SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

GOP - 10
16 a 21 Outubro de 2005
Curitiba - Paraná

GRUPO IX
GRUPO DE ESTUDO DE OPERAÇÃO DE SISTEMAS ELÉTRICOS - GOP

Segurança em Sistemas EMS/SCADA

Ayru L. Oliveira Filho*

CEPEL – Centro de Pesquisas de Energia Elétrica

RESUMO

Durante muitos anos, os sistemas de Supervisão e Controle (SCADA/EMS) das empresas de energia elétrica puderam ser tratados como imunes a problemas de segurança devidos a acessos via meios eletrônicos. Entretanto, este cenário já não é real na maioria das empresas do setor. As evoluções nas áreas de comunicação e Tecnologia da Informação possibilitaram a interconexão do ambiente de Operação em tempo real com outros domínios da corporação. O objetivo deste trabalho é levantar a questão da segurança digital em sistemas EMS/SCADA no Brasil. Serão apresentados os possíveis riscos aos quais tais sistemas estão expostos, as tecnologias disponíveis para mitigá-los e os esforços e desenvolvimentos atuais específicos para a segurança de sistemas SCADA.

PALAVRAS-CHAVE

SCADA, EMS, Supervisão e Controle, Segurança eletrônica, Internet.

1.0 - INTRODUÇÃO

A questão da segurança no acesso a recursos computacionais e dados corporativos tem sido alvo de crescentes investimentos nos últimos anos por parte das empresas. No setor de energia elétrica, isto também vem acontecendo e a grande maioria das empresas do setor mantém algum nível de proteção ao acesso remoto à sua infra-estrutura computacional. Estes investimentos, entretanto, nem sempre são suficientes para impedir o acesso indevido a dados e o comprometimento de sistemas pelas várias formas de ataques digitais que acontecem diariamente. Dados de entidades que monitoram e contabilizam tais ataques mostram um significativo aumento das vulnerabilidades dos sistemas digitais acompanhado por um também expressivo aumento nos relatos de ataques bem sucedidos.

Dentre os diversos sistemas digitais existentes em uma empresa de energia elétrica, o Sistema de Supervisão e Controle – EMS/SCADA se destaca como essencial para a operação segura e eficiente do sistema elétrico controlado. Por sua importância e características particulares, a questão da segurança relativa aos sistemas EMS/SCADA comumente é tratada com especial atenção. Senhas de acesso, câmeras de vídeo e outros dispositivos de segurança física são freqüentemente encontrados no ambiente de supervisão e controle. Do ponto de vista da segurança de acesso via meios digitais, algumas características peculiares a tais sistemas contribuíam, até recentemente, para um alto grau de segurança digital. A conexão com equipamentos de campo

*Av. Um s/n – Cidade universitária - CEP 21941-590 – Rio de Janeiro - RJ - BRASIL
Tel.: (21) 2598-6240 - Fax: (21) 2260-6211 - e-mail: ayru@cepel.br

isolados através de protocolos proprietários ou pouco difundidos, a ligação fraca ou inexistente com a rede corporativa da empresa e o uso de tecnologias particulares garantiam tal nível de segurança.

Entretanto, este cenário naturalmente protegido está mudando rapidamente. A conexão forte entre o sistema EMS/SCADA e a rede corporativa da empresa é, hoje, quase essencial. Dados de tempo real são valiosa fonte de informação para as demais áreas corporativas, em especial no ambiente mais regulado e competitivo que vem se consolidado no setor em todo o mundo. As conexões para troca de dados de tempo real estão deixando de ser dedicadas e sobre soluções proprietárias, dando lugar a conexões via rede, algumas vezes utilizando infra-estrutura pública, sobre protocolos padronizados. A troca de dados de tempo real entre empresas através de protocolos SCADA também tem se tornado freqüente, abrindo novas portas de acesso a tais sistemas. Por outro lado, as tecnologias utilizadas em sistemas de Tecnologia da Informação estão, cada vez mais, sendo incorporadas às soluções EMS/SCADA presentes no mercado. Isso traz para o ambiente de Supervisão e Controle todas as vulnerabilidades publicamente conhecidas de tais tecnologias.

Tudo isso mostra que os sistemas EMS/SCADA estão mais vulneráveis que no passado e cada vez mais conectados a infra-estruturas públicas de comunicação (leia-se Internet). Toda esta exposição já tem causado eventos de invasões e contaminações relatadas neste tipo de sistema, ainda que nenhum evento de interrupção de energia tenha tido como causa direta um ataque digital. Entretanto, existem relatos em outros setores, que também utilizam sistemas SCADA, como o tratamento de água e esgoto, de incidentes que tiveram como causa a atuação não autorizada e remota sobre o sistema de controle existente.

2.0 - EXPOSIÇÃO A RISCOS

2.1 Evolução da Arquitetura

A FIGURA 1 mostra duas situações extremas: no lado esquerdo vemos uma típica configuração de um sistema SCADA isolado. No lado direito, imaginamos uma configuração conceitual que utiliza diversas novas tecnologias de comunicação e de TI para as funções de Supervisão e Controle.

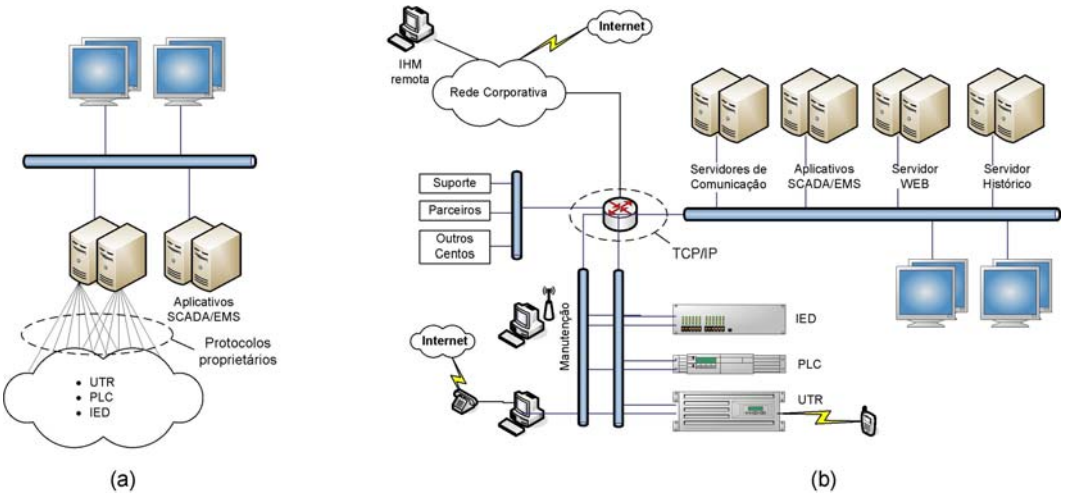

FIGURA 1 – Arquiteturas de sistemas EMS/SCADA

Os sistemas SCADA em operação atualmente apresentam arquiteturas que combinam características de ambas as configurações, com a tendência crescente de migração para uma situação mais próxima daquela exposta na FIGURA 1-(b). O que podemos observar nesta figura é que, inicialmente, os sistemas SCADA eram completamente desconectados dos demais sistemas corporativos e utilizavam tecnologias proprietárias e de conhecimento restrito a um pequeno número de pessoas. Protocolos de comunicação com UTR, por exemplo, eram também proprietários e de uso exclusivo para a finalidade de comunicação entre o sistema SCADA e os equipamentos de campo. Estas características tornavam um sistema com esta configuração praticamente imune a interferências externas no sistema digital de supervisão e controle.

Como os dados de tempo real são fonte valiosa de informação para a corporação, a conexão do ambiente de operação em tempo real com o resto da empresa é inevitável. Esta conexão pode se dar de diversas formas, entre elas: através de canais de acesso remoto via a interconexão da rede SCADA com a rede corporativa, via o acesso corporativo a bases de dados do ambiente de operação em tempo real ou através de protocolos entre sistemas externos e o próprio sistema de supervisão e controle. Seja por qual mecanismo for, a quebra do isolamento

arquitetural dos sistemas SCADA cria caminhos para o acesso indevido a tais sistemas e permite que a atividade das redes externas interfira no desempenho do sistema de controle.

Outra diferença marcante nesta evolução é a utilização predominante do protocolo TCP/IP para todo o tipo de comunicação na arquitetura da Figura 1-(b) em substituição da camada de transporte dos protocolos proprietários especificamente projetados para a comunicação entre o SCADA e os equipamentos ou sistemas remotos. Esta migração vem acontecendo gradualmente devido ao estabelecimento do TCP/IP como protocolo padrão para comunicação via rede de computadores. Se, por um lado, a adoção deste padrão simplifica e viabiliza a comunicação de/para o Centro de Controle, por outro contribui para um aumento na exposição a riscos de acessos não autorizados ao sistema SCADA. O TCP/IP é um conjunto de protocolos com reconhecidas falhas de segurança (7). Sua maciça utilização como protocolo básico para a Internet faz com que tais falhas sejam amplamente exploradas por hackers e ferramentas automáticas disponíveis em diversos *sites* a qualquer usuário. Também a progressiva migração para o uso de protocolos de aplicação padronizados e com especificação aberta faz com que as informações suas características e possíveis falhas de segurança sejam publicamente conhecidas e que um número cada vez maior de pessoas tenham o conhecimento especifico de tais protocolos.

2.2 Evolução da Tecnologia da Informação em Sistemas EMS/SCADA

Na arquitetura da FIGURA 1-(b), também podemos considerar o uso cada vez maior de produtos de software padronizados ou “de prateleira” para a implementação das funcionalidades do Centro de Controle. Sistemas operacionais de uso geral tais como o MS-Windows e o Linux alcançaram um grau de robustez que permite que sejam utilizados em todas as funções de um sistema EMS/SCADA. Outros protocolos tais como SNMP, HTTP, RCP, SOAP, dentre vários outros estão também sendo utilizados em funções diversas. Sistemas gerenciadores de banco de dados e serviços WEB habilitam o Centro de Controle a fornecer informações tratadas para a apresentação a outros setores da empresa.

Entretanto, todas estas facilidades permitidas pela evolução das tecnologias de TI trazem consigo novos riscos de acessos indevidos a informações e ao próprio sistema EMS/SCADA. Apesar de útil e necessário à evolução do papel do Centro de Controle nas corporações, o uso de qualquer tecnologia deve ser acompanhado do tratamento dos riscos de segurança inerentes.

2.3 Riscos Decorrentes

Como visto, os sistemas SCADA estão cada vez mais conectados a redes corporativas e a redes de troca de dados de tempo real. Isto significa, primeiramente, que existem novas portas, muitas vezes abertas, pelas quais podem se dar acessos indevidos. Imagine, por exemplo, que a empresa A estabeleça um canal de comunicação com a empresa B para troca de dados de supervisão. Este canal, em princípio, é utilizado apenas para este fim e por ele somente trafegam dados sobre o protocolo acordado entre as partes. Entretanto, tanto a empresa A quanto a empresa B mantêm outras conexões com outras entidades externas e desconhecidas de suas contrapartes. Ou seja, um simples canal de comunicação entre duas empresas, com finalidade bem específica, pode significar a conexão a uma rede de tamanho e configuração desconhecidos. Na verdade, muito provavelmente, este canal se torna também um novo caminho para internet cujas características de segurança são desconhecidas.

As colocações feitas anteriormente não têm o objetivo de sugerir que tais conexões não devam ser feitas. Ao contrário disso, entendemos como necessária a existência de tais conexões com empresas parceiras, fornecedores e entidades do setor. Entretanto, tal procedimento deve ser feito sempre considerando critérios de segurança e utilizando-se as ferramentas disponíveis de proteção. Além disso, caminhos entre o ambiente de operação e uma rede desconhecida (internet) normalmente já existem nos centros de controle da maioria das empresas.

Sejam para a internet ou para conexões privadas entre entidades, a criação de portas no ambiente crítico da operação em tempo real expõe os sistemas SCADA às mazelas do mundo da comunicação digital. O fato de ser cada vez mais comum o uso de produtos padronizados e de prateleira para a composição das funcionalidades de um SCADA/EMS contribui também para o aumento das vulnerabilidades do sistema de controle. Um sistema baseado em MS-Windows, por exemplo, herda todas os pontos vulneráveis dos componentes do sistema operacional os quais são amplamente divulgados e para os quais existe grande ferramental de exploração disponível publicamente. Sistemas de controle baseados em Unix são menos vulneráveis, dada a menor disponibilidade de ferramentas de exploração, mas não imunes, a interferências indiretas na sua operação.

Dado que um sistema SCADA/EMS em operação muito provavelmente está conectado a redes externas, deve-se considerar as seguintes ameaças:

- *Malwares*: Vírus, worms e Trojans[1] que circulam pelas redes; estes softwares podem causar tanto danos diretos aos computadores afetados quanto congestionamentos nas redes de comunicação, podendo ser causa da indisponibilidade de máquinas ou de redes;
- Deny of Service - DoS: este é um ataque direcionado a um serviço conhecido que busca tirar o serviço de funcionamento através do envio de grandes quantidades de dados inválidos. Como se comportaria um protocolo SCADA se seu servidor fosse inundado com mensagens inválidas?
- Manipulação de Tráfego: trata-se da interrupção ou insersão de tráfego não pertinente à uma comunicação. Muitos protocolos SCADA não são baseados em sessões, o que faze com que servidores respondam a mensagens sem uma validação da sua fonte;
- Acesso não autorizado (hackers): hackers podem tentar o acesso a sistemas corporativos por diversos motivos; desde a obtenção de reconhecimento da comunidade, obtenção de informações ou utilização da plataforma para o lançamento de outros ataques;
- Ataques especificamente direcionados visando algum tipo de dano à companhia. Por exemplo, (ex)funcionário insatisfeito ou concorrente;

A existência destas vulnerabilidades e ameaças nos parece real e crescente. Aliado a isto, devemos considerar como fatores de aumento de risco o fato de existir pouca disseminação da cultura de segurança eletrônica entre os engenheiros de supervisão e controle, a muitas vezes inexistente política de segurança da empresa que abranja o sistema SCADA, a inexistência ou configuração indevida de mecanismos de bloqueio de acesso (*firewalls*), a inexistência de mecanismos de monitoramento da rede de tempo real e a comum desatualização dos sistemas (*patches*).

2.4 Eventos Recentes

Eventos de ataques bem sucedidos costumam não serem relatados por revelarem fragilidades nos sistemas de uma corporação. Até a data deste trabalho, não se conhecia relato de evento de interrupção de energia devido a algum tipo de interferência eletrônica externa, o quê não significa que já não tenha ocorrido. Entretanto, alguns eventos foram relatados por algumas empresas que utilizam sistemas SCADA.

Talvez o evento conhecido de maiores conseqüências até hoje e amplamente divulgado seja um ataque a uma companhia australiana de tratamento de esgotos ocorrido em 2000 (3). Entre janeiro e abril daquele ano o sistema SCADA sofreu 47 falhas inexplicáveis o que causou o derramamento de milhões de litros de esgoto na rede de água local. O atacante, um ex-prestador de serviços descontente com a negativa de emprego, utilizou seu conhecimento do sistema e um acesso *wireless* para executar comandos no sistema SCADA da companhia.

Em janeiro de 2003 o *worm* Slammer passou pelas proteções da rede corporativa da usina nuclear Davis-Besse em Ohio, causando a desativação do sistema de monitoramento de segurança da usina por aproximadamente 6 horas (2). Neste caso a entrada do worm se deu através de um canal T1 com uma empresa contratada.

Também foi relatado um ataque direto ao operador do sistema elétrico da Califórnia - Cal-ISO em maio de 2001 (4). Hackers, possivelmente da China, tiveram acesso a um computador da empresa, mas não ao seus sistemas de controle.

Estes eventos mostram que os sistemas SCADA estão expostos a riscos tanto de ataques diretos quanto a ataques indiretos devidos a vírus e *worms*. Mesmo sistemas que não utilizam internet, ao utilizarem infra-estrutura comercial para tráfegos de dados SCADA podem estar sujeitas aos efeitos de vírus uma vez que o serviço de comunicação é compartilhado com outras atividades.

2.5 Estatísticas

O Banco de Dados de Incidentes de Segurança na Indústria (ISID) gerenciado pelo Instituto de Tecnologia British Columbia armazena informações classificadas de incidentes em sistemas industriais. A análise destas informações revela que as fontes mais comuns de ataques e mostra que a distribuição entre incidentes, ataques internos e ataques externos vêm mudando com o passar do tempo (1). Até a divulgação dos resultados, acreditava-se que a principal fonte de ataques fosse interna (8), o que era confirmado pelos dados até o ano 2000.

---

[1] **Virus**: Programa que contém código para se auto-copiar e que pode “infectar” outros programas modificando-os de forma que sua execução causa a execução do código do vírus e sua replicação.
Worms: Programa auto-suficiente que possui a habilidade de disseminar-se através de cópias funcionais dele mesmo a outros sistemas de computadores. Diferentemente de um vírus, worms não precisam de outros programas para anexar-se.
Trojan Horses: Programa que executa algum código não documentado diferente do objetivo divulgado.

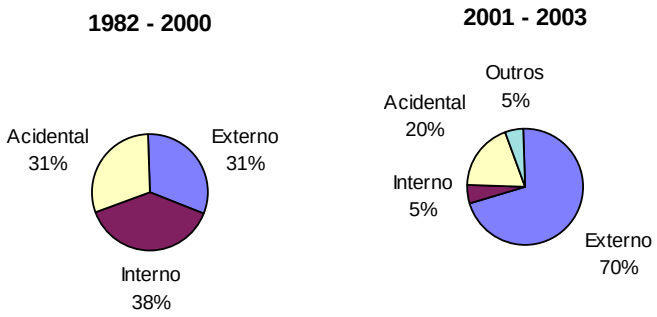

FIGURA 2 – Estatísticas de incidentes de segurança na indústria

Observa-se que de 2001 a 2003 a principal fonte de ataques passou a ser externa. Esta modificação pode ser explicada pela incorporação das evoluções tecnológicas apresentadas na seção 2.2 e também pela existência cada vez maior de ataques automatizados dispersos pela Internet. Apesar dos ataques internos terem diminuído proporcionalmente, a estes não se deve dar menor importância pois as fontes internas, em geral, têm maior conhecimento dos processos internos e podem gerar taques com conseqüências mais diretas a sistemas como o SCADA.

Os caminhos de entrada para estes crescentes ataques externos podem ser vários (vide seção 2.1) no caso de um sistema SCADA. As conexões via Internet, diretas ou indiretas, continuam sendo as principais portas de acesso. Entretanto, acessos remotos via conexões discadas, VPN, conexões com parceiros e fornecedores, conexões *wireless* e pela rede de dados SCADA constituem importantes caminhos a serem protegidos.

3.0 - TECNOLOGIAS PARA MITIGAR RISCOS

Diversas tecnologias têm sido utilizadas para mitigar os riscos de acessos indevidos e interferências externas no funcionamento de sistemas em geral. A FIGURA 3 ilustra uma configuração conceitual onde alguns destes componentes de segurança estão presentes.

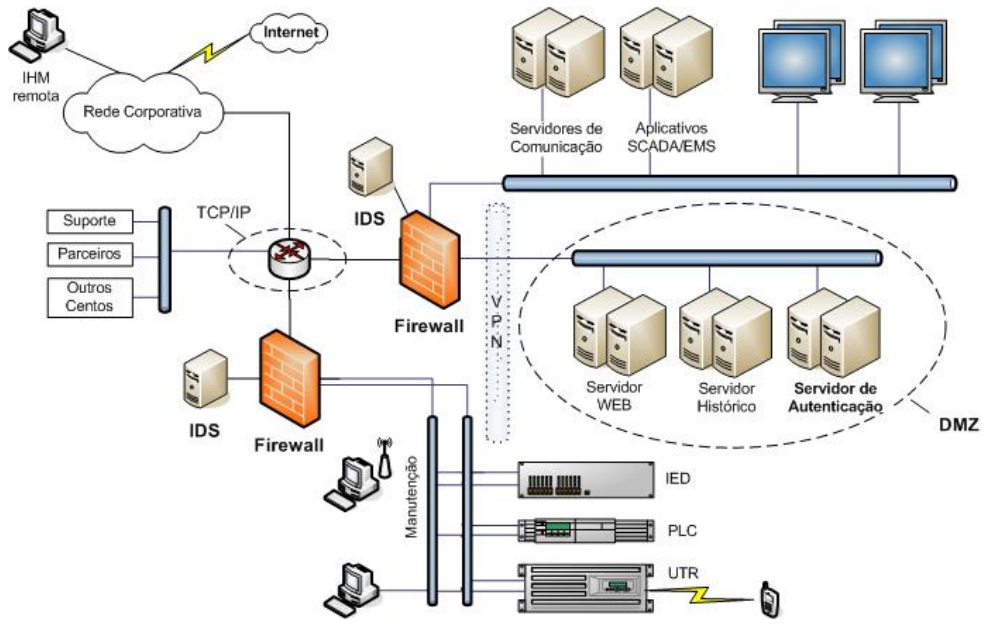

FIGURA 3 – Elementos de segurança; arquitetura conceitual.

Os primeiros elementos que destacamos na FIGURA 3 são os *Firewalls*. Estes equipamentos inspecionam os pacotes de dados que fluem entre suas interfaces e permite ou não este tráfego, baseando-se em regras pré-definidas. Através destas regras é possível estabelecer filtros que consideram aspectos de endereçamento dos

pacotes (origem, destino, protocolo, porta e o sentido do tráfego) e que interpretam o conteúdo da mensagem analisando a porção de dados dos pacotes. *Firewalls* podem ser implementados em *harwares* específicos ou em computadores de uso geral com software específico. Em ambos os casos, os *firewalls* também são alvo de ataques e a gerência de sua configuração, tanto de regras quanto de atualizações (*patches*), deve ser considerada crítica para a segurança do sistema protegido. *Firewalls* definem perímetros de segurança para os quais diferentes conjuntos de regras e filtros são definidos de acordo com as características específicas de acesso de cada um. Na FIGURA 3 podemos identificar um perímetro onde se encontram os equipamentos que implementam o sistema EMS/SCADA, um perímetro onde estão os equipamentos de campo e um perímetro especial chamado de DMZ[2]. Na DMZ estão os serviços que podem ser acessados por entidades externas ao ambiente de supervisão e controle. Nela colocamos, como um exemplo, o acesso a dados de tempo real servidos ao ambiente corporativo através de banco de dados históricos ou através de serviços WEB. A zona EMS/SCADA fica assim isolada de qualquer acesso externo direto.

Na DMZ também representamos um servidor de autenticação. Este servidor é responsável por garantir a autenticidade de um agente, seja ele humano ou um processo remoto, que deseja ter acesso a serviços ou equipamentos internos. Existem várias formas de autenticação segura. Estes mecanismos evitam que senhas sejam trocadas abertamente pela rede de comunicação e utilizam mecanismos de chaves e algoritmos de criptografia para checar a autenticidade da identificação de um usuário (7). Também é possível combinar o serviço de autenticação segura com cartões inteligentes ou *tokens* a fim de proporcionar maior segurança ao acesso às consoles de operação.

Também aparecem na FIGURA 3 sistemas de detecção de intrusos – IDS. Este software ou hardware também inspeciona os pacotes que chegam a uma rede, entretanto, ao invés de bloquear o tráfego, ele busca por padrões não usuais no tráfego que possam indicar tentativas de invasão ou comportamentos anormais. Um IDS pode ser visto como um sensor, tal como um detector de fumaça que gera um alarme caso detecte um tráfego suspeito na rede. Esta funcionalidade pode ser implementada em um hardware especial ou ser inserida no *firewall*. IDS de uso geral podem ser utilizados em sistemas EMS/SCADA, entretanto existem esforços no sentido de se construir bases de regras específicas para protocolos SCADA tais como DNP3, Modbus/TCP e OPC (9).

Dados trafegando em formatos livres de codificação comprometem a confidencialiade e a segurança (como no caso do trânsito de senhas), pois são passíveis de serem capturados em seu trajeto. Diversos mecanismos de criptografia podem ser utilizados para se garantir a confidencialidade, assim como a autenticidade, dos dados. Em conexões ponto a ponto, via modems, pode-se utilizar equipamentos que executam a função de criptografia de forma transparente e inserindo atrasos pouco significativos (6). Para conexões via rede, as Redes Virtuais Privadas - VPN podem ser utilizadas. Uma VPN pode ser vista como um túnel seguro construído sobre uma rede insegura. Após o estabelecimento da VPN, as unidades em cada uma das extremidades passam a compartilhar de maneira transparente, uma rede pela qual todos os dados são criptografados. As VPN podem ser utilizadas tanto para a troca de dados de supervisão quanto para o acesso remoto interno e externo ao sistema SCADA. Entretanto, o uso de VPN ou de hardware de criptografia em conexões via modems carece de avaliação prévia de desempenho para sua aplicação nos canais de comunicação de um sistema SCADA.

As tecnologias acima apresentadas estão maduras e podem ser utilizadas para se aumentar a segurança de um sistema EMS/SCADA. Entretanto, existem especificidades não cobertas por estas tecnologias e que ainda são objeto de pesquisa (10).

4.0 - ASPECTOS ESPECÍFICOS DE SEGURANÇA EM SISTEMAS SCADA

A segurança em sistemas SCADA tem sido reconhecida no setor elétrico como crítica devido às conseqüências potenciais de um acesso indevido ao sistema (11). Em especial nos Estados Unidos, a conscientização desta criticidade e da falta de padrões de segurança específicos para este tipo de sistema levou à criação de um conjunto de recomendações desenvolvidas emergencialmente pelo NERC (NERC 1200) (12). As recomendações desta norma serão válidas até agosto de 2005 enquanto o padrão definitivo (NERC 1300) (13) não está terminado. Até o momento da escrita deste artigo, o padrão 1300 estava com sua versão inicial concluída e em fase revisão pela comunidade. Neste padrão encontram-se recomendações para os seguintes tópicos:

- Gerência da segurança;
- Ativos virtuais críticos;
- Pessoal e treinamento;
- Segurança eletrônica;
- Segurança física
- Gerência da segurança de sistemas
- Plano de resposta a incidentes
- Planos de recomposição

Além destas recomendações e futuras normas, existem outros esforços de pesquisa e desenvolvimento em andamento que buscam atender às necessidades específicas de sistemas SCADA. Estão sendo investigados tópicos tais como *firewalls* e IDS capazes de interpretar protocolos SCADA, desenvolvimento de algoritmos de criptografia leves o bastante para serem executados pela CPU de PLC e UTR, desenvolvimento de cartões de

[2] DMZ: sigla em Inglês para Zona Desmilitarizada.

rede seguros para PLC, construção de equipamentos para criptografia para serem colocados junto aos PLC e UTR visando a segurança de sistema legados, desenvolvimento de mecanismos de autenticação segura e avaliação da segurança dos protocolos mais recentes tais como ICCP e IEC 61850 e proposição de melhorias.

As questões de segurança relacionadas aos protocolos DNP, ICCP e IEC 61850 estão sendo consideradas na proposta de padrão IEC 62351 cujo desenvolvimento se iniciou em fevereiro de 2004. Em paralelo a isto, um recente estudo conduzido pela Symantec (14) avaliou aspectos de segurança no uso do protocolo ICCP. Por exemplo, apesar dos dados trocados via ICCP serem codificados (ANS.1) eles não são criptografados, o que viabiliza a sua alteração. Por outro lado, o ICCP utiliza o endereço IP de sua contraparte para validar pedidos remotos, não existindo suporte à autenticação segura de usuários.

Ainda neste contexto, no âmbito do projeto SAGE[3], o CEPEL vem trabalhando no sentido de desenvolver um mecanismo de autenticação segura que contemple tanto o acesso dos operadores de tempo real quanto os acesso remoto a recursos como serviços WEB e bases de dados históricos. Por exemplo, um operador poderia utilizar seu cartão inteligente para ter acesso à console de tempo real, sendo que, através do mesmo mecanismo de autenticação, este mesmo operador poderia ter acesso a relatórios via WEB a partir de outra máquina fora da rede de tempo real.

5.0 - CONCLUSÕES

Neste artigo procuramos apresentar o cenário onde se encontram os sistemas EMS/SCADA com relação à segurança eletrônica. Os riscos de acessos indevidos a sistemas de supervisão e controle em tempo real podem parecer pequenos à primeira vista. Ataque de hackers, vírus que param um sistema supervisório ou uso indevido do sistema por pessoal da própria empresa podem também parecer muito pouco prováveis. Entretanto, como sabemos, as conseqüências de um evento causado por algum destes fatores podem ser graves e justificam esforços para investimentos em segurança.

Como visto nas seções anteriores, muita atenção tem sido dada a esta questão pela comunidade internacional ultimamente. Dadas as características particulares dos sistemas SCADA, ainda é necessário o desenvolvimento de ferramentas específicas para o setor. Mas, por outro lado, as ferramentas existentes para a segurança de redes de comunicação e sistemas de informação em geral também se aplicam a tais sistemas, ainda que não cubram todas os pontos de insegurança já identificados. Seguindo-se as recomendações de melhores práticas relativas à segurança e utilizando-se ferramentas de prateleira ou mesmo software livre, é possível dar os primeiros passos em direção a um sistema SCADA mais seguro e eliminar uma grande parte das ameaças aqui levantadas. Outros passos fundamentais são o estabelecimento de uma política de segurança bem definida e documentada para o sistema SCADA e a criação equipe responsável pela implantação e monitoramento da segurança neste ambiente.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) Byres, E., Lowe, J. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, *VDE Congress 2004*, Berlin.

(2) SQL Slammer Worm Lessons Learned For Consideration By The Electric Sector. North American Electric Reliability Council, 20 Jun 2003, Princeton.

(3) Baker, G. Cyber Terrorism a Mouse-click Away. The Age. http://www.theage.com.au/content/4/22579.html, Oct 2001, Australia

(4) Verton, D. California Hack Points to Possible IT surveillance Threat. Computerworld, 12 jun 2001. Http://www.computerworld.com/industrytopics/energy/strory/0,10801,61313,00.html.

(5) Control Center Protection Profile For Industrial Control Systems V 0.50. Digital Bond, Inc. 17 feb 2004.

(6) Risley, A. Roberts, J. LaDow, P. Electronic Security of Real-Time Protection and SCADA Comunications. 5th Annual Western Power Delivery Automation Conference, Sopkane, Washington, apr 2003.

(7) Pfleeger C.P., Pfleeger S.L. Security in Computing, 3d. Ediion, Prentice Hall, 2003, USA.

(8) Durst, R., at al. Testing and Evaluating Computer Intrusion Detection Systems. Com of the ACM, v42 n7, Jul 1999.

(9) Peterson D. Intrusion Detection and Cyber Security Monitoring of SCADA Networks. Distributech, San Diego, CA, 2005, USA.

[3] SAGE - Sistema Aberto de Gerenciamento de Energia. Solução para sistemas EMS/SCADA desenvolvida pelo CEPEL (15)

(10) Carlson, Rolf. High Security SCADA LDRD Final Report. Sandia National Laboratories, apr. 2002, Albuquerque, USA.

(11) GAO-040354. Critical Infrastructure Protection, mar 2004.

(12) Urgent Action Standard 1200. NERC, aug. 2003.

(13) Standard 1300 – Cyber Security. Draft version 1.0, NERC, sep. 2004.

(14) Katipamula, S., Hadley, M.D., McKenna, T.P. Evaluation of Symantec Products in an AREVA T&D Implemented SCADA Environment using TCP/IP Communication serves. May 2004. http://enterprisesecurity.symantec.com/Content/displaypdf.cfm?PDFID=804

(15) G.P.Azevedo, A.L. Oliveira Filho. Control Centers with Open Architectures. IEEE Computer Applications in Power, v. 14, n. 4, p. 27-32, 2001