UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
ESPECIALIZAÇÃO EM AUTOMAÇÃO INDUSTRIAL

LUIZ COSTA STREHL

PROSPECÇÃO DE TECNOLOGIAS PARA AUMENTAR A SEGURANÇA EM SISTEMAS SCADA

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2012

LUIZ COSTA STREHL

PROSPECÇÃO DE TECNOLOGIAS PARA AUMENTAR A SEGURANÇA EM SISTEMAS SCADA

Projeto de Monografia apresentado como requisito parcial para obtenção do título de Especialista em Automação Industrial, do Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Área de Concentração: Tecnologia e Desenvolvimento.

Orientador: Prof. Dr. Flávio Neves Júnior

CURITIBA
2012

RESUMO

RESUMO STREHL, Luiz C. **Prospecção de tecnologias para aumentar a segurança em sistemas SCADA**. 2012. 64 f. Monografia (Especialização em Automação Industrial) – Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2012.

Serviços essenciais para as pessoas como a eletricidade, transporte, abastecimento de água, alimentação e outros, são controlados por sistemas de supervisão e controle. A maioria das pessoas pode não conhecer a importância de tais sistemas, mas o monitoramento e o seu perfeito funcionamento garantem o bem estar, a segurança e a comodidade de todos.
A utilização de sistemas de controle e supervisão em ambientes industriais iniciou-se a partir da década de 60 e, desde então, acompanharam o crescimento e a modernização alcançada pela tecnologia computacional. As mudanças sofridas deixaram as soluções proprietárias e evoluíram para sistemas e protocolos abertos, produtos de prateleira e difusão do uso da internet nas comunicações. Criou-se, então, um ambiente com consideráveis possibilidades de ataques a esses sistemas, tornando-os vulneráveis as mesmas ameaças e riscos dessas novas tecnologias.
Entretanto, como no ambiente de Automação as prioridades não são as mesmas do ambiente de Tecnologia da Informação, é preciso entender as tecnologias, os prós e contras, antes de implementá-las.
Este projeto de dissertação tem como tema prospectar tecnologias para aumentar a segurança de sistema de controle e supervisão. Como resultado da pesquisa, um conjunto de tecnologias é selecionado para aplicação em qualquer rede industrial, independente da área de atuação da empresa.
A compreensão do que seriam sistemas de supervisão e aquisição de dados e sua evolução, as principais normas voltadas para o assunto de Segurança da Informação e principais diferenças entre os ambientes de automação industrial e TI são abordados nesse trabalho. As ameaças e vulnerabilidade que acometem nos sistemas e as principais tecnologias e contramedidas são exploradas com base na literatura pesquisada.
Com o objetivo de prover um uso prático para esta pesquisa, elaborou-se um questionário que, considerando as tecnologias e contramedidas selecionadas, também fornece insumos para que a empresa, ao utilizá-lo, obtenha uma avaliação de segurança do seu ambiente de automação industrial.
O questionário foi aplicado em 10 unidades industriais e obteve, como resultado, um panorama atual da segurança do sistema de controle de cada uma dessas unidades.

Palavras-chave: Cibersegurança. Segurança. SCADA. Redes Industriais.

ABSTRACT

RESUMO STREHL, Luiz C. **Prospecção de tecnologias para aumentar a segurança em sistemas SCADA**. 2012. 64 f. Monografia (Especialização em Automação Industrial) – Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2012.

Essential services for people such as electricity, transport, water supply, food and others are controlled by systems of supervision and control. Most people may not know the importance of such systems, but monitoring and guarantee of perfect performance take us the welfare, safety and good life.
The use of supervisory and control systems in industrial environments began from the 60s and has since followed the growth and modernization achieved by computer technology. The changes undergone have evolved to open protocols and systems, COTS products and widespread use of internet communications. Then, it was created an environment with considerable possibilities of attacks on these systems, making them vulnerable to the same threats and risks of these new technologies.
However, as the environment of Automation priorities are not the same an environment of Information Technology, one must understand the technologies, the pros and cons before implementing them.
The theme of this dissertation is to explore technologies to increase the safety system of control and supervision. As a result of the research, a set of technologies is selected for use in any industrial network, regardless of the area of operations of the company. The understanding of what would be the supervisory and data acquisition and its evolution, the main regulations to the subject of Information Security and key differences between the environments of Industrial Automation and IT are addressed in this work. The major threats and vulnerabilities that affect the systems and key technologies and countermeasures are explained on the basis of literature.
With the goal of providing a practical use for this research, a questionnaire was prepared and, considering the selected technologies and countermeasures, also provides inputs for the company, to get a security assessment of your industrial automation environment. The questionnaire was applied in 10 industrial units and obtained, as a result, a current view of system security control of each of these units.

Palavras-chave: Cibersecurity. ISA99. SCADA. Industrial network.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O capítulo primeiro desse trabalho aborda as informações referentes ao tema, delimitação da pesquisa, problemas e premissas, objetivos, justificativas e estrutura dessa monografia.

1.1 TEMA

Serviços essenciais para as pessoas como a eletricidade, transporte, abastecimento de água, alimentação, farmacêutico, comunicação, produção de combustível e outros, são controlados por sistemas de supervisão e controle de automação, normalmente categorizados como SCADA[1].

A maioria das pessoas pode não conhecer a importância de tais sistemas, mas o monitoramento e controle automático de processos industriais críticos garantem a segurança, o bem estar e a comodidade de todos.

A utilização de sistemas de controle e supervisão em ambientes industriais iniciou-se a partir da década de 60, isto só foi possível com o surgimento dos primeiros computadores da época denominados de *mainframe* (SHAW, 2006).

No início, soluções robustas que atendessem às demandas das indústrias era o foco dos fabricantes, e a tecnologia das décadas de 60, 70 e 80 era bem segura contra ataques cibernéticos por causa dos sistemas proprietários e protocolos específicos (SHAW, 2006).

Os sistemas SCADA acompanharam o crescimento e a modernização alcançada pela tecnologia computacional, e as mudanças sofridas, deixaram as soluções proprietárias e evoluíram para sistemas abertos, produtos de prateleira, comunicação Ethernet e Protocolo de Controle de Transmissão/Protocolo Internet (do inglês,

[1] SCADA cujo acrônimo é Supervisory Control and Data Acquisition System, são sistemas configuráveis, destinado à supervisão, ao controle e à aquisição de dados de plantas industriais (Moraes; Castrucci, 2007).

Transmission Control Protocol/Internet Protocol - TCP/IP), mas também os tornaram vulneráveis as mesmas ameaças e riscos dessas novas soluções (TECHNICAL INFORMATION BULLETIN 04-1, 2004).

A partir do século XXI, novas preocupações nortearam o desenvolvimento dos fabricantes, e a segurança da informação, nos seus vários aspectos, está sendo amplamente discutida no ambiente industrial, onde coexistem várias gerações de equipamentos (SHAW, 2006).

Entretanto, a segurança desses sistemas é dificultada por vários fatores. Primeiramente, aumentar a segurança requer investimentos e pesquisa, e as empresas não podem assumir esse custo. As limitações da tecnologia atual impedem a implementação de medidas de segurança, elas não são facilmente aplicáveis, os sistemas operam em tempo real e a adoção de algumas medidas pode reduzir o seu desempenho (THE WHITE HOUSE WASHINGTON, 2003, p. 47, tradução nossa).

A necessidade de proteção contra ataques nos computadores instalados no ambiente de Automação Industrial e Sistema de Controle (do inglês, Industrial Automation and Control System - IACS) tem crescido significativamente na última década. A utilização combinada de sistemas abertos, plataformas e protocolos no ambiente IACS, e o aumento de parcerias, fusões e terceirizações, tem papel principal no aumento das ameaças e na probabilidade de ataques cibernéticos (AMERICAN NATIONAL STANDARD INSTITUTE, 2007, p. 9).

Com base nesse contexto introdutório, esse trabalho aborda a evolução dos sistemas de supervisão e aquisição de dados e os aspectos tecnológicos de segurança. As principais normas existentes sobre o assunto e as principais medidas de segurança em ambientes industriais serão exploradas.

Como contribuição para o assunto, a pesquisa almeja prospectar tecnologias e medidas para aumentar a segurança de uma rede industrial com sistema SCADA, de aplicação geral e independente do ramo de atuação da empresa.

1.2 DELIMITAÇÃO DA PESQUISA

O assunto segurança da informação pode ser abordado de várias formas, desde o campo da tecnologia até o campo organizacional e político da companhia. Por sua vez, o ambiente industrial é bem complexo e, desde a sua concepção, é tarefa difícil a obtenção de uma padronização de rede (protocolos e arquitetura) e de equipamentos (*hardware e software*).

A segurança a ser aplicada no mundo industrial, será abordada nesse trabalho. Todavia, devido à complexidade do assunto e a profusão de abordagens que poderiam ser feitas, a pesquisa almeja tratar, de forma concisa, as principais tecnologias de segurança que podem ser utilizadas em ambientes industriais que possuam sistema SCADA implementado.

1.3 PROBLEMAS E PREMISSAS

O conceito de segurança cibernética como aplicado no Relatório Técnico ANSI/ISA-TR99.00.02-2007 está no mais amplo sentido possível, e abrange todos os tipos de componentes, plantas, instalações e sistemas de todas as indústrias e infraestruturas críticas (AMERICAN NATIONAL STANDARD INSTITUTE, 2007, p. 13).

Um investimento na segurança para reduzir a zero os riscos pode ser muito caro, por outro lado, um pequeno investimento pode reduzir as ameaças a um nível aceitável de probabilidade (SHAW, 2006, p. 246).

Um caso recente e emblemático foi o ataque do W32.Stuxnet*,* uma das mais complexas ameaças que se tem notícia em sistemas de controle industrial e que, quando instalado, tenta buscar estações programáveis de um fabricante específico e reprogramá-la, modificando o código do Controlador Lógico Programável (MCAFEE, 2011).

O ataque do Stuxnet infectou mais de 100.000 computadores, sendo que mais de 60% deles estava localizado no Irã (MCAFEE, 2011, p. 5).

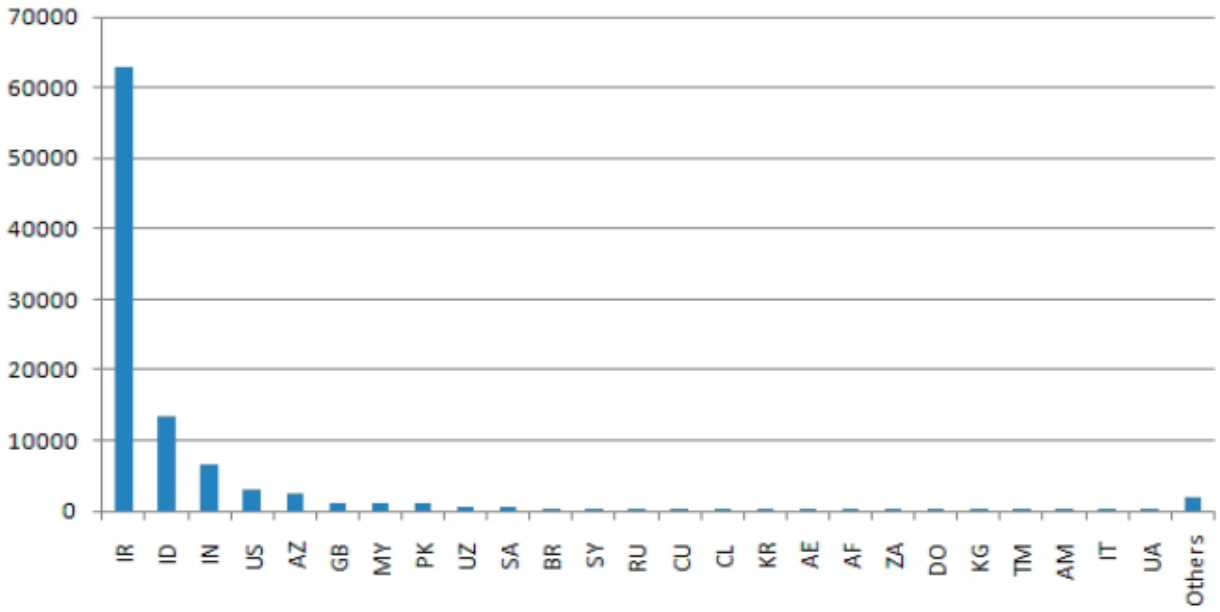

Figura 1 - Computadores infectados por país
Fonte: W32.Stuxnet Dossier (2010, p. 5).

Em um mundo globalizado e cada vez mais complexo politicamente, as indústrias precisam prever investimentos para melhorar a segurança do seu ambiente industrial. Normalmente, as tecnologias disponíveis são comparadas a uma análise custo/benefício, mas quando se fala de segurança em sistemas SCADA, que tecnologias poderiam ser elencadas? Quais as principais vantagens e desvantagens de cada uma delas?

Nesse contexto, a pergunta que norteia essa pesquisa é: Quais tecnologias podem ser implementadas em uma empresa, com sistema SCADA instalado, para aumentar a segurança?

Para esse estudo, adotar-se-á a premissa de que todas as tecnologias prospectadas contribuem para o aumento da segurança nos sistemas SCADA, e que a adoção ou não, é uma decisão que depende exclusivamente dos gestores das unidades industriais.

1.4 OBJETIVOS

1.4.1 Objetivo Geral

Prospectar tecnologias que, quando aplicadas, possam aumentar a segurança de uma rede industrial com sistema SCADA instalado.

1.4.2 Objetivo Específico

O objetivo proposto será alcançado com a abordagem aos seguintes tópicos:

a) Apresentar os componentes e a evolução do sistema SCADA;
b) Descrever o ambiente de Automação Industrial e de Tecnologia de Informação;
c) Levantar os principais requisitos de segurança em um ambiente industrial;
d) Identificar as principais tecnologias e suas ameaças e vulnerabilidades;
e) Identificar as principais contramedidas;
f) Identificar conceitos de avaliação de riscos;
g) Identificar tecnologias para aumentar a segurança de uma rede industrial com SCADA;
h) Elaborar um questionário com base nas principais tecnologias.

1.5 JUSTIFICATIVA

A infraestrutura crítica da nação é composta por instituições públicas e privadas nos setores de agricultura, alimentos, água, saúde pública, serviços emergenciais, governamentais, defesa, informação e telecomunicações, energia, transportes, bancos e finanças, química e materiais perigosos, correios e navios (THE WHITE HOUSE WASHINGTON, 2003, p. 7, tradução nossa).

O *Cyberspace* é o sistema nervoso, o sistema de controle de um país. *Cyberspace* é composto de centenas de milhares de computadores interconectados, servidores, roteadores, *switches*, e cabos de fibra ótica que permitem a infraestrutura crítica trabalhar. Dessa forma, o funcionamento saudável do *cyberspace* é essencial para a economia e segurança nacional (THE WHITE HOUSE WASHINGTON, 2003, p. 7, tradução nossa).

Infraestruturas Críticas definem, segundo o Departamento de Segurança da Informação e Comunicações Brasileiro, as instalações, serviços e bens que se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional (GABINETE DE SEGURANÇA INSTITUCIONAL, 2010b, p. 7). A interrupção da produção de uma indústria tem como consequência muito mais do que problemas financeiros e danos aos equipamentos.

Atualmente o Brasil está posicionado como líder global emergente, todavia, quando comparado a outros países, as políticas de cibersegurança são bem distintas. No relatório anual da McAfee de 2011, denominado Proteção de Infraestrutura Críticas, com destaque para empresas de energia, petróleo, gás e água, é apresentado um comparativo sobre a adoção de medidas de segurança em vários países (MCAFEE, 2011).

O Brasil foi o país que menos aplicou medidas de cibersegurança, opostamente à China, em que o governo parece desempenhar um papel agressivo ao exigir segurança de sua infraestrutura crítica (MCAFEE, 2011, p. 8).

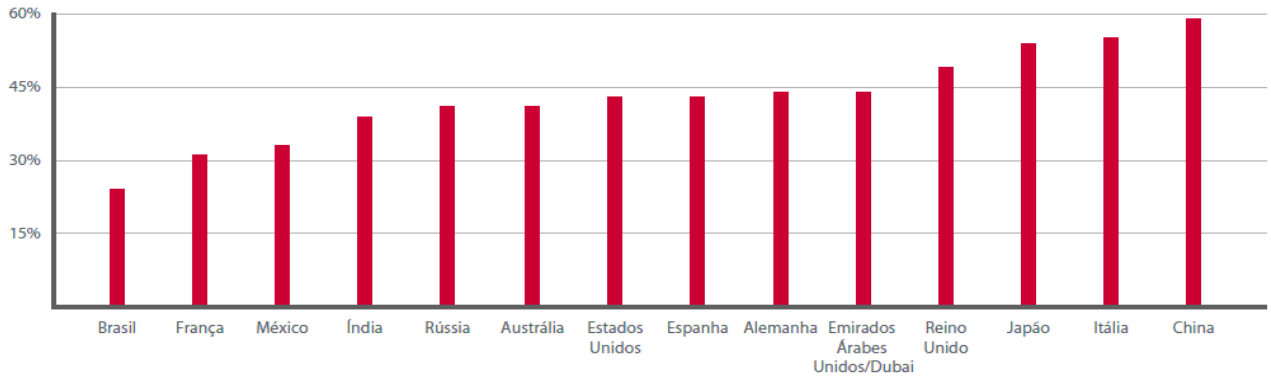

Figura 2 - Taxa de adoção de medidas de segurança relatadas por país
Fonte: Relatório McAfee (2011, p. 17).

A pesquisa se justifica, portanto, por apresentar as principais tecnologias, ora em discussão na bibliografia consultada, visando aumentar a segurança em sistemas SCADA, com possibilidade de aplicação em indústrias nacionais.

1.6 ESTRUTURA

Esta dissertação está estruturada em cinco capítulos que buscam apresentar os assuntos da pesquisa de forma gradual.

O capítulo 1 contempla a introdução com a descrição do tema, objetivos, justificativa e premissas/problemas da pesquisa.

A compreensão do que seriam sistemas de supervisão e aquisição de dados e sua evolução, as principais normas voltadas para o assunto de segurança da informação e as principais diferenças entre os ambientes de automação industrial e TI será apresentada no capítulo 2.

No capítulo 3 serão explorados as vulnerabilidades/ameaças e contramedidas, respectivamente, com foco na utilização das tecnologias existentes, e a avaliação de riscos.

As tecnologias selecionadas e a metodologia adotada para a pesquisa estão consolidadas no capítulo 4.

A conclusão e considerações finais compõe o capítulo 5, final desse trabalho.

2 SISTEMA SCADA

Neste capítulo serão apresentados os principais componentes de um SCADA e a sua evolução dividida em três gerações. As principais normas e padrões utilizados pela Segurança da Informação e as diferenças e prioridades existentes entre os ambientes de Tecnologia da Informação e o de Automação.

2.1. COMPONENTES DE UM SISTEMA SCADA

O sistema SCADA pode ser muito simples ou muito complexo, depende do porte da empresa e do escopo para qual está sendo utilizado, desde monitoramento de uma estação de medição até a distribuição da água de uma cidade. No início o SCADA se utilizava apenas de linhas telefônicas, mas hoje em dia trafega em ambientes de rede WAN/LAN (*Wide Area Network/Local Area Network*) e recentemente aproveitando-se da tecnologia *wireless* (SHAW, 2006).

As primeiras indústrias que adotaram a tecnologia SCADA foram as do ramo elétrico, entretanto, hoje elas são relutantes em adotar novas tecnologias, devido a impactos operacionais e financeiros. Muitas ainda utilizam sistemas de comunicação obsoletos (equipamentos e protocolos) por causa da grande quantidade já instalada. E mesmo, novos sistemas SCADA, podem não ser capazes de suportar a comunicação com equipamentos antigos porque os fabricantes não existem mais (SHAW, 2006).

Entre as responsabilidades do National Communications System (NCS) dos EUA está o gerenciamento do Programa Federal de Padronização das Telecomunicações, que identifica, desenvolve e coordena propostas de padronização do Governo Federal Americano. Um dos trabalhos do NCS foi o *Technical Information Bulletin 04-1* (TIB-04-1), de outubro de 2004, que apresenta uma visão geral dos sistemas SCADA.

Os componentes de um sistema SCADA, segundo TIB-04-1, deveriam consistir de:

- Equipamentos de campo: obtém os dados e transmitem para o SCADA central, normalmente RTU ou PLC;
- Sistema de comunicação: entre os equipamentos de campo e o SCADA central;
- Servidor ou servidores centrais (MTU) e
- Grupo de *software*: padrão ou não, para uso dos operadores do sistema.

2.1.1. RTUs

Os equipamentos denominados *Remote Terminal Unit* (RTU) convertem os sinais eletrônicos, recebido de outras interfaces (sensores), e transformam em uma linguagem (protocolo) para posterior envio (comunicação) para o SCADA (SHAW, 2006).

RTUs e outros equipamentos de campo se comunicam usando protocolo serial, normalmente um canal analógico ou via rede IP.

2.1.2. PLC

De acordo com o IEC 61131-1, o termo *Programmable Logic Controller* (PLC) é um sistema eletrônico de operação digital para uso em um ambiente industrial, que usa uma memória programável para armazenamento interno de instruções orientada ao usuário para implementar funções como lógicas, sequenciamento, temporização, contadores e matemáticas, para controlar através de entradas e saídas, digitais ou analógicos, vários tipos de máquinas ou processos.

Um PLC é constituído basicamente de: fonte de alimentação, UCP (unidade central de processamento), memórias do tipo fixo e volátil, dispositivos de entrada e saída e terminal de programação (MORAES; CASTRUCCI, 2007).

Usado para monitoramento e controle nas mais diversas indústrias, o PLC pode enviar dados para o SCADA e atuar sozinho (*stand-alone*) conforme configurações.

O SCADA nasceu com as aplicações de telemetria, recebendo e trabalhando as informações originárias das unidades remotas. O PLC é originário da indústria da automação e evoluiu controlando e atuando na origem do dado, disponibilizando por tanto, poucos protocolos de comunicação quando comparados às RTUs instaladas no campo (SHAW, 2006).

2.1.3. MTU

Segundo Boyer (2004), no centro de cada sistema SCADA está o equipamento que lança todos os comandos, agrupa todos os dados, armazena algumas informações, passa outras para os sistemas associados, faz a interface com as pessoas que operam o processo. Este equipamento é o *Master Terminal Unit* (MTU), também chamado de *host computer* em algumas indústrias.

2.1.4. IHM

Segundo Moraes e Castrucci (2007), sistemas supervisórios poderiam ser divididos em dois grandes grupos SCADA e IHM (interface homem máquina). Uma IHM é um *hardware* industrial composto normalmente por uma tela de cristal líquido e um conjunto de teclas pra navegação, ou inserção de dados, que utiliza um *software* proprietário para sua programação. Com base nessa visão, sistemas constituídos por IHM e RTU inteligente, com funcionalidades iguais a de um PLC, podem ser considerados um sistema SCADA.

2.2. EVOLUÇÃO DE SISTEMAS SCADA

De acordo com o TIB-04-1, os sistemas SCADA acompanharam a evolução da tecnologia computacional, e podem ser divididos em três gerações:

- 1ª Geração – Sistemas Monolíticos;
- 2ª Geração – Sistemas Distribuídos;
- 3ª Geração - Sistemas em Rede.

2.2.1. 1ª Geração – Sistemas Monolíticos

Na época do desenvolvimento dos primeiros sistemas SCADA, a tecnologia dominante eram os sistemas do tipo *mainframe*, e os sistemas SCADA eram basicamente *stand-alone*, sem conectividade com outros sistemas (TECHNICAL INFORMATION BULLETIN 04-1, 2004, p.10).

As comunicações eram, em sua maioria, proprietárias e desenvolvidas pelos fabricantes de equipamentos de campo (RTU), que se limitava a enviar os dados para o SCADA. O meio físico de acesso utilizava-se de linhas telefônicas (*dial-in*) disponíveis na época (SHAW, 2006).

Para contornar falhas, utilizava-se o processo de redundância *stand-by*, segundo Moraes e Castrucci (2007), redundância *stand-by* configura-se mediante dois subsistemas idênticos, mas em cada momento somente um deles está ligado à saída através de chave seletora.

Nessa época não havia uma preocupação em proteger sistemas contra ataques, e os engenheiros se concentravam em resolver os problemas e erros do sistema, torná-los redundantes, robustos e capazes de operar ininterruptamente ou parcialmente, com aceitáveis e controlados níveis de falhas e degradação (SHAW, 2006).

A figura 3 apresenta a arquitetura da 1ª Geração, e a comunicação *Wide Area Network* (WAN) era feita por linhas telefônicas sujeitas às falhas e intempéries associadas a esse meio físico.

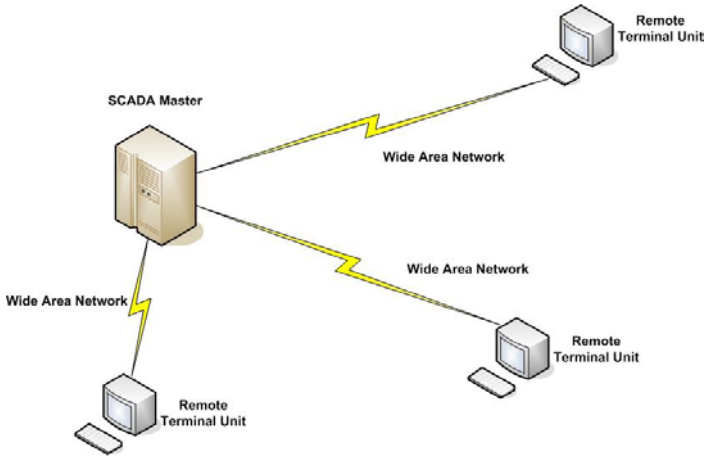

Figura 3 - 1ª Geração da arquitetura SCADA
Fonte: TECHNICAL INFORMATION BULLETIN 04-1 (2004, pág. 11).

2.2.2. 2ª Geração – Sistemas Distribuídos

Com a difusão dos computadores e das redes *Local Area Network* (LAN), os equipamentos passaram a rodar em rede, e a redundância pode ser feita pelo uso de outro equipamento, sem a necessidade de chaveamento entre *primary/stand-by*. Essa geração também estava marcada pela dependência dos fornecedores, quanto aos protocolos, e limitada pelas tecnologias de *hardware* e *software* difundidas na época (TECHNICAL INFORMATION BULLETIN 04-1, 2004).

A 2ª Geração, como apresentado na figura 4, reflete o desenvolvimento da arquitetura mediante utilização da rede LAN para estruturar o funcionamento do SCADA.

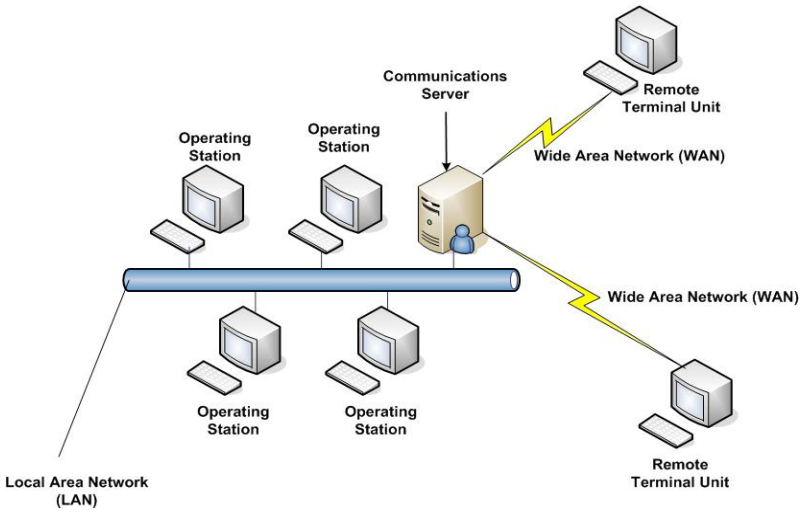

Figura 4 - 2ª Geração da arquitetura SCADA
Fonte: TECHNICAL INFORMATION BULLETIN 04-1 (2004, pág. 12).

A tecnologia SCADA utilizada na 1ª Geração e 2ª Geração era bem segura contra ataques cibernéticos por causa dos sistemas proprietários e protocolos específicos, além da incapacidade de conectividade, interoperabilidade e compatibilidade com os demais sistemas da época (TECHNICAL INFORMATION BULLETIN 04-1, 2004).

2.2.3. 3ª Geração – Sistema em Rede

O marco da 3ª geração foi a utilização de arquitetura aberta, com a utilização de protocolos e padrões abertos de comunicação, desta forma, a utilização do SCADA alcançava ambientes LAN e WAN (TECHNICAL INFORMATION BULLETIN 04-1, 2004).

Com a abertura surgiram novos fornecedores que podiam concorrer para a prestação de serviços e comercialização dos produtos, que passariam a ser considerados de prateleira. As soluções de *hardware* e *software* da área de Tecnologia da Informação (TI) foram facilmente adotadas para sistemas SCADA, e os especialistas em SCADA não se preocupavam com o desenvolvimento de Sistemas Operacionais nem *hardware* específico, podendo se concentrar em melhorar as funcionalidades do seu produto (SHAW, 2006).

A figura 5 apresenta a utilização da nuvem no ambiente de automação, sendo o SCADA um dos protagonistas dessa evolução.

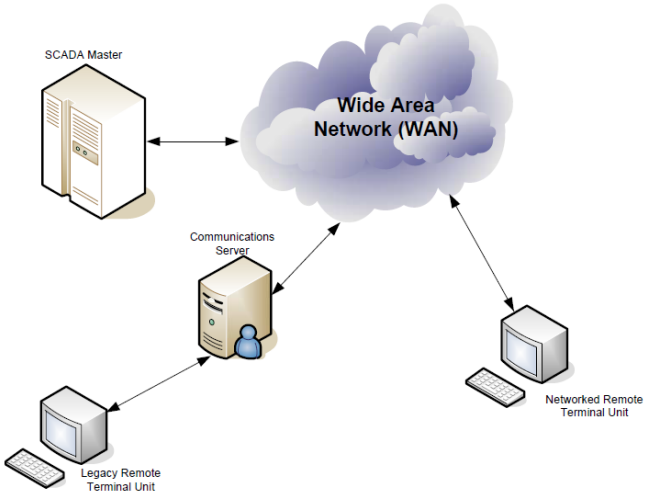

Figura 5 - 3ª Geração da arquitetura SCADA
Fonte: TIB-04-1 (2004, pág. 13).

Desde então, sistemas SCADA passaram a usufruir as benesses da TI e, em contrapartida, de todos os seus problemas. Pouca atenção tinha sido dada aos riscos de segurança, uma vez que se acreditava que estas redes eram praticamente imunes a *cyber* ataques.

2.3. SEGURANÇA DA INFORMAÇÃO

2.3.1. Normas e Padrões

O desenvolvimento de padrões de segurança da informação, em níveis internacionais, envolve o International Organization for Standardization (ISO) e o International Electronics Consortium (IEC). Embora outros corpos forneçam padrões específicos, eles são geralmente derivados ou referem-se ao padrão ISO (BLANDING, 2011).

Nos EUA, os padrões internacionais de segurança da informação são apoiados pelo American National Standards Institute (ANSI) e International Committee for Information Technology Standards (INCITS) (BLANDING, 2011).

Os padrões ISO/IEC 17799 e ISO/IEC 27001 são excelentes para descrever sistemas de gerenciamento de *cybersecurity* para sistemas de informação utilizados em áreas de negócios (ambiente corporativo), e muito do conteúdo desse padrão é aplicado ao Industrial Automation and Control System (IACS) (AMERICAN NATIONAL STANDARD INSTITUTE, 2009).

Para balizar a implantação de soluções de segurança em redes de automação, a Instruments, Systems, and Automation Society (ISA), formalmente Instrument Society of America lançou, em 2004, a primeira versão da norma ANSI/ISA-99 Integrating Electronic Security into the Manufacturing and Control Systems Environment*,* e desde então, a adequação a esta norma tem se difundido para as infraestruturas consideradas críticas (SHAW, 2006).

A ISA desenvolve guias para melhorar a segurança dos sistemas de automação, inclusos SCADA, DCS e PLCs. Como parte desse esforço, especialistas e empresas do ramo contribuíram para a criação do relatório técnico ANSI/ISA-TR99.00.02-2004, que apresenta um conjunto de recomendações sobre as principais tecnologias utilizadas (AMERICAN NATIONAL STANDARD, 2009).

O padrão ANSI/ISA–99.02.01–2009 enfatiza a necessidade de consistência entre as práticas para gerenciar uma segurança do ambiente IACS com as práticas de gerenciar em sistemas de TI e de negócio (AMERICAN NATIONAL STANDARD INSTITUTE, 2009).

Atualmente as normas ISA99 incluem os seguintes documentos:

- **ANSI/ISA–99.01.01–2007** – Terminologia, conceitos e modelos;
- **ANSI/ISA–TR99.01.02–2007** – Tecnologias de Segurança para Automação Industrial e Sistemas de Controle;
- **ANSI/ISA–99.02.01–2009** – Estabelecendo um Programa de Segurança de Automação Industrial e Sistema de Controle;
- **ISA–99.02.02** – (em desenvolvimento) – Operando um Programa de Segurança de Automação Industrial e Sistema de Controle;

- **ISA–99.03.xx** – Requisitos Técnicos de Segurança para Automação Industrial e Sistema de Controle.

Muitas organizações, preocupadas com cibersegurança, estabeleceram programas para implementar Sistemas de Gerenciamento em Cibersegurança (do inglês, Cyber Security Management Systems - CSMS) como definido pelo ISO/IEC 17799 e ISO/IEC 27001, desta maneira, as organizações seguem um método de proteção dos seus ativos (AMERICAN NATIONAL STANDARD INSTITUTE 99.02.01, 2009, p.11).

A North American Electric Reliability Council (NERC), em cooperação com organizações governamentais e laboratórios (ex.: National Institute of Standars and Technology) iniciou o desenvolvimento de recomendações e padrões para fazer os sistemas SCADA, e infraestruturas do sistema elétrico, mais seguros contra ameaças terroristas, *cyber* e físicas. NERC trabalhou nas edições dos documentos Critical Infrastructure Protection, CIP-002-1 até CIP-009-1, considerando aspectos das utilidades elétricas e a confiabilidade das redes, embora outras agências e organizações também contribuíram com recomendações similares para outros segmentos industriais (SHAW, 2006, pág. 353).

No setor de óleo e gás, a American Petroleum Institute (API) publicou o documento: Padrão 1164, em setembro 2004, para segurança em gasodutos e oleodutos gerenciados por meio de sistemas SCADA.

A mais recente recomendação internacional sobre o tema foi divulgada em junho de 2011, o *Special Publication 800-32 Guide to Industrial Control Systems Security* pelo National Institute of Standars and Technology (NIST).

No âmbito de iniciativas nacionais, o Gabinete de Segurança Institucional, ligado a Presidência da República, disponibiliza documentos que podem ser utilizados como referência para tratamento da Segurança das Infraestruturas Críticas. O documento intitulado: Livro Verde Segurança Cibernética no Brasil, 2010, apresenta uma breve visão do país em alguns vetores nacionais (Político, Econômico, Social, etc.) e algumas diretrizes a serem contempladas na política nacional de segurança cibernética. O documento: Guia de Referência para a Segurança das Infraestruturas Críticas da Informação, 2010, reúne várias informações técnicas, requisitos mínimos de segurança e metodologias para mapear os ativos de informação, analisar ameaças e gerar alertas.

Empresas procuram adequar as normas ao seu perfil de negócio e infraestrutura existente, como é o caso da American Gas Association (AGA), que propôs um algoritmo de encriptação para integração de protocolos seriais. O Relatório AGA número 12 denominado Proteção Criptográfica para Comunicação SCADA - Recomendações Gerais, trata do assunto de segurança em canais de comunicação do sistema SCADA, entre o servidor central e as remotas em campo (SHAW, 2006 e TEUMIM, 2005).

No trabalho *A Holistic SCADA Security standard for the Australian Context* de Christopher Beggs (2008), verifica-se que os padrões e normas disponíveis, de certa forma, possuem o foco em setores específicos, e não necessariamente fornece uma compreensão ou entendimento holístico da segurança SCADA. Há muitos padrões que não são usados ou estão limitados de acordo com o setor ou organização onde o sistema de supervisão e controle está inserido. O autor cita que sistemas do setor de ferrovias são, ultimamente, diferentes dos utilizados em setores de abastecimento de água. Existem diferentes regulações e regras para cada infraestrutura, e desta forma, a montagem do SCADA deve seguir ou respeitar essas regras de negócio. A sugestão do trabalho é que cada padrão deve cobrir todos os aspectos da segurança do seu setor, mas com algumas similaridades com os demais. O autor propõe o uso de um SCADA holístico por setor específico, o que possibilitaria que a organização, e o seu processo, pudessem implementá-lo com relativa facilidade.

2.3.2. Disponibilidade, Integridade e Confidencialidade

No ambiente de TI, quando se discute cibersegurança, geralmente fala-se de um grupo de tecnologias e arquiteturas, políticas e procedimentos para garantir a tríade Confidencialidade-Integridade-Disponibilidade - CIA (AMERICAN NACIONAL STANDARD INSTITUTE, 2007).

No ambiente de controle, a prioridade é diferente, a primeira preocupação é manter disponíveis os componentes do sistema, integridade vem em segundo e confidencialidade fica por último, conforme representado na figura 6.

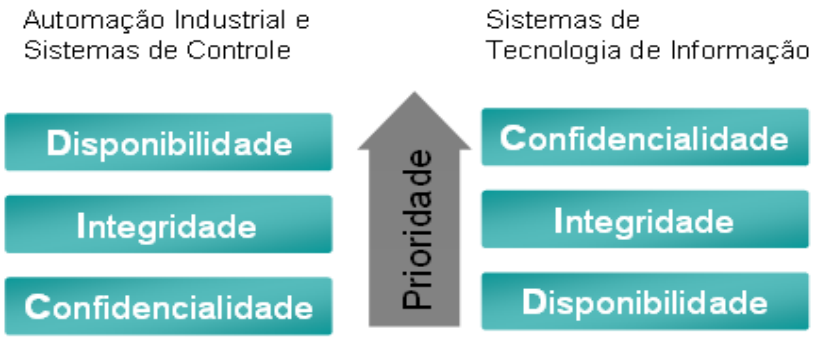

Figura 6 – Disponibilidade, integridade e confidencialidade
Fonte: Adaptado pelo autor, baseado em ANSI/ISA-99.00.01 (2007, pág. 36).

Obviamente, em certas indústrias e cenários, a prioridade pode ser diferente, e a organização deve priorizar medidas de segurança que primeiramente atendam as suas prioridades.

Historicamente, a confidencialidade recebeu mais atenção, provavelmente por causa da sua importância para os militares e governos. Como resultado, a confidencialidade está mais avançada em sistemas de computadores do que as outras duas (TIPTON, 2011, pág. 1556-1562).

A segurança da informação, em um contexto geral, pode ser definida como a preservação da confidencialidade, integridade e disponibilidade da informação, em adição, outras propriedades como autenticidade, responsabilidade, não-repúdio e confiabilidade também podem ser envolvidas (INTERNATION STANDARD IEC 17799, 2005).

Para entender melhor a tríade CIA, a ISA-99.00.01-2007 (pág. 37) define sete requisitos fundamentais de segurança que devem ser identificados no ambiente de segurança industrial:

- Controle de acesso (AC) – controle de acesso ou informações de equipamentos, para proteção contra acesso não autorizados ao equipamento ou a informação;
- Controle do uso (UC) – controle do uso dos equipamentos ou informação para proteção contra operação não autorizada do equipamento ou uso da informação;

- Integridade de dados (DI) – garantir a integridade dos dados nos canais de comunicação para proteger mudanças não autorizadas;
- Confidencialidade de dados (DC) – garantir a confidencialidade do dado no canal de comunicação para proteção contra escutas não autorizadas;
- Restrição ao fluxo de dados (RDF) – restrição do fluxo de dados no canal de comunicação para proteção contra a publicação da informação por fontes não autorizadas;
- Tempo de resposta oportuno (TER) – responder as violações de segurança notificando a autoridade apropriada, relatando necessidades de evidência jurídicas da violação, e automaticamente tomando ações corretivas, seja da forma de missão crítica ou situações críticas de segurança;
- Disponibilidade dos recursos (RA) – garantir a disponibilidade de todos os recursos da rede para proteção contra ataques do tipo Negação de Serviço (do inglês, *Denial of Service* - DoS).

As tecnologias de segurança que podem ser utilizadas nos ambientes de automação, abordadas no Capítulo 3 – Ameaças e Vulnerabilidades, atendem a um ou mais requisitos fundamentais de segurança.

2.4. AUTOMAÇÃO INDUSTRIAL E TI

Segundo a norma ANSI/ISA-99.00.01-2007, automação industrial e controle incluem os componentes de controle dos supervisórios tipicamente encontrados em processos industriais. Também incluem sistemas SCADA que operam em infraestrutura crítica das indústrias como: transmissão e distribuição de eletricidade, rede de distribuição de gás e água, operação da produção de óleo e gás e transmissões de gases e líquidos em tubulações. Operando em um ambiente complexo, e uma vez conectado ao processo industrial, a perda das informações trafegadas podem acarretar perdas de vida, produção, risco ambiental, violação de leis regulatórias e degradar, de várias outras formas, a empresa e a nação.

Atualmente a arquitetura de um SCADA é semelhante a qualquer sistema de TI, utilizam processadores INTEL ou compatíveis, arquitetura cliente-servidor, comunicação via TCP/IP, normalmente redundante, meio físico Ethernet, sistemas operacionais da Microsoft ou Linux/Unix, banco de dados comerciais (Oracle, Plant Information ou SyBase) como base de dados histórica e as IHM são micros comuns do tipo PC ou *workstations*, além de outras tecnologias comuns aos sistemas de TI (SHAW, 2006).

Com o incremento do uso das redes, da difusão da internet e da padronização de algumas soluções de *hardware* e *software*, criou-se um ambiente com consideráveis possibilidades de ataques virtuais aos sistemas de TI e, consequentemente, aos sistemas SCADA. Sistemas como DCS, SCADA, PLCs e outros sistemas de controle são utilizados por décadas em plantas industriais, e o interesse dos *hackers* tem se comprovado com o incremento dos ataques após 2001.

A figura 7 pretende exemplificar o vertiginoso aumento dos ataques por meio de conexões pela internet, o gráfico foi elaborado pelo Grupo de Resposta a Incidentes de Segurança para a internet brasileira (CERT.BR).

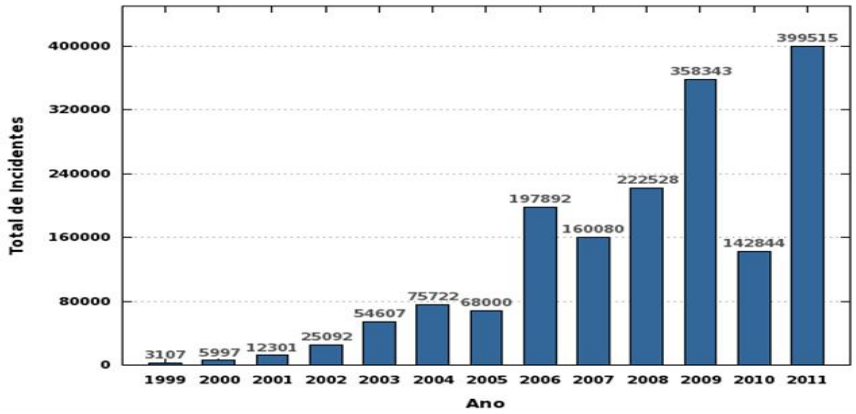

Figura 7 – Incidentes reportados por ano
Fonte: CERT.br

Em grandes organizações o departamento de TI cuida da segurança: *firewall*, servidores, *sites* e a rede da empresa (LAN/WAN). Em casos onde o departamento de TI não exista, ou é bem pequeno, os requisitos de segurança do sistema SCADA recaem sobre o pessoal de operação que, na maioria das vezes, consultam o suporte do fornecedor ou fabricante (SHAW, 2006).

A maioria dos funcionários da área de TI não conhece, ou vivenciam, a cultura operacional associada ao uso de sistemas de automação, e soluções que funcionam bem no mundo TI podem ser incompatíveis com o sistema SCADA (ISA-99, 2007 e SHAW, 2006). Por exemplo, a troca de mensagens entre dois servidores para tornar a comunicação mais segura (tecnologia de encriptação capítulo 3.1.4) pode causar um atraso numa comunicação RTU => SCADA, que poderia ser inaceitável dependendo do processo em curso. Dificilmente estruturas analógicas e tecnologias de comunicação antigas são estudadas numa área que trabalha, quase sempre, na busca por solução "estado da arte", como é a área de TI.

Equipamentos e soluções de segurança no mundo TI (*firewall*, sistema operacional, certificados digitais, IDS, servidores, etc) precisam estar sempre sendo atualizados com *updates*, *patches* e suporte constante para garantir a sua funcionalidade.

É difícil para o mercado de automação, com tempo médio de amortização do investimento entre 10 e 20 anos, acompanhar a evolução dos processadores, que pela conhecida Lei de Moore dobraria o seu poder de processamento em 18 meses. Sendo assim, não é raro encontrar versões antigas de microprocessadores (486, 386) e de sistemas operacionais em funcionamento nesses ambientes (SHAW, 2006).

O sistema de controle do ônibus especial da NASA e do Controle de Tráfego Americano (FAA) estão obsoletos por décadas porque é muito caro e complexo a sua atualização (DICKMAN, 2009).

No ambiente industrial, o uso de soluções comerciais, desenvolvidas no ambiente de TI para sistemas administrativos, tem possibilitado o crescimento de ataques contra seus equipamentos. O uso de soluções de TI traz vantagens financeiras, entretanto, sem compreender bem as consequências, pode implicar também em prejuízos (AMERICAN NATIONAL STANDARD INSTITUTE, 2009).

Devem-se separar práticas e soluções clássicas do ambiente de TI, daquelas que podem ser utilizadas num ambiente de operação e sistema de controle. Pode-se citar como principais diferenças entre os ambientes de automação e de TI segundo a ISA-99:

- Os riscos na automação incluem perda de vidas, plantas e equipamentos, coloca em perigo a população e/ou sua saúde;

- Não se protege a informação diretamente no ambiente de automação, e sim o processo e a planta. Conforme a arquitetura, equipamentos como PLC e RTU são mais críticos do que o SCADA;
- Sistemas de automação necessitam de alta disponibilidade;
- Sistemas de controle envolvem tempo de resposta que pode ser crítico e procedimentos que incluam atrasos podem ser degradantes (ex.: senha em PLC);
- A comunicação na automação pode envolver rede e protocolos proprietários, não baseados em IP, e ferramentas usuais de TI são ineficientes;
- Integridade da informação pode ser mais crítica no sistema de controle, porque um valor ruim pode causar um desajuste ou desarme de equipamentos;
- Manutenção no *software* e mudanças no gerenciamento do ambiente de automação devem envolver o fornecedor do sistema, as empresas devem utilizar apenas *software* testado e homologado pelo fornecedor;

De maneira geral, as diferenças entre os dois ambientes concentram-se no gerenciamento de riscos, nos requisitos de desempenho e na disponibilidade das informações.

3 AMEAÇAS E VULNERABILIDADES

Em resposta ao 11/09, os Estados Unidos da América formaram o Department of Homeland Security (DHS), com a responsabilidade de proteger os americanos de pessoas e organizações “más”. Um dos resultados recentes foi reconhecer que sistemas SCADA, DCS e PLC, amplamente usados nos EUA, não tinham mecanismos de proteção intrínsecos (SHAW, 2006).

Todo negócio ou sistema, seja de TI ou de Automação, está sujeito a ameaças e vulnerabilidades.

Uma ameaça é a ação potencialmente danosa, intencional ou não, ou capacidade, interna ou externa, para contrariamente impactar através de uma vulnerabilidade (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2006).

Uma ameaça sem uma vulnerabilidade relevante não coloca a organização em risco (LAYTON, 2007).

Vulnerabilidade é a falha ou fraqueza em um sistema, implementação, operação ou gerenciamento que pode ser explorada para violar a integridade do sistema ou política de segurança (AMERICAN NATIONAL STANDARD INSTITUTE, 2007, pág. 31).

O ciclo de vida de uma vulnerabilidade, conforme apresentado na figura 8, pode ser resumido em quatro etapas: descoberta da vulnerabilidade, anúncio da vulnerabilidade, popularização e emissão de correções pelo fornecedor (TEUMIM, 2005).

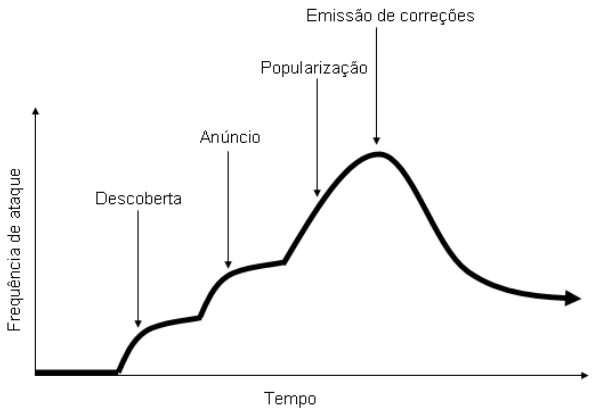

Figura 8 – Ciclo de vida das vulnerabilidades
Fonte: Traduzido pelo autor, baseado em Teumim (2005, pág. 6).

3.1. AMEAÇAS E VULNERABILIDADES DE SISTEMAS SCADA

O sistema SCADA está sujeito às vulnerabilidades convencionais do ambiente de TI quando se utiliza de soluções de *hardware* e *software* de prateleira, denominadas de soluções COTS (*Comercial-Off-The-Shelf*), e também as inerentes do processo a que esteja inserido e/ou controlando.

Para Teumim (2005), o movimento para soluções COTS em redes industriais proporciona algumas vantagens: padronização, compatibilidade com sistemas administrativos, custos menores, interfaces conhecidas e menos tempo e esforço em treinamento. Em contrapartida também existem desvantagens: atualizações forçadas no *software* sobre um ciclo de vida muito rápido, milhões de linhas extras de código para facilidades que podem não ser necessárias em aplicações industriais, grande número de lançamentos e a necessidade contínua de instalar *patches* de segurança.

O estudo das atuais tecnologias revelam as ameaças e vulnerabilidades que os sistemas SCADA estão submetidos. Este capítulo explora, com aderência ao Relatório Técnico 99.00.01-2007 preparado pela ISA-99, algumas tecnologias de segurança que podem ser utilizadas num ambiente de automação e suas principais vulnerabilidades.

3.1.1. Autenticação e Autorização

O processo de autenticação e autorização determina quem – autentica - e o que pode ser permitido – autoriza - dentro do sistema.

A autenticação pode ser considerada a primeira proteção dos ativos críticos de um sistema de controle e supervisão (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

Os principais tipos de tecnologias de autenticação e autorização são: senhas, físico (ex.: *token*), cartão inteligente, controle de acesso baseado na função (do inglês, *Role-Based Access Control* – RBAC), desafio/resposta, biométrica, localização base e equipamento-para-equipamento.

A autenticação por meio de senhas é amplamente utilizada, e as senhas podem variar em caracteres (letras e/ou números) e tamanhos (poucos caracteres até uma longa sequencia ex.: *passphrase*). A preocupação, num ambiente industrial, reside nas situações críticas, onde a intervenção humana é iminente e não há tempo para esquecimento de senha pelos operadores (AMERICAN NATIONAL STANDARD INSTITUTE ISA-TR99.00.01, 2007, pág. 26).

Para melhorar a segurança, a utilização de senhas exige um processo periódico de renovação. De acordo com um grande fabricante de PLC, a maioria dos produtos que são vendidos possuem serviços pela internet habilitados. Uma pesquisa indicou que 13% dos seus clientes configuraram e usaram esses serviços, e que os 87% deixaram os serviços pela internet ativos com a senha padrão de fábrica, como por exemplo: 1111 (TURK, 2005).

Autenticação física é similar ao conceito de senha, entretanto, utiliza-se de um equipamento denominado *token* que fica em poder do usuário. O uso dessa tecnologia tem potencial para ter um papel importante num ambiente industrial.

Os cartões inteligentes são similares aos *tokens*, com a vantagem de tirar proveito do seu formato para prover outras funcionalidades (ex.: acessos a edificações, salas ou como identidade dentro da companhia).

O uso de ferramentas gráficas para gerenciar o acesso aos usuários, considerando regras, hierarquias e níveis de acesso define a tecnologia RBAC. Devido à necessidade de centralização e uniformização numa única ferramenta, e dado o mix de fabricantes encontrados num ambiente industrial, o seu uso ainda não está muito difundido (AMERICAN NATIONAL STANDARD INSTITUTE ISA-TR99.00.01, 2007, pág. 24).

Autenticação desafio/resposta melhora a segurança da tecnologia por meio de senhas, acrescentando um código secreto entre o requisitante e o provedor do serviço. Quando o serviço é requisitado, o provedor envia um número aleatório ou *string* com um desafio para o requisitante, e o requisitante usa esse código secreto para gerar uma resposta única para o provedor. Apesar de incrementar a segurança essa tecnologia pode trazer latência ao sistema de controle.

Autenticação biométrica compara alguma característica biológica singular da pessoa que requisita o acesso para proceder à autenticação. Os principais meios

biométricos incluem: impressão digital, geometria facial, identificação da retina e íris, padrões de voz, padrões digitais e geometria da mão.

A autenticação baseada na localização utiliza-se de sistemas GPS e endereços IP para validar o acesso. A localização física do equipamento, ou da pessoa que requisita o acesso, pode validar a autenticação. Em ambientes de segurança com redes sem fio é de grande potencial de uso.

A tecnologia equipamento-para-equipamento tenciona garantir que o dado transmitido não sofra alterações entre os equipamentos, privilegiando a integridade do dado. Assim como apresentado na figura 6 (capítulo 2.3.2), a integridade dos dados em comunicações industriais, na maioria das empresas, é mais importante do que a confidencialidade.

Pode-se concluir que, as tecnologias de autenticação e autorização disponíveis tornaram-se uma boa solução para incrementar a segurança dos ambientes industriais, desde que, bem utilizadas e configuradas.

3.1.2. Controle de Acesso, Filtros e Bloqueios

Tecnologias de filtro e bloqueio são construídas para regular e direcionar o fluxo de informação entre equipamentos ou sistemas, dado que a autorização tenha sido concedida. As redes virtuais e os equipamentos denominados de *firewall* se enquadram nessa tecnologia.

O uso de redes virtuais, comumente conhecidas como VLAN (do inglês, *Virtual Local Area Network*), segrega as redes físicas em pequenas redes lógicas visando melhorar o desempenho, o gerenciamento e a segurança. Uma VLAN, quando bem configurada, pode ainda segregar tráfegos e mitigar os riscos resultantes de *scanning* de portas ou atividade de vírus (AMERICAN NATIONAL STANDARD INSTITUTE ISA-TR99.00.01, 2007).

Há vasta literatura técnica na TI sobre *firewall*, e pode-se citar três classes gerais de funcionamento: filtro de pacote, inspeção de estado e aplicação *proxy*.

- Filtro de pacote: analisa o endereço da informação de cada pacote de dado e permite, ou nega, passagem baseado num grupo de critérios pré-estabelecidos;
- Inspeção de estado: filtra pacotes nas camadas de rede, determina se o pacote da sessão é legítimo e avalia o conteúdo dos pacotes na camada de aplicação;
- Aplicação *proxy*: examina os pacotes da camada de aplicação e filtra o tráfego baseado nas regras especificas da aplicação, como as aplicações específicas (ex.: navegadores) ou protocolos (ex.: FTP).

É sabido da importância de se ter *firewall* separando a rede administrativa da internet, no entanto, é mais importante ainda ter um entre a rede administrativa e a rede industrial. Adicionalmente, como boa prática, cria-se uma zona desmilitarizada (do inglês, *Demilitarized Zone* - DMZ) para acomodar os servidores dos sistemas de controle e servidores que se comunicam com o mundo externo – internet (AMERICAN NATIONAL STANDARD INSTITUTE, 2009).

A figura 9 apresenta a arquitetura modelo, com *firewall* e DMZ, para incrementar a segurança.

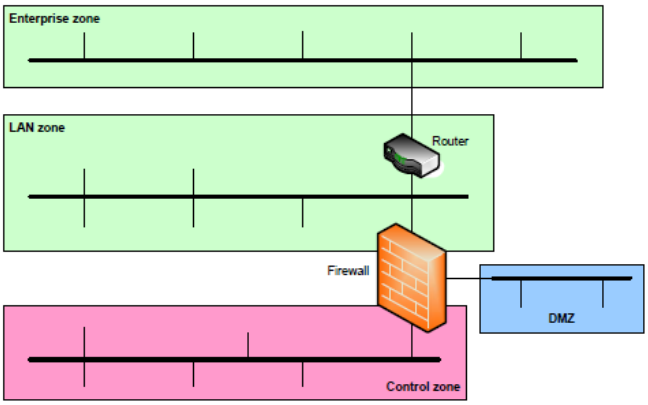

Figura 9 – Zona desmilitarizada
Fonte: American National Standard Institute ISA-99.02.01 (2009, pág. 125).

Firewall é um equipamento originário do ambiente de TI, sendo assim, utiliza-se de alguns conceitos como manutenção, configuração e atualizações de *patches* desse

ambiente, acrescenta-se que se tornou um equipamento complexo que permite inúmeras configurações, o que torna difícil o ajuste do filtro visando uma segurança ótima num ambiente de rede industrial (SHAW, 2006).

O conceito de *firewall* industrial, ou de controle, pressupõe que estes compreendam os protocolos utilizados no ambiente industrial, ou que, possuam tecnologias de inspeção profunda em pacotes. Fabricantes comercializam equipamentos que controlam até a camada sete (aplicação) do modelo OSI (*Open Systems Interconnection*), e alguns possuem a funcionalidade de mapear regras automaticamente. Funcionam durante um tempo determinado (ex.: uma semana), aprendendo o funcionamento da rede e, automaticamente, aplicam as regras necessárias para que, após confirmação do usuário, a configuração seja concluída (SHAW, 2006).

Firewall que roda diretamente nos computadores (*software*) é raro em ambientes industriais, e os fornecedores geralmente proíbem o seu uso visando manter a garantia do produto ou porque podem comprometer a operação normal.

Há a concepção errada de que redes industriais permanecem independentes da rede de TI, ou que um *firewall* de TI seja suficiente para garantir a segurança. Ter apenas um *firewall* como conexão de toda a rede de produção da empresa é uma proteção insuficiente (DICKMAN, 2009).

Obviamente um *firewall* não irá proteger o sistema SCADA de comunicações seriais, por exemplo, via protocolo MODBUS ou PROFIBUS, todavia, um *hacker* não poderá utilizar essa comunicação para realizar ataques convencionais. Não se deve descartar o risco de ataques em comunicações seriais, entretanto, a alteração dos dados ou do controle visando causar danos, normalmente, é feita por pessoas de dentro (SHAW, 2006).

3.1.3. Segurança Física

Controle de segurança física é qualquer medida física, seja ativa ou passiva, que limite o acesso físico a qualquer informação dos ativos no ambiente de automação. É a principal defesa para prevenir acessos não autorizados, destruição das informações e dos

ativos. Citam-se os sistemas de monitoramento de acesso: vídeo câmeras e sensores, e os sistemas de limitação de acesso: portas, cercas, muros, guardas, etc (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

O Relatório Técnico da ISA-99 inclui a segurança pessoal, ou seja, reduzir riscos causados pelas pessoas, erros intencionais ou não, roubos, fraudes ou usos inapropriados das informações. Uma maneira de se reduzir esses riscos é instalar um programa de segurança pessoal, que incluiria políticas de contratação e práticas para os empregados, contratados e temporários.

Uma boa solução de segurança, utilizada em estratégias militares, é a separação de tarefas, onde somente quando houver concordância de duas pessoas é que o evento será autorizado.

Como boa prática, devem-se fazer checagens periódicas nas pessoas que possuem acesso, a altos níveis de permissão, e estabelecer um perímetro de segurança física em torno dos sistemas críticos. Este perímetro nem sempre é fácil de ser feito, ainda mais quando é necessário envolver códigos de acesso, guardas, câmeras e outros artifícios, entretanto, é relevante que haja a preocupação em se manter um mínimo de segurança física, uma “barreira” entre os sistemas críticos (SCADA) e pessoas não autorizadas (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

Hoje em dia, é possível transportar uma quantidade enorme de dados (arquivos e programas completos) em *pen-drive*, CD/DVD, *laptop*, PDA, celulares, MP3 *player* e câmeras digitais, etc. O transporte manual de dados em mídia eletrônica removível, de um computador para outro, é denominado de *sneakernet*, que intencionalmente ou não, representa uma brecha na segurança (SHAW, 2006).

Tradicionalmente, os operadores são considerados confiáveis, e de certo modo, toda a segurança está fundamentada nessa veracidade. Mas, dependendo da área de atuação da empresa, essa tradição pode ser questionada.

Os programas mais prejudiciais, que são capazes de paralisar os sistemas de automação, são frequentemente introduzidos internamente. Pesquisas revelaram que aproximadamente 40% dos incidentes envolveram pessoas de dentro da companhia (RICHARDSON, 2007).

No trabalho *Guidelines for the Physical Security of Water Utilities* da American Society of Civil Engineers (ASCE) e American Water Works Association (AWWA) de 2006,

o objetivo é aplicar segurança física em unidades de fonte de águas potáveis, tratamento e sistema de distribuição. Os riscos, nesse ambiente, foram classificados em quatro elementos: vândalos, criminosos, sabotadores e pessoas de dentro (empregados, fornecedores, contratados, entregadores...). A preocupação física se estende em diversas observações que visam esconder da visão ou do acesso, cabos, linhas telefônicas e outras comunicações, e quando possível, mantê-las dentro dos prédios para aumentar a segurança.

3.1.4. Encriptação e Validação de dados

A escrita em códigos, conhecida como criptografia, vem do grego kryptós, que significa “oculto”, e gráphein “escrita”, sendo utilizada como técnica de ocultar a comunicação desde os tempos egípcios, principalmente em situações de guerra.

Encriptação é o processo de codificar e decodificar os dados em ordem, garantindo que a informação esteja acessível somente para quem tiver autorização de acesso.

Criptografia não está completamente difundida no ambiente de automação. Para equipamentos dentro da rede, a encriptação não se faz necessária devido às baixas vulnerabilidades dos dados dentro da segurança física da área (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

Entretanto, quando existe comunicação com sites externos, deve-se avaliar a necessidade de se encriptar os dados, e se ela é apropriada ou não. O uso de chaves públicas para comunicação com redes externas, muito utilizadas no ambiente de TI, podem não ser viáveis por trazer latência na comunicação (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

Uma das maneiras de se encriptar dados é através de uma Rede Privada Virtual (do inglês, *Virtual Private Network* - VPN), uma rede privada que trabalha como uma sobrecamada da infraestrutura pública.

Segundo Da Silva (2003), a conexão virtual pode ser feita das seguintes formas:

- Entre duas máquinas, servidores e estações, interligadas via internet (figura 10);
- Entre um ou vários usuários remotos e uma rede (figura 11);

- Entre duas redes (figura 12).

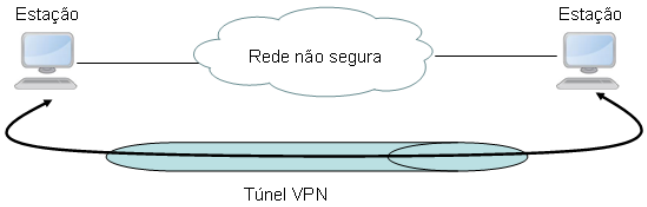

Figura 10 – VPN entre estações
Fonte: Autoria própria.

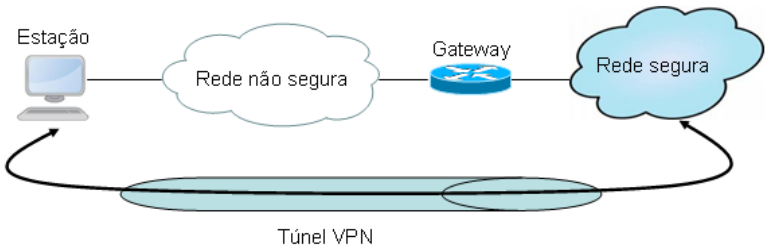

Figura 11 – VPN entre estação e rede
Fonte: Autoria própria.

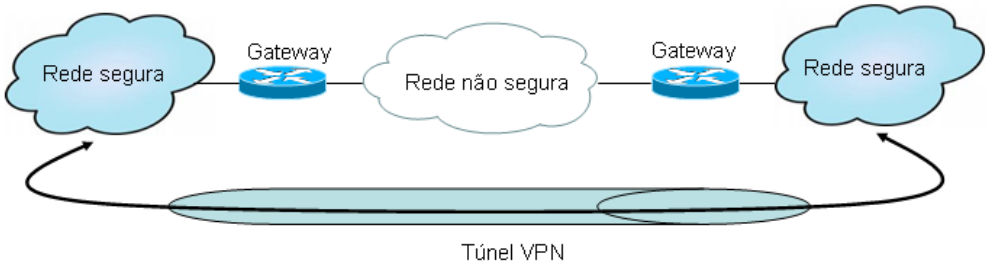

Figura 12 – VPN entre redes
Fonte: Autoria própria.

VPN são frequentemente usadas no ambiente industrial para prover acesso seguro com redes não seguras. Quando apropriadamente configuradas podem prover restrição de acesso (de e para) aos computadores do sistema de controle e, desta forma, aumentar a segurança.

A solução VPN também tem sido utilizada para acesso remoto dos operadores e conexões visando à manutenção ou acesso dos fabricantes. Todavia, assim como a

encriptação e o uso de chaves públicas, a utilização de VPN deve ser analisada sob o ponto de vista de trazer latência na comunicação.

As fragilidades do VPN estão diretamente relacionadas às arquiteturas adotadas e investimento feito na arquitetura e nos serviços. Serviços como: servidor de correios, servidor *web* e servidor de banco de dados, podem ser agrupados em um mesmo equipamento (g*ateway* do VPN). A adoção de uma arquitetura individualizada traz mais segurança, todavia, a economia na não individualização do *hardware* se reverte em maior exposição aos riscos (ex.: vírus, política de backup, falhas de *hardware*, etc).

O uso de tecnologia VPN, ou uma comunicação criptografada, proporciona um nível de proteção razoável para as interfaces, rede e equipamentos que utilizam protocolo IP.

3.1.5. Gerenciamento, Auditoria, Monitoramento e Ferramentas de Detecção

Há diversas ferramentas de auditoria, monitoramento e detecção que analisam as vulnerabilidades de segurança de uma rede ou equipamentos, essas tecnologias incluem aquelas que detectam vírus no sistema, intrusos, utilitários que gravam *log* em servidores e que auditam serviços.

Essas tecnologias são utilizadas e conhecidas por profissionais de segurança do ambiente de TI e, num ambiente de automação, onde a rede é mais estável, a preocupação sobre a segurança se concentra nas autenticações e no perfeito registro e integridade da instalação (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

Ferramentas de detecção de intruso (do inglês, Intrusion Detection System - IDS) rodam em computadores e observam os recursos e aplicações à procura de anomalias, tradicionalmente denominadas de HIDS (*host-based intrusion detection systems*). Outra variação de IDS existente é quando a observação está no tráfego de rede, nesse caso, são denominadas de NIDS (*network-based intrusion detection systems*). Independente de o foco ser na rede (NIDS) ou nos servidores (HIDS), as ferramentas IDS rodam, na sua maioria, em protocolos baseados em tecnologia IP. Essas ferramentas devem ser

analisadas caso a caso e deve-se buscar não comprometer as funcionalidades do sistema (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

Soluções IDS podem ser instaladas e conectadas ao *firewall* para incrementar a segurança, todavia, a solução IDS não é típica em sistemas de controle.

3.1.6. Aplicativos de computador

O *software* usado nos equipamentos do ambiente industrial é um fator vital para determinar a inteira segurança do sistema de controle. Há três componentes chaves citados pelo Relatório Técnico da ISA-99:

- Servidores e sistemas operacionais das estações de trabalho;
- Tempo real e sistemas operacionais embarcados;
- Servidores *web* e tecnologias internet.

Provavelmente, os sistemas operacionais são a última linha de defesa dos sistemas de controle. Estão presentes em quase todos os computadores e utilizam basicamente a plataforma Windows e UNIX. Os demais equipamentos PLC, RTUs e controles do DCS podem usar sistemas especializados ou sistemas operacionais embarcados.

Na maioria das empresas pode-se dizer que não existe, no ambiente de automação, uma política de atualização de *patches* nos sistemas operacionais, havendo sempre o risco de que atualizações comprometam o perfeito funcionamento das operações.

Como os sistemas SCADA estão utilizando *hardware* comercial e sistemas operacionais de mercado, os fabricantes contam com as soluções de segurança dessas empresas (Microsoft, Intel e outras) para se beneficiarem (SHAW, 2006).

Apesar da tendência de aproximação, ainda existe um legado de equipamentos com sistema operacional não usual, *drivers/dlls* específicos, emuladores, *hardware* obsoletos, etc, e que após atualizações podem entrar em conflito e não funcionarem

corretamente. Outra questão são os vários tipos de *software* que rodam em *background*, antivírus, gerenciamento de ativos, *Intrusion Prevention System* (IPS) e outros, que podem comprometer a execução do aplicativo principal e ocasionar distúrbios no processo ou em equipamentos de rede (REVISTA INTECH, 2007, pág. 36–40).

3.2. PROTOCOLOS DE COMUNICAÇÃO

A Ethernet é a rede dominante em redes corporativas a mais de uma década e, mesmo utilizando o conceito de rede não determinística, vem ganhando espaço no ambiente industrial.

Entre os principais protocolos de uso industrial, baseados em IP, que são tipicamente usados para interconexão (troca de mensagens) em redes com sistemas SCADA, cita-se: FTP, HTTP, HTTPS, SMTP, SNMP, ICCP, DCOM, IP-DNP3, IP-MODbus e mais recentemente o OPC.

Todos esses protocolos apresentam a possibilidade de interface, baseado em IP, entre o sistema SCADA e outras redes, e não a comunicação do SCADA na sua própria rede (SHAW, 2006).

Protocolos antigos de comunicação de rede: DECnet, SNA, Token-Ring e outros, foram abandonados por serem problemáticos, não existindo o desenvolvimento de funcionalidades de segurança. Em situações onde há protocolos muito antigos, costuma-se aplicar o conceito de segurança pela obscuridade, onde a segurança pode ser garantida pelo desconhecimento dos protocolos. Todavia, ataques internos e falta de qualquer segurança intrínseca é motivo de preocupação (SHAW, 2006).

A cada dia que passa, as redes industriais estão se rendendo aos aplicativos de prateleira, tornando-se mais padronizada, incorporando soluções *plug-and-play* e protocolos baseado no TCP/IP. Desta forma, soluções de segurança amplamente utilizadas no ambiente de TI tornar-se-ão mais próximas de uso no ambiente industrial e, com os devidos ajustes, certamente adicionarão mais segurança à rede e aos usuários.

3.3. CONTRAMEDIDAS

Contramedidas são ações que visam reduzir o risco para um nível aceitável ou que mereçam políticas próprias de segurança. Contramedidas não eliminam os riscos, e a aplicação depende da natureza da ameaça a ser enfrentada.

Para agentes externos, segundo ANSI/ISA–99.00.01–2007 (pág. 46), as seguintes contramedidas servem de exemplo:

- Autenticação de usuários e/ou computadores;
- Controle de acesso;
- Detecção de intruso;
- Criptografia;
- Assinatura digital;
- Isolação ou segregação dos recursos;
- Rastreamento de *software* malicioso;
- Monitoramento da atividade do sistema;
- Segurança física;

No caso de ameaças com agentes internos, diferentes contramedidas devem ser aplicadas, porque o atacante pode, possivelmente, burlar algumas contramedidas externas. Nesse caso, sugere-se dar mais ênfase em contramedidas como: políticas de segurança, separação dos trabalhos, monitoramento das atividades, auditoria nos sistemas e criptografia (AMERICAN NATIONAL STANDARD INSTITUTE ISA-TR99.00.01, 2007, pág. 46).

Políticas de segurança para a operação de sistema SCADA são diferentes das políticas utilizadas pela TI para sistemas como: banco de dados, ERP (*Enterprise Resource Planning*), aplicação WEB e outras. Todavia, a aplicação de políticas de segurança, normas e procedimentos são essenciais para sensibilizar os envolvidos e ter atuação efetiva na segurança (SHAW, 2006).

Um programa de segurança deve incluir políticas de acesso, procedimentos, orçamento, metodologias, mudança de cultura da equipe, que na prática deve envolver todas as áreas da empresa (SHAW, 2006).

Seis contramedidas foram consideradas essenciais para se construir um Sistema de Gerenciamento de Cibersegurança (CSMS) pela ANSI/ISA-99.02.01-2009 (pág. 31-32) por possuírem grande impacto nas políticas e na arquitetura:

- Segurança pessoal;
- Segurança física e ambiental;
- Segmentação de rede;
- Controle de acesso: administração da conta;
- Controle de acesso: autenticação;
- Controle de acesso: autorização;

Quando a rede IP estiver sendo usada no campo, é preciso analisar a possibilidade de que, uma vez penetrando nessa rede, o *hacker* pode, a partir dela, acessar outros *sites* com PLCs e RTUs interconectados. A sugestão para medidas adequadas de segurança remete-se a certificado digital, VPN, autenticação e encriptação entre todos os equipamentos da rede (SHAW, 2006).

Comumente, os fabricantes acessam via linha discada os sistemas para suporte remotamente e diagnósticos. Com o crescimento exponencial da internet, esta se tornou a opção mais viável e, pela disponibilidade ou pré-existência nas empresas, a preferida pelos fabricantes. Uma boa forma de se proteger é a utilização de VPN, e se possível com o uso de certificado digital temporário.

É razoável se pensar que, para atacar um sistema SCADA, os *hackers* ou os vírus busquem alguma brecha no sistema por meio de técnicas e tecnologia utilizadas pelo mundo da TI, e que as contramedidas devem se situar no mesmo ambiente. O uso de políticas e procedimentos de recuperação e cópias de segurança pode ser considerado como a próxima linha de defesa nesses casos (SHAW, 2006).

Medidas convencionais de segurança, conhecidamente adotadas pela área de TI, às vezes não estão presentes no sistema SCADA, pode-se citar: sistema alternativo de energia (ex.: baterias), cópias de segurança e armazenamento, procedimento de

recuperação do sistema, relatório de incidentes, coleta e armazenamento de *log* para auditoria.

Para identificar sistemas que afetam grandes operações, pode-se utilizar o *Special Publication 800:30* do NIST para categorização dos sistemas. Esta categorização permite a classificação e documentação do estado dos ativos para futuras identificações e auditorias. Para determinar se os ativos estão protegidos apropriadamente, uma avaliação técnica de vulnerabilidade deve ser realizada no mínimo uma vez por ano nesses ativos. A linha base de avaliação inclui: descobrir as redes, descobrir todos os pontos de acesso da zona de segurança, identificar as portas, identificar serviços disponíveis, procurar por contas e senhas padrão, quebra de senhas, procurar mensagens SNMP (*Simple Network Management Protocol*), revisar a configuração dos equipamentos de rede, servidores e estações e qualquer outro serviço desejado pela organização (MCBRIDE, 2011, pág. 1640-1646).

O Department of Energy (DoE) dos EUA, cuja missão é garantir a segurança e prosperidade Americana pela discussão energética, ambiental e desafios nucleares através da transformação científica e soluções tecnológicas (tradução livre do site http://energy.gov/mission, acesso em: 10 ago. 2011) disponibilizou 21 passos que podem ser seguidos para proteger a rede SCADA:

1. Identificar todas as conexões existentes na rede SCADA;
2. Desconectar as conexões não necessárias da rede;
3. Avaliar e fortalecer a segurança das conexões remanescentes;
4. Fortalecer a rede removendo ou desabilitando serviços desnecessários;
5. Não confiar em protocolos proprietários para proteger o seu sistema;
6. Implementar as funcionalidades de segurança disponibilizados pelos fabricantes de equipamentos e sistemas;
7. Estabelecer fortes controles sobre qualquer meio de conexão que possa ser utilizado como *backdoor*;
8. Implementar sistemas de detecção de intrusão internos e externos e estabelecer monitoramento de incidentes 24h por dia;
9. Executar auditorias técnicas na rede, em todos os equipamentos conectados a ela e identificar pontos de preocupação;

10. Conduzir inspeções de segurança física e avaliar a segurança de todos os sites remotos conectados à rede;
11. Estabelecer grupos para identificar e avaliar possíveis cenários de ataques;
12. Definir claramente os papéis na segurança eletrônica, responsabilidade, poderes dos gerentes, administradores dos sistemas e usuários;
13. Documentar a arquitetura da rede e identificar sistemas que possuam funções críticas ou contenham informações sensíveis que necessitem de níveis de proteção adicional;
14. Estabelecer um rigoroso e contínuo processo de gerenciamento de riscos;
15. Estabelecer uma estratégia de proteção de rede baseada no princípio defesa em profundidade (princípio abordado no item 6.1 desse trabalho);
16. Identificar claramente os requisitos de segurança eletrônica;
17. Estabelecer efetivos processos de gerenciamento da configuração;
18. Conduzir rotinas de auto-avaliação;
19. Estabelecer sistemas de backup e planos de recuperação de desastres;
20. A liderança da organização deveria definir expectativas para o desempenho da segurança eletrônica e designar responsáveis individuais para cumprimento das expectativas;
21. Estabelecer políticas e realizar treinamentos para minimizar a possibilidade de que pessoas da organização forneçam, inadvertidamente, informações sensíveis sobre o sistema SCADA, arquitetura, operação ou controles de segurança.

O conceito de Gerenciamento Integrado de Ameaças (do inglês, Integrated Threat Management - ITM) está focado nas ameaças que podem afetar a organização. Uma solução ITM deveria proteger a companhia contra ameaças e prover monitoramento e gerenciamento, o que incluiria as seguintes funções: IDS, antivírus, anti*spyware*, filtro de *spam*, filtros para conteúdo de *e-mail* e *instant message*, filtro de URL, *firewall* e conectividade VPN. Ou seja, uma solução ITM deveria integrar inúmeras soluções de segurança de TI (MCBRIDE, 2011, pág. 1640-1646).

No âmbito de iniciativas nacionais, o Guia de Referência para a Segurança das Infraestruturas Criticada da Informação (versão 01, nov. 2010), conhecido como livro azul,

apresenta uma metodologia para identificação e classificação de ativos de informação, um questionário para mapeamento de ativos de informação, além de uma sugestão de avaliação de riscos dos ativos baseado na probabilidade, impacto e níveis. Propõem-se também, vários controles para os ativos de informação, sendo que o Acesso ao Sistema e Proteção das Comunicações abrange os seguintes controles: conta, senha, configuração, acesso, sessão, chave criptográfica, comunicação VOIP, isolamento do sistema e do *software* aplicativo, ferramentas e tecnologias para detecção de invasão e interrupção de serviço entre outros.

O conceito de desmembramento em zonas de segurança, conforme descrito na metodologia da ISA-99 e exemplificado na figura 13, define que, para cada zona, pode existir um grupo específico de características e requisitos de segurança.

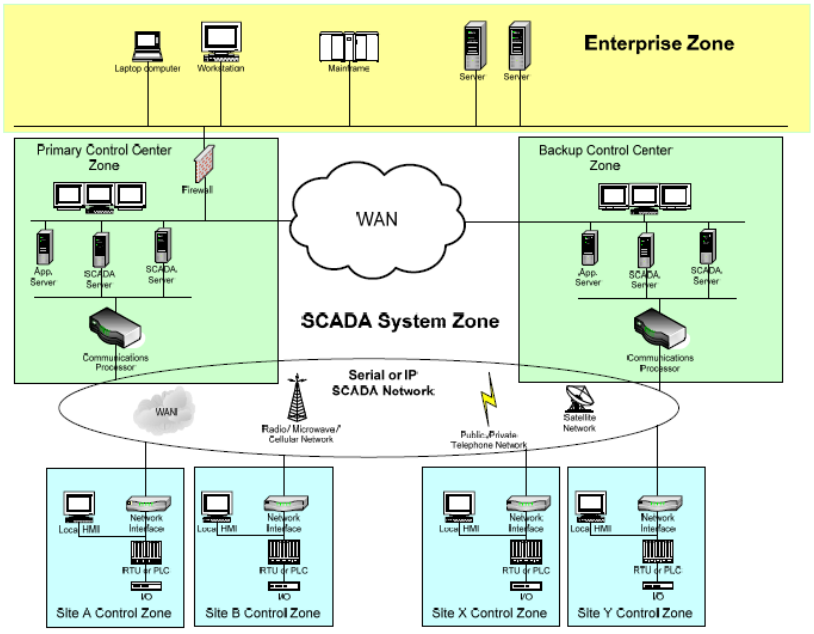

Figura 13 – Exemplo de zonas de segurança SCADA
Fonte: ISA-99.02.01 (2009, pág. 83).

Os requisitos de segurança aplicáveis em cada zona se dividem em: políticas de segurança, inventário dos ativos, requisitos e controles de acesso, ameaças e vulnerabilidades, consequências de quebra da segurança, tecnologia autorizada e processo de gerenciamento de mudança (AMERICAN NATIONAL STANDARD INSTITUTE, 2007).

A divisão em zonas também possibilita o uso de outra medida para incrementar a segurança: defesa em profundidade.

3.3.1. Defesa em Profundidade

Às vezes, técnicas e medidas simples podem não atingir os objetivos de segurança desejados, um enfoque maior com aplicação de várias medidas, em camadas ou de maneira gradativa, é conhecida como defesa em profundidade (AMERICAN NATIONAL STANDARD INSTITUTE, 2007, pág. 37).

A combinação dessas medidas para proteção contra vulnerabilidades é exemplificada na figura 14, que apresenta uma visão geral proposta por uma empresa da área de segurança industrial.

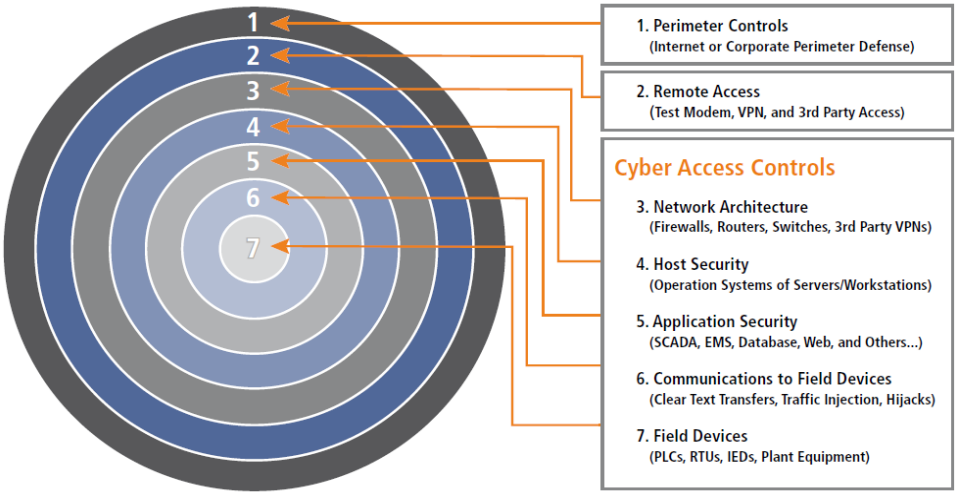

Figura 14 – Enfoque de segurança em camadas
Fonte: Industrial Defender (2009, pág. 1).

Segundo o Relatório *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies* do U.S Department of Homeland Security, de Outubro de 2009, uma estratégia de implementação de defesa em profundidade deveria ser estruturada conforme a figura 15:

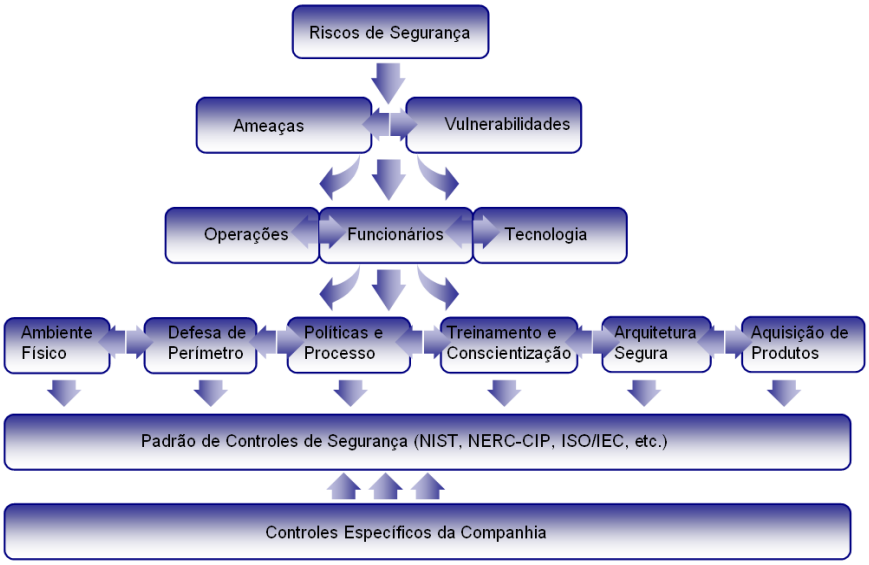

Figura 15 – Estruturação de uma estratégia de defesa em profundidade
Fonte: Tradução livre do autor, baseado em *DHS Recommended Practice* (2009, pág. 15).

Ainda segundo esse relatório, como princípios básicos e edificadores dessa estrutura, deve-se:

- Conhecer os riscos de segurança da organização;
- Quantificar e qualificar os riscos;
- Usar recursos chaves para mitigar os riscos de segurança;
- Definir as competências de cada recurso e identificar áreas sobrepostas;
- Obedecer aos existentes e novos padrões de segurança para controles específicos;
- Criar e customizar controles específicos únicos para a organização.

Para organizar a implementação de uma estratégia de defesa em profundidade é necessário conhecer os riscos do ambiente. Riscos de sistemas de controle industrial são melhores entendidos pelo conhecimento das ameaças e vulnerabilidades da organização. E para entender os riscos, a organização deveria fazer uma rigorosa avaliação de riscos para cobrir todos os aspectos da organização (U.S. DEPARTMENT OF HOMELAND SECURITY, 2009).

3.4. AVALIAÇÃO DE RISCOS

Segundo Goble (1998), a ciência da engenharia da confiabilidade desenvolveu um número de técnicas qualitativas que permitem ao engenheiro entender o sistema de operação na presença de falha de um componente. Essas técnicas incluem modelos de falha e análises de efeitos (FMEA), análise de árvore de falhas qualitativas (FTA), e *hazard and operational analysis* (HAZOP), além de outras baseadas sobre teoria de probabilidades e estatísticas: confiabilidade das redes, modelo Markov e *Life-Cycle cost.*

A eliminação, por completo, de todos os riscos torna-se impraticável, e as organizações devem concentrar a avaliação de riscos nas aplicações e infraestruturas mais críticas (AMERICAN NATIONAL STANDARD INSTITUTE, 2009, pág. 119).

É importante notar que, avaliação de risco de segurança da informação é um processo de negócio e não um assunto de tecnologia. Algumas dimensões, dentro das muitas avaliações de risco de segurança, serão técnicas em natureza, mas o resultado, das análises e das saídas, são escritas e feitas para os líderes do negócio, visando dar uma descrição acurada dos riscos que suas organizações e negócios estão expostos (LAYTON, 2007).

Avaliação de risco para sistemas gerais, incluindo redes WAN/LAN, são sugeridas para serem realizadas no mínimo a cada cinco anos, ou com uma frequência maior quando há grandes mudanças nas operações, no *software*, no *hardware* ou nas configurações (BLANDING, 2011).

Segurança é realmente uma balança entre o risco versus o custo, e no caso do ambiente industrial, o investimento exagerado em segurança pode, por exemplo, diminuir as funcionalidades que são necessárias para o seu perfeito funcionamento (AMERICAN NATIONAL STANDARD INSTITUTE, 2009).

Uma das mais conhecidas avaliação de risco de segurança da informação é o modelo de gerenciamento descrito no *Special Publication 800-30* do National Institute of Standars and Technology (NIST). O ISO/IEC 17799:2005 (27002) *Code of Practice for Information Security Management* é também amplamente utilizado pelas organizações para a implementação de segurança da informação. Este é composto por 133 controles,

cujo benefício é proporcionar que as organizações possam avaliar qual controle se aplica, ou não, ao seu modelo de negócio (LAYTON, 2007).

Segundo ISO/IEC 17799:2005, um completo inventário dos ativos é pré-requisito para um efetivo gerenciamento técnico das vulnerabilidades e uma avaliação de riscos deve identificar, quantificar e priorizar riscos contra critérios de aceitação de riscos e objetivos relevantes da organização. O resultado deve determinar apropriadas ações de gerenciamento, prioridades para gerenciar as informações de risco de segurança e implementar controles selecionados para proteção contra esses riscos. A avaliação de riscos deve incluir estimativa da magnitude do risco (análise do risco) e o processo de comparação do risco estimado contra o critério de risco para determinar o valor do risco (avaliação do risco).

Gerenciamento de risco inclui a identificação da informação e outros ativos do sistema, ameaças que poderiam afetar a confidencialidade, integridade ou disponibilidade do sistema, vulnerabilidades do sistema a ameaças, potenciais impactos das atividades ameaçadoras, identificação dos requisitos de proteção para controlar os riscos e seleção de medidas apropriadas de segurança (BLANDING, 2011).

A discussão clássica sobre gerenciamento de risco e mitigação envolve uma série de cálculos estatísticos, considerando os custos de substituição de um ativo crítico, o custo de perder o ativo e a probabilidade e frequência de uma possível ameaça acontecer. Essas análises e decisões são relevantes quando se discute a chance de se perder um servidor Web utilizado para realizar Comércio Eletrônico, mas não ficam claras sobre a segurança de um SCADA. Isto porque, o impacto de se perder um sistema SCADA está além dos valores financeiros ou regras do negócio, deve-se considerar o assunto segurança pública. Caso haja interrupção na distribuição de eletricidade, gás natural ou fornecimento de água, a tradicional análise financeira custo-benefício pode não ser a adequada para justificar o investimento e as medidas necessárias de proteção. Mesmo o uso de sistemas legais no âmbito estadual ou federal, que estabeleçam ações punitivas contra as empresas, pode não resultar numa medida adequada de proteção (SHAW, 2006, pág. 246).

Segundo Blanding (2011), existem duas formas de análise de riscos: automática e questionário ou *checklist*. A avaliação automática é realizada por aplicações que analisam de forma geral as vulnerabilidades de rede. Questionário é uma maneira de

agrupar as informações relevantes e pode ser simples e rápido, além de ser uma ferramenta efetiva de suporte para avaliação de riscos informal e formal. Um questionário ou *checklist* pode ser a primeira etapa para determinar se uma avaliação de risco, mais formal e extensiva, precisa ser feita, além de também ser um guia da avaliação dos riscos.

4. TECNOLOGIAS SELECIONADAS E METODOLOGIA

Nesse momento, é de suma importância relembrar a pergunta que norteia a pesquisa: Quais tecnologias podem ser implementadas numa empresa, com sistema SCADA instalado, para aumentar a segurança?

De acordo com o apresentado nessa dissertação, torna-se possível selecionar um grupo de tecnologias e medidas de segurança com possibilidades de implementação em ambientes industriais.

A seleção consolida o que foi encontrado na literatura pesquisada e mantêm consenso quanto ao incremento na segurança de qualquer ambiente com SCADA instalado.

Também se considera o fato de serem tecnologias maduras no ambiente de TI e já estarem sendo utilizadas, com alguma escala, no ambiente industrial.

A figura 16 apresenta as tecnologias e as contramedidas de segurança selecionadas.

TECNOLOGIAS E CONTRAMEDIDAS SELECIONADAS	
Autenticação e Autorização	• Usuário/senha • Token • Cartão Inteligente • Equipamento-para-equipamento • Identificação biométrica • Desafio/resposta • Proteção baseada na localização
Controle de Acesso, Filtros e Bloqueios	• Firewall • VLAN • DMZ
Segurança Física	• Portas controladas • Perímetro de segurança • Monitoramento de acesso físico
Encriptação e Validação de Dados	• VPN • Criptografia
Gerenciamento, Auditoria, Monitoramento e Ferramentas de Detecção	• Antivírus • *Log* eventos e falhas
Aplicativos de Computador	• Sistema operacional atualizado
Contramedidas	• Política de segurança de ativos • Zonas de segurança • Defesa em profundidade • Fonte alternativa de energia • Cópia de segurança • Levantamento e avaliação de riscos em ativos críticos

Figura 16 – Tecnologias e contramedidas selecionadas
Fonte: Autoria própria.

Elaborou-se um questionário com o objetivo de prover um uso prático para esta pesquisa e, considerando as tecnologias e contramedidas selecionadas, o questionário também fornece insumos para que a empresa, ao utilizá-lo, obtenha uma avaliação de segurança do seu ambiente de automação industrial.

Para Marconi e Lakatos (2006), a elaboração do questionário requer a observância de normas precisas, a fim de aumentar a sua eficácia e validade, o pesquisador deve conhecer bem o assunto e o questionário deve ser limitado em

extensão e finalidade. Deve conter de 20 a 30 perguntas e demorar cerca de 30 minutos para ser respondido, variando conforme o tipo de pesquisa e os informantes.

O questionário, apresentado no Apêndice 1, contém 22 questões diretas e traz, agregado ao seu conteúdo e praticidade, os seguintes conhecimentos:

- Apresenta as principais tecnologias e contramedidas disponíveis;
- Identifica a situação da segurança na unidade operacional;
- Serve como um pequeno guia, onde investimentos para responder de forma positiva ao questionário tornarão a rede mais segura;

Quanto à forma, o questionário aplicado utiliza perguntas fechadas ou dicotômicas, também denominadas limitadas ou alternativas fixas, e o informante escolhe entre duas opções: sim e não (MARCONI; LAKATOS, 2006, pág. 101).

Para validar e adequar o questionário, realizou-se um pré-teste em uma unidade industrial com o objetivo de verificar alguma inconsistência ou interpretação errônea das perguntas propostas.

O pré-teste tem o objetivo de verificar três elementos segundo Marconi e Lakatos (2006, pág. 100):

1) Fidedignidade: obtenção sempre dos mesmos resultados independente da pessoa que o aplique;
2) Validade: os dados recebidos são necessários à pesquisa;
3) Operatividade: vocabulário e significado acessível e claro.

4.1. RESULTADO DO QUESTIONÁRIO

O questionário foi aplicado, por meio eletrônico, em dez unidades industriais e foi respondido apenas pelo responsável técnico pela automação da planta. Normalmente esse papel é desempenhado por um Engenheiro ou um técnico de elevada experiência. O resultado está apresentado no quadro comparativo da figura 17.

		Unidade Operacional									
		A	B	C	D	E	F	G	H	I	J
Questão	1	NAO	NÃO[1]	NÃO[1]	SIM	SIM	SIM	SIM	SIM	SIM	SIM
	2	NÃO	NÃO[1]	NÃO[1]	SIM	SIM	SIM	NÃO[1]	SIM	NÃO	NÃO
	3	SIM	NÃO[1]	NÃO[1]	NÃO	SIM	SIM	NÃO[1]	SIM	NÃO	NÃO
	4	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	NÃO	NÃO	NÃO
	5	NÃO	NÃO	SIM	NÃO	SIM	NÃO	NÃO	NÃO	NÃO	SIM
	6	NÃO	NÃO	NÃO	NÃO	SIM	SIM	SIM	NÃO	NÃO	NÃO
	7	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	SIM[2]	NÃO	NÃO
	8	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO
	9	SIM	NÃO	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
	10	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM	SIM
	11	NÃO	NÃO	NÃO	SIM	SIM	SIM	SIM	SIM	NÃO	SIM
	12	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	NÃO
	13	SIM[1]	NÃO	SIM	NÃO	NÃO	NÃO	NÃO	NÃO	SIM[1]	NÃO
	14	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO
	15	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO
	16	SIM[1]	SIM	SIM	NÃO	SIM	SIM	SIM[1]	SIM	NÃO	NÃO
	17	NÃO	NÃO	NÃO[2]	NÃO[2]	NÃO[2]	NÃO[2]	NÃO[2]	NÃO[2]	NÃO[2]	NÃO[2]
	18	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO
	19	NÃO	NÃO	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	NÃO
	20	NÃO	NÃO	NÃO	NÃO	SIM	NÃO	NÃO	NÃO	NÃO	NÃO
	21	NÃO	SIM	SIM	NÃO	SIM	SIM	NÃO	NÃO	NÃO	SIM
	22	3	Nenhum	Nenhum	4	Nenhum	Nenhum	3	Nenhum	---	1

Figura 17 – Quadro comparativo das respostas
Fonte: Autoria própria.

A figura 18 apresenta a legenda que foi aplicada na elaboração do quadro comparativo das respostas visualizados na figura anterior.

LEGENDA	
NÃO[1]	Não existe comunicação externa estabelecida
NÃO[2]	NÃO, pois não possui conexão wireless habilitada
SIM[1]	SIM, mas não sabe se foram homologados pelo fornecedor
SIM[2]	SIM, mas sem processo periódico de renovação
---	Não monitora histórico de incidentes no sistema

Figura 18 – Legenda do quadro comparativo das respostas
Fonte: Autoria própria.

4.1.1. Tecnologias em uso

A tecnologia que obteve um maior número de respostas afirmativas (SIM) foi àquela relacionada ao uso de fonte alternativa de energia para garantia de funcionamento, todas as 10 unidades (100%) informaram possuir sistema de fonte alternativa. Em segundo lugar, com 90%, encontram-se as rotinas de cópia de segurança.

A figura 19 apresenta as tecnologias classificadas por percentual de uso nas unidades pesquisadas.

Unidade	Tecnologias/Contramedidas Utilizadas
100%	Fonte alternativa de Energia
90%	Cópias de segurança
70%	Sistema Operacional atualizado Firewall entre redes internas
60%	Levantamento e avaliação de riscos em ativos críticos
50%	*Log* implementado
40%	VPN Firewall para comunicação com redes externas
30%	DMZ VLAN Antivirus homologado
20%	Usuário e senha com processo periódico de renovação Wireless sem segurança habilitada
10%	Criptografia Política de Segurança de Ativos Portas Controladas Perímetro de segurança física
0%	Monitoramento de acesso físico Outras soluções próprias do fornecedor Zonas de segurança Defesa em profundidade

Figura 19 – Tecnologias e contramedidas em uso nas 10 unidades pesquisadas
Fonte: Autoria própria.

Nota-se que tecnologias como: usuários e senhas com processo periódico de renovação (10%), portas controladas (10%) e perímetro de segurança física (10%) são soluções de simples implementação e quase sempre de pouco custo, entretanto, ainda estão pouco implementadas nessas unidades.

Os conceitos de zonas de segurança, conforme descrito na ISA-99, e defesa em profundidade não foram citados por nenhuma das unidades.

4.1.2. Análise das tecnologias nas Unidades Operacionais

Conforme explicado anteriormente, é possível extrair das respostas um panorama da segurança na unidade operacional.

A figura 20 apresenta o quantitativo de tecnologias e contramedidas em uso pelas unidades e os incidentes identificados, conforme solicitado na questão 22.

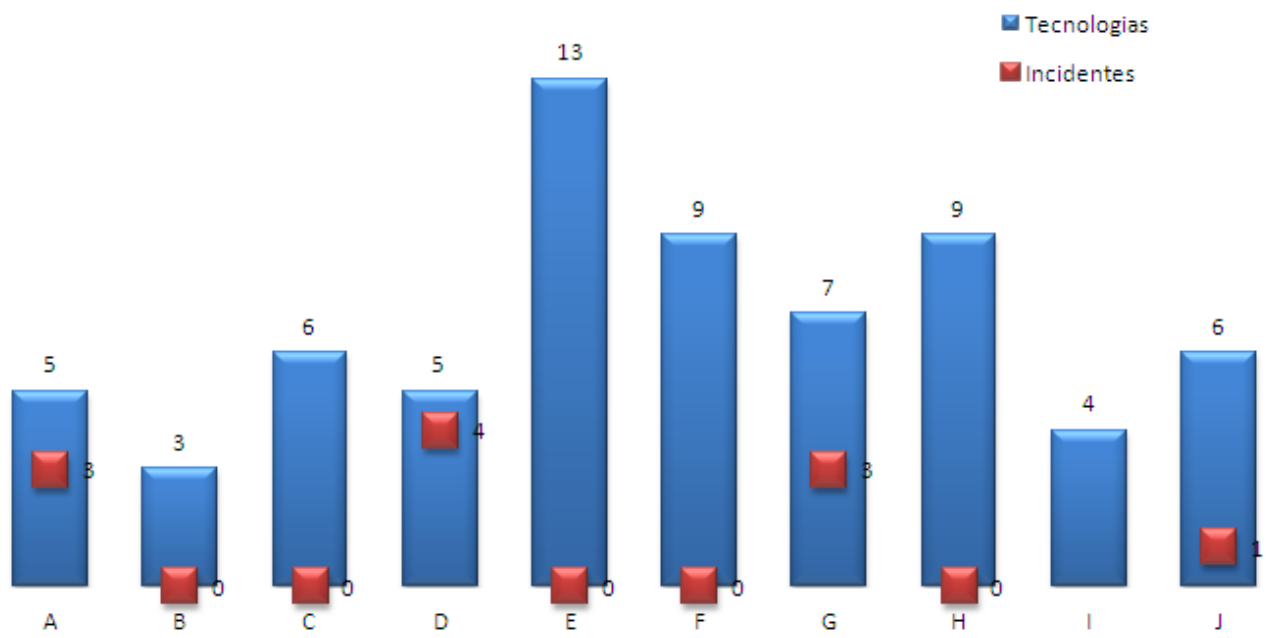

Figura 20 – Quantitativo de tecnologias em uso e incidentes identificados
Fonte: Autoria própria.

As unidades que utilizam um maior número de tecnologias de segurança (Unidade E com 13 tecnologias e Unidade F e H com 9 tecnologias), registraram 0 incidentes. As Unidades A (5 tecnologias) e a Unidade G (7 tecnologias) registraram 3 incidentes, e a Unidade D (5 tecnologias) registrou 4 incidentes. A Unidade J com 6 tecnologias registrou 1 incidente.

A unidade B, com apenas 3 tecnologias, registrou 0 incidentes. Conforme análise das respostas às questões 1, 2 e 3, de que não existe conexão externa estabelecida, caracteriza que o sistema de controle da unidade trabalha de forma isolada das redes de *internet*, o que reduz sensivelmente a sua exposição às ameaças. Pode-se também conjeturar que o sistema de controle esteja protegido pelo conceito de segurança pela obscuridade, mas nesse caso, questões específicas precisariam ser feitas para validar essa hipótese.

A unidade I respondeu que não monitora histórico de incidentes no sistema.

5. CONCLUSÕES

Em termos de tecnologias e medidas de segurança conclui-se que há um vasto conjunto de alternativas, assim sendo, a empresa deve estar apta para saber avaliá-las. Para auxiliar nessa decisão a empresa pode recorrer às normas da ISA-99, que são de grande utilidade na identificação das alternativas tecnológicas e, como descrito no próprio objetivo do seu Relatório Técnico, servem também como uma guia para uso dessas tecnologias e contramedidas.

A empresa também pode utilizar-se de outras fontes de recomendações técnicas, quer seja de companhias que atuam na mesma área ou de metodologias mundialmente conhecidas, como por exemplo, as elaboradas por organizações como: NIST, NERC e ISO.

A aproximação das técnicas utilizadas pela TI no ambiente industrial disponibiliza uma enorme quantidade de soluções e, uma vez que se tenha a garantia de não comprometimento da disponibilidade do ambiente industrial, as soluções de TI são de grande aplicabilidade e relevância.

Entretanto, para a aplicação dessas tecnologias, algumas barreiras precisam ser transpostas. Normalmente não há uma cultura, do pessoal de operação da unidade industrial, para trabalhar com essas tecnologias, não existe pessoal capacitado, e não há procedimentos operacionais, similares aos adotados pelos técnicos da área de TI. Adiciona-se que nem sempre há orçamento e, se não houver aval dos fornecedores e fabricantes dos sistemas SCADA para uso dessas soluções, certamente não serão implementadas ou ficarão relegadas a segundo plano.

O resultado do questionário aplicado corrobora com pesquisas citadas nessa monografia, de que indústrias brasileiras investem pouco em tecnologias e contramedidas de segurança, além de demonstrar que o uso destas continua pouco difundido no ambiente industrial. O panorama extraído da aplicação do questionário será utilizado como um guia de investimentos para essas empresas e soou também como uma alerta para a situação das unidades onde houve vários incidentes registrados.

Em virtude da profusão de assuntos que podem ser explorados, considerando a complexidade de cada um, citam-se alguns que podem ser apresentados e aperfeiçoados em trabalhos futuros:

- Custo/benefício das soluções de segurança em ambientes industriais;
- Avaliação de Riscos: metodologias, comparativos, aderência ao ambiente industrial;
- Novas tecnologias de segurança em TI e os seus impactos na operabilidade de plantas industriais;
- Segurança industrial: riscos, soluções, impactos, aplicabilidade em setores específicos e regulações.

REFERÊNCIAS

AMERICAN NATIONAL STANDARD INSTITUTE. **ANSI/ISA–99.02.01–2009**: Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. ISA, 2009

AMERICAN NATIONAL STANDARD INSTITUTE. **ANSI/ISA–99.00.01–2007**: Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models. ISA, 2007.

AMERICAN NATIONAL STANDARD INSTITUTE. **ANSI/ISA–TR99.00.01**. Technical Report Security Technologies for Industrial Automation and Control Systems, out. 2007. ISA, 2007.

American society of Civil engineers (ASCE) e American Water Works Association (AWWA). Guidelines for the Physical Security of Water Utilities, dez. 2006. Draft American National Standard for Trial Use. Disponível em: <http://awwa.org/files/science/wise/Guidelines_Physical_security_Wastewater_Stormwater.pdf>. Acesso em: 20 jul. 2011.

BEGGS, Christopher. A Holistic SCADA Security Standard for the Australian Context, In: 9th Australian Information Warfare and Security Conference, Perth Western Australia, 1 dez. 2008. Disponível em: <http://ro.ecu.edu.au/isw/27>. Acesso em: 10 nov. 2011.

BLANDING, Steven F. LAN/WAN Security, **Encyclopedia of Information Assurance**, EUA, v. 3, p.1790-1804, 2011.

BOYER, Stuart A. **SCADA – Supervisory Control and Data Acquisition**. 3 ed. ISA, 2004.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: Segurança cibernética no Brasil.** Brasília: GSIPR/SE/DSIC, 2010a. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: 24 dez. 2011.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Guia de referência para a segurança das infraestruturas críticas da informação**. Brasília: GSIPR/SE/DSIC, 2010b. Disponível em: <http://dsic.planalto.gov.br>. Acesso em: 24 dez. 2011.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.BR). **Estatísticas**. Disponível em: <www.cert.br/stats/incidentes>. Acesso em: 10 fev. 2012.

CERVO, Amado L.; BERVIAN, Pedro A.; DA SILVA, Roberto. **Metodologia Científica,** 6 ed. São Paulo: Pearson Prentice Hall, 2007.

DA SILVA, Lino S. **VPN- Virtual Private Network:** Aprenda a construir redes privadas virtuais em plataformas Linux e Windows, 2003, Novatec LTDA, 2003.

DICKMAN, Frank. Hacking de industrial network. **White Paper Phoenix**, 2009. Disponível em: <www.phoenixcontact.com>. Acesso em: 20 jun. 2011.

INDUSTRIAL DEFENDER. Risk Assessment, 2009. Disponível em: <www.industrialdefender.com>. Acesso em: 20 ago. 2011.

INTERNATIONAL STANDARD. IEC 61131-1 – Programmable controllers – Part1: General information. IEC, 2003-05.

INTERNATIONAL STANDARD. ISO/IEC 17799:2005. Information technology – Security techniques - Code of practice for information security management. ISO, 2005.

GOBLE, William M. **Control System Safety Evaluation & Reliability**. 2 ed. ISA, 1998.

LAYTON, Timothy P. **Information Security**: Design, Implementation, Measurement, and Compliance, Auerbach, 2007.

MARCONI, Marina de A.; LAKATOS, Eva M. **Técnicas de Pesquisa**: Planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados. 6 ed. São Paulo: Atlas, 2006.

MCAFEE. **Relatório anual da McAfee sobre Proteção de Infraestruturas Críticas 2011**. Disponível em: <www.mcafee.com/br>. Acesso em: 06 jan. 2012.

MCBRIDE, George G. Integrated Threat Management. **Encyclopedia of Information Assurance**, EUA, v. 3, p.1640-1646, 2011.

MORA, Halley R. M. Introdução à Segurança em Redes de Automação. **Revista InTech**., n. 91, p. 36–40, 2007.

MORAES, C.C.; CASTRUCCI, P.D.L **Engenharia de Automação industrial**. Rio de Janeiro: LTC, 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Special Publication: 800-12, An Introduction to Computer Security**: The NIST Handbook, 2006. National Institute of Standars and Technology. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>. Acesso em: 17 fev. 2012.

RICHARDSON, Robert. CSI Survey 2007: The 12th Annual Computer Crime and Security Survey. Computer Security Institute. Disponível em: <www.GoCSI.com>. Acesso em: 22 jun. 2011.

SHAW, William T. **Cybersecurity for Scada Systems**. Oklahoma: Penwell, 2006.

SYMANTEC, Secure Response. W32.Stuxnet Dossier, Setembro 2010, v.1. Disponível em: <http://www.wired.com/images_blogs/threatlevel/2010/10/w32_stuxnet_dossier.pdf>. Acesso em: 24 dez. 2011.

TECHNICAL INFORMATION BULLETIN 04-1. National Comunications System, EUA. **Supervisory Control and Data Acquisition (SCADA) Systems**, out. 2004. Disponível em: <http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf>. Acesso em: 20 out. 2011.

TEUMIM, David J. **Industrial Network Security**. ISA, 2005

THE WHITE HOUSE WASHINGTON, EUA. **The National Strategy to Secure Cyberspace**, fev. 2003. Disponível em: <http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf>. Acesso em: 20 out. 2011.

TIPTON, Harold F. Information Security Management: Purpose. **Encyclopedia of Information Assurance**, EUA, v. 3, p.1556-1562, 2011.

TURK, Robert J. **Cyber Incidents Involving Control Systems**. Idaho National Laboratory, out. 2005. Disponível em: <www.inl.gov/technicalpublications/Documents/3480144.pdf>. Acesso em: 20 jun. 2011.

U.S. DEPARTMENT OF ENERGY, EUA. **21 Steps to improve Cyber Secrutiy of SCADA Networks.** Disponível em: <http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf acessado em 10/08/2011>. Acesso em: 15 out. 2011.

U.S. DEPARTMENT OF HOMELAND SECURITY. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, Out. 2009. Disponível em: http://www.us-cert.gov/control_systems/pdf/DHS_Common_Vulnerabilities_R1_08-14750 Final_7-1-09.pdf>. Acesso em: 10 dez. 2011.

U.S DEPARTMENT OF HOMELAND SECURITY. **Report Common Cybersecurity Vulnerabilities in Industrial Control Systems**, maio 2011. Disponível em: <http://www.us-cert.gov/control_systems/pdf/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf >. Acesso em: 01 dez 2012.

APÊNDICE 1 - QUESTIONÁRIO

1) Existe firewall, configurado e operacional, entre a rede administrativa e a rede do sistema de supervisão/controle da unidade?

( ) SIM ( ) NÃO ( ) Não existe comunicação entre as redes

2) O sistema de supervisão/controle faz uso de firewall para se conectar a sistemas externos a unidade?

( ) SIM ( ) NÃO ( ) Não existe comunicação externa estabelecida

3) O sistema de supervisão/controle faz uso da tecnologia VPN para se conectar a sistemas externos a unidade?

( ) SIM ( ) NÃO ( ) Não existe comunicação externa estabelecida

4) O sistema de supervisão/controle faz uso da tecnologia de criptografia para se comunicar interna ou externamente?

( ) SIM ( ) NÃO

5) O sistema de supervisão/controle faz uso da tecnologia de Rede Virtual (VLAN) entre os seus sistemas/equipamentos?

( ) SIM ( ) NÃO

6) O sistema de supervisão/controle faz uso da tecnologia de zona desmilitarizada (DMZ) para segregar equipamentos/sistemas?

( ) SIM ( ) NÃO

7) Para acesso ao sistema de supervisão/controle, utilizam-se usuário e senha únicos por usuário, e um processo periódico de renovação?

( ) SIM ( ) NÃO ( ) SIM¸ mas sem processo periódico de renovação

8) O sistema de supervisão/controle se utiliza de alguma dessas tecnologias para autorizar acesso interno ou remoto: equipamento-para-equipamento (device-to-device), identificação biométrica, desafio/resposta (challenge/response), token ou cartão inteligente (smart-card)?

( ) SIM ( ) NÃO

9) Existe uma rotina de cópias de segurança (backup) dos dados que compõem o Sistema de supervisão/controle?

( ) SIM ( ) NÃO

10) O sistema de supervisão/controle da unidade está conectado a uma fonte alternativa de energia (gerador/UPS) para garantia de funcionamento em caso de falta ou pane elétrica?

( ) SIM ( ) NÃO

11) A unidade já realizou algum trabalho de levantamento dos ativos críticos e/ou avaliação de riscos dos ativos de automação?

( ) SIM ( ) NÃO

12) A unidade possui alguma política formal de segurança de ativos de automação (ex.: treinamento do pessoal, procedimentos, monitoramento, avaliação de riscos etc.) ?

( ) SIM ( ) NÃO

13) Existe antivírus, homologado pelo fornecedor, sendo executado nas máquinas do sistema de supervisão/controle?

( ) SIM ( ) NÃO ( ) SIM¸ mas não homologado pelo fornecedor

14) A unidade utiliza alguma outra solução específica do fabricante/fornecedor (exceto antivírus) com o objetivo de incrementar a segurança da rede do sistema de supervisão/controle?

( ) SIM ( ) NÃO

15) A unidade utiliza o conceito de zonas de segurança (conforme descrito na norma ISA-99) ou o conceito de defesa em profundidade para incrementar a segurança do sistema de supervisão/controle?

( ) SIM ( ) NÃO

16) O sistema operacional está atualizado com os patches do fabricante e foram homologados pelo fornecedor do sistema de supervisão/controle?

( ) SIM ( ) NÃO ( ) SIM¸ mas não sei se foram homologados pelo fornecedor

17) No caso de existência de comunicações wireless com o sistema de supervisão/controle, existe alguma medida de segurança (ex.: proteção baseada na localização GPS) implementada?

( ) SIM ( ) NÃO ( ) NÃO¸ pois não possuo conexão wireless habilitada

18) Existe sistema de monitoramento do tipo câmeras e sensores, com a intenção de vigiar o acesso de pessoas ao sistema de supervisão/controle?

( ) SIM ( ) NÃO

19) Existe um perímetro de segurança física em torno do sistema de supervisão/controle (ex.: porta com código) com um processo de renovação periódica dos acessos?

( ) SIM ( ) NÃO ( ) SIM¸ mas sem processo periódico de renovação

20) Os equipamentos críticos que compõem o sistema de supervisão/controle estão desabilitados para uso de CD, DVD, pendrives ou possuem outras portas físicas disponíveis controladas?

( ) SIM ( ) NÃO

21) Existe algum monitoramento online dos eventos e falhas dos equipamentos (log) que compõem a rede de supervisão/controle e estes podem auditados?

( ) SIM ( ) NÃO

22) Em relação ao histórico de incidentes de segurança que acometeram o sistema de supervisão/controle, quantos incidentes foram identificados até hoje?

( ) Nenhum ( )1 ( )2 ( )3 ( )4 ( )5 ( )Mais de 5 incidentes ( )Não monitoramos histórico de incidentes no sistema