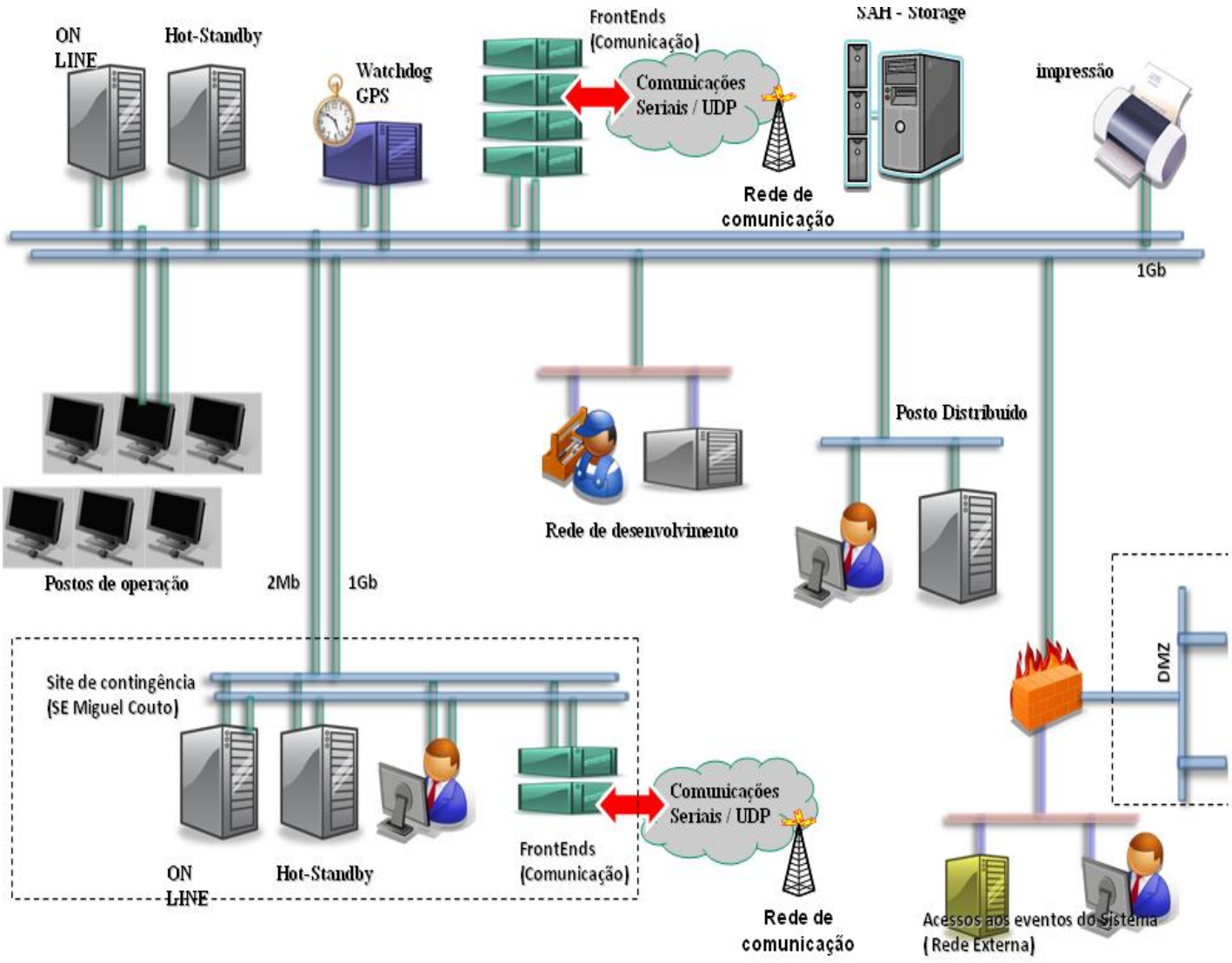


Figura-8 - Diagrama resumido do ambiente SCADA da Enersul.

O objetivo maior do enfoque "segurança" no ambiente SCADA é propiciar a integração da rede operativa com redes menos seguras, além de garantir uma proteção da rede interna contra ameaças que podem surgir com possíveis falhas ainda não detectadas.

Neste informe dispusemos a importância de divulgar a proposta da arquitetura de segurança da rede operativa da Enersul (Figura-8), com o objetivo de fornecer um modelo e diretrizes às demais concessionárias do setor elétrico que estarão presentes neste Seminário a fim de evitar falhas no ambiente SCADA e garantir a disponibilidade da operação do sistema elétrico.

4. Referências bibliográficas

_____

1 : Integrante do Grupo Rede Energia, a Enersul e responsavel pela distribuicao de energia eletrica no Estado de Mato Grosso do Sul.

2 : Propriedade de um equipamento resistir e ultrapassar as adversidades mantendo seu funcionamento inicial.