O USO DE PADRÕES ABERTOS PARA PROTEÇÃO DE SISTEMAS SCADA E DE AUTOMAÇÃO[1]

Eric J. Byres [2]
Marcelo Ayres Branquinho[3]

Resumo

Crescentes evidências sugerem que ignorar a segurança custa às empresas mais que o custo financeiro e que os riscos financeiros e de produção devidos à pobre segurança são fáceis de serem subestimados. Os incidentes de segurança são intermitentes, incompreendidos e normalmente não relatados. Estudos comprovam que a maioria dos problemas começam no interior da empresa, vindos de pessoas e sistemas, que são ambos bem intencionados confiáveis. Para complicar as coisas existe o fato de que os sistemas de controle têm necessidades específicas que não são abordadas pela maioria das soluções de segurança de TI que estão disponíveis no mercado. Estas necessidades incluem requisitos de segurança física e suporte para os protocolos de comunicação exclusivos que são comuns em redes industriais. Tais sistemas exigem também a possibilidade de instalar, configurar e testar essas soluções de segurança sem colocar a planta em risco. Este trabalho apresenta métodos para implementar a segurança em redes de automação industrial utilizando padrões abertos definidos por vários organismos internacionais de padronização, como o ISA (*The International Society of Automation*). Utilizamos as melhores práticas, baseadas no novo padrão de segurança ANSI/ISA-99, que os líderes da indústria usam para proteger seus sistemas de controle de uma maneira bastante efetiva. Os conceitos de uma estratégia de defesa em profundidade serão apresentados, inclusive como utilizar o modelo de zonas e conduítes da ISA-99 para assegurar sistemas de controle.

Palavras-chave: Segurança; ANSI/ISA-99; SCADA, Riscos.

USE OF OPEN STANDARDS TO PROTECT SCADA AND AUTOMATION SYSTEMS

Abstract

Growing evidence that suggests ignoring security costs companies more than just money and that the financial and production risks from poor security in automation systems are easy to underestimate. Security incidents are intermittent, misunderstood and typically under reported. Studies have noted that most of the problems start on the inside, from individuals and systems that are both well intended and are trusted. Complicating matters is the fact that control systems have unique requirements that are not approached by most IT-based security solutions now available. These requirements include physical security requirements and support for unique communication protocols that are common in industrial networks. Such systems also require the ability to install, configure and test these security solutions without putting the plant at risk. This paper presents methods to implement security in industrial automation networks using open standards defined by various international organizations for standardization such as the ISA (The International Society of Automation). We look at the best practices, based around the new ANSI/ISA-99 security standards that industry leaders use to secure their control systems in a cost effective manner. The concepts of a defense-in-depth strategy will be outlined, including how to use ISA-99 zone and conduit models to secure control systems.

Key words: Security; ANSI/ISA-99; SCADA, Risks.

[1] *Contribuição técnica ao 14° Seminário de Automação de Processos, 6 a 8 de outubro de 2010, Belo Horizonte, MG.*

[2] *Byres Security Inc, Canada*
[3] *TI Safe Segurança da Informação Ltda, Brasil*

1 INTRODUÇÃO

Durante os últimos anos, o controle de serviços essenciais para as pessoas como a eletricidade, produção de combustíveis, água, transportes, manufatura e comunicações, tem utilizado sistemas de controle de automação conhecidos como SCADA. Pouca atenção foi dada à riscos de segurança, uma vez que se acreditava que estas redes eram praticamente imunes a cyber-ataques.(1)
Eventos recentes como o apagão de 11/11/09 que atingiu 18 estados no Brasil tem mostrado que esta tranquilidade está acabando, e os sistemas de automação tem, cada vez mais, sido alvo de ataques de grupos terroristas, hackers e funcionários insatisfeitos com suas empresas. Não só o número de incidentes tem crescido, mas também a seriedade dos mesmos tem também aumentado, levando as empresas a prejuízos incalculáveis que tem como resultado não só a perda de dinheiro, mas também manchas na reputação, impactos ambientais, danos em equipamentos e, em alguns casos, a morte de pessoas.
Para balisar a implantação de soluções de segurança em redes de automação, a ISA (*International Society of Automation*) 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 tornado item mandatório para infraestruturas críticas. Soluções de segurança em redes industriais devem necessariamente mesclar a experiência do especialista em segurança de rede com a experiência do especialista no sistema de controle de produção.(2)
Este trabalho apresenta métodos para implementar a segurança em redes de automação industrial utilizando padrões abertos. Utilizamos as melhores práticas, baseadas no padrão de segurança ANSI/ISA-99,(3) que os líderes da indústria usam para proteger seus sistemas de controle de uma maneira bastante efetiva. Os conceitos de uma estratégia de defesa em profundidade são apresentados, inclusive como utilizar o modelo de zonas e conduítes descrito na norma para assegurar sistemas de controle e supervisão (Scada).

2 MATERIAL E MÉTODOS

A Metodologia aplicada ao desenvolvimento deste trabalho é estritamente baseada na norma ANSI/ISA-99.
Elaborada pela ISA no ano de 2004 para estabelecer segurança da informação em redes industriais, a norma ANSI/ISA-99 é um conjunto de boas práticas que visa minimizar o risco de redes de sistemas de controle sofrerem Cyber-ataques.
A norma é composta de dois relatórios técnicos:

- Relatório Técnico ANSI/ISA-TR99.00.01-2007 – "*Security Technologies for Industrial Automation and Control Systems*":(4) este relatório técnico fornece métodos para avaliação e auditoria de muitos tipos de tecnologias de cybersegurança, métodos para mitigação, e ferramentas que podem ser aplicadas para proteger os sistemas de controle de automação industriais (IACS) de invasões e ataques. Para as variadas tecnologias, métodos e ferramentas detalhados neste relatório, uma discussão para seu desenvolvimento, implementação, operação, manutenção, engenharia e outros serviços de usuários são fornecidos. O relatório também fornece guias para fabricantes, revendedores e profissionais de segurança em empresas

capazes de aplicar contramedidas para segurança de IACS contra cyberataques.

- Relatório Técnico ANSI/ISA-TR99.00.02-2004 – "*Integrating Electronic Security into the Manufacturing and Control Systems Environment*":[5] este relatório técnico fornece um *Framework* para o desenvolvimento de um programa de segurança para sistemas de controle, fornecendo a organização recomendada e a estrutura para o plano de segurança. O Relatório fornece informação detalhada sobre os elementos mínimos a serem incluídos neste plano.

Dentro da norma ANSI/ISA-99 existe uma detalhada descrição de uma estratégia para defesa em profundidade denominada modelo de zonas e conduítes. Este modelo é usado para descrever os grupos lógicos de ativos dentro da empresa ou de um departamento da empresa. Os ativos são agrupados em entidades (ou seja, negócio, local da instalação, site ou sistema de controle industrial) que poderão então ser analisados para políticas de segurança e requerimentos de proteção.

O modelo ajuda a verificar ameaças comuns, vulnerabilidades, e as contramedidas correspondentes necessárias para atingir o nível de segurança necessário (SLT) para proteger o grupo de ativos. Ao agrupar os ativos, uma política de segurança poderá ser definida para todos os ativos que são membros de uma determinada zona. Esta análise pode ser usada para determinar a proteção apropriada necessária baseado nas atividades executadas em cada zona.

Na construção de um programa de segurança, as zonas são uma das ferramentas mais importantes para o sucesso do programa e a boa definição das zonas é o aspecto mais importante do processo. Ao definir as zonas, devem ser usadas a arquitetura de referência e modelo dos ativos para desenvolver zonas de segurança apropriadas e os níveis de segurança para satisfazer os objetivos de segurança estabelecidos na automação industrial e sistemas de controle de segurança comuns.

Quando diferentes níveis de atividades são realizadas dentro de um dispositivo físico, uma organização pode mapear o dispositivo físico para os mais rigorosos requisitos de segurança, ou criar uma zona separada com política de segurança própria, cuja política teria uma mistura de requisitos das duas zonas. Um exemplo típico deste processo ocorre em servidores de bancos de dados históricos. Para serem eficientes, os servidores tem acesso aos dispositivos de controle críticos que são a fonte dos dados a serem coletados. No entanto, para atender a necessidade das empresas de apresentar esses dados aos supervisórios e às equipes de processos de otimização, um acesso mais liberal ao dispositivo é necessário, se comparado aos típicos requisitos de segurança.

Se várias aplicações envolvendo diferentes níveis de atividades estão sendo executados em um único dispositivo físico, uma zona lógica de fronteira também pode ser criada. Neste caso, o acesso a uma determinada aplicação é restrita a pessoas que têm privilégios para aquele nível de aplicação. Um exemplo é uma única máquina rodando um servidor OPC e ferramentas de análises baseadas em clientes OPC. O acesso ao servidor OPC é restrito a pessoas com nível superior de privilégios, enquanto o acesso a planilhas utilizando cliente OPC plug-in está disponível para todos os empregados.

Conduítes são zonas de segurança que se aplicam a processos de comunicações específicas. Assim como as zonas de segurança, os condítes são um agrupamento lógico de ativos (ativos de comunicação neste caso). Um conduíte de segurança protege a segurança dos canais que ele contém, da mesma forma que conduítes físicos protegem cabos de danos físicos. Conduítes pode ser pensado como "tubos"

que conectam as zonas ou que são utilizados para a comunicação dentro de uma zona. Conduítes internos (dentro da zona) e externos (fora da zona) encapsulam ou protegem os canais de comunicações (conceitualmente cabos), que estabelecem as ligações entre os ativos. A maior parte das vezes, em um ambiente de sistemas de automação, o conduíte é o mesmo que uma rede. Isto é, o conduíte é o cabeamento, roteadores, switches e dispositivos de gestão de rede que compõem a comunicação em estudo.

Físicamente um conduíte pode ser um cabo que conecta zonas para fins de comunicação. O conduíte é um tipo de zona que não pode ter sub-zonas, isto é, um conduíte não é feita de sub-conduítes. Conduítes são definidas na lista de todas as zonas que compartilham os canais de comunicação. Tanto os dispositivos físicos quanto as aplicações que utilizam os canais contidos em um conduíte definem seus limites.

O conceito de nível de segurança foi criado para se pensar em uma zona de segurança como base em vez de um dispositivo individual base ou sistema base. Muitas vezes um sistema de automação e controle consiste em dispositivos e sistemas de múltiplos fornecedores, todos juntos para fornecer o funcionamento integrado de funções de automação industrial e operação. Assim como as capacidades funcionais de cada um dos dispositivos contribuem para a capacidade do sistema, as capacidades de segurança dos dispositivos individuais e as contramedidas implementadas devem funcionar uns com os outros para alcançar um nível desejado de segurança de uma zona. Níveis de segurança fornecem um quadro de referência para a tomada de decisões sobre o uso de contramedidas e dispositivos com diferentes capacidades de segurança inerentes. Níveis de segurança fornecem uma abordagem qualitativa para o endereçamento de segurança para uma zona. Como um método qualitativo, a definição de um nível de segurança tem aplicabilidade para comparar e gerenciar a segurança das zonas dentro de uma organização. Quanto mais dados se tornam disponíveis e as representações matemáticas de riscos, ameaças e incidentes de segurança são desenvolvidas, este conceito vai passar para uma abordagem quantitativa para a seleção e verificação dos níveis de segurança (SL). Ela terá aplicabilidade tanto para o usuário final, empresas e fornecedores de produtos de segurança e sistemas de automação e controle. Será usado para selecionar os dispositivos e contramedidas do sistema de automação a serem utilizados dentro de uma zona e para identificar e comparar a segurança das zonas em diferentes organizações entre segmentos da indústria.

Cada organização utilizando o método do nível de segurança deve estabelecer uma definição do que representa cada nível e como medir o nível de segurança para a zona. Esta definição ou caracterização deve ser utilizada de forma consistente em toda a organização. O nível de segurança deve ser utilizado para identificar uma estratégia abrangente de defesa em profundidade para uma zona que inclui contramedidas técnicas baseadas em hardware e software, juntamente com contramedidas administrativas.

3 RESULTADOS

A empresa na qual o trabalho foi desenvolvido é uma grande refinaria norte-americana com múltiplas áreas operacionais em suas instalações como destilação, hidrotratamento, reformadores catalíticos e utilitários (existem oito áreas operacionais, mas somente duas são mostradas para simplificar). A empresa

escolheu seguir os conceitos das normas ANSI/ISA-95.00.01-2000[6] e ANSI/ISA–99.02.012000,[7] dividindo seus processos operacionais em níveis que variam de zero a quatro.

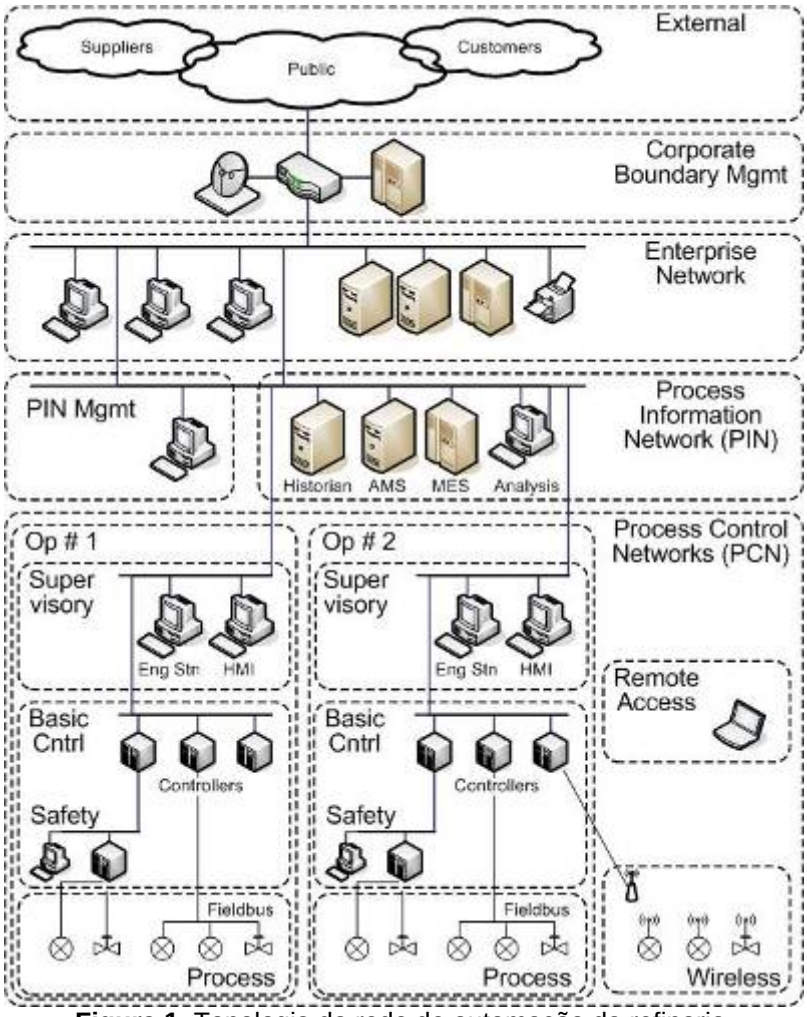

Figura 1. Topologia da rede de automação da refinaria.

Devido à natureza de suas operações, muitas (mas não todas) as suas operações necessitam de sistemas integrados de segurança. Na empresa também existem algumas áreas de controle que estão começando a usar tecnologia de redes sem fio. Finalmente, fornecedores (como por exemplo fabricantes de sistemas de controle) e clientes precisam interfacear com estes sistemas de controle a partir de redes externas.[8]

Adotamos o modelo de zonas e conduites preconizado pela norma ANSI/ISA-99 e dividimos os Sistemas em zonas baseadas em suas funções operacionais, níveis de processos, requerimentos de segurança e recursos de segurança. Todas as funções de controle foram designadas a pertencer a uma zona única de controle de processos (Zona A). Dentro desta zona existem outras zonas (O1, O2… On), uma para cada unidade operacional de destaque.

Desta forma os requerimentos de Segurança para uma operação particular podem ser ajustados para seus riscos potenciais (ou seja, a segurança para uma unidade com baixas consequências como a de águas residuais poderia ser relaxada se comparada com a unidade de recirculação de águas). Finalmente, as zonas

operacionais foram divididas em sub-zonas baseado no nível em que elas operam, conforme mostra a Figura 2:

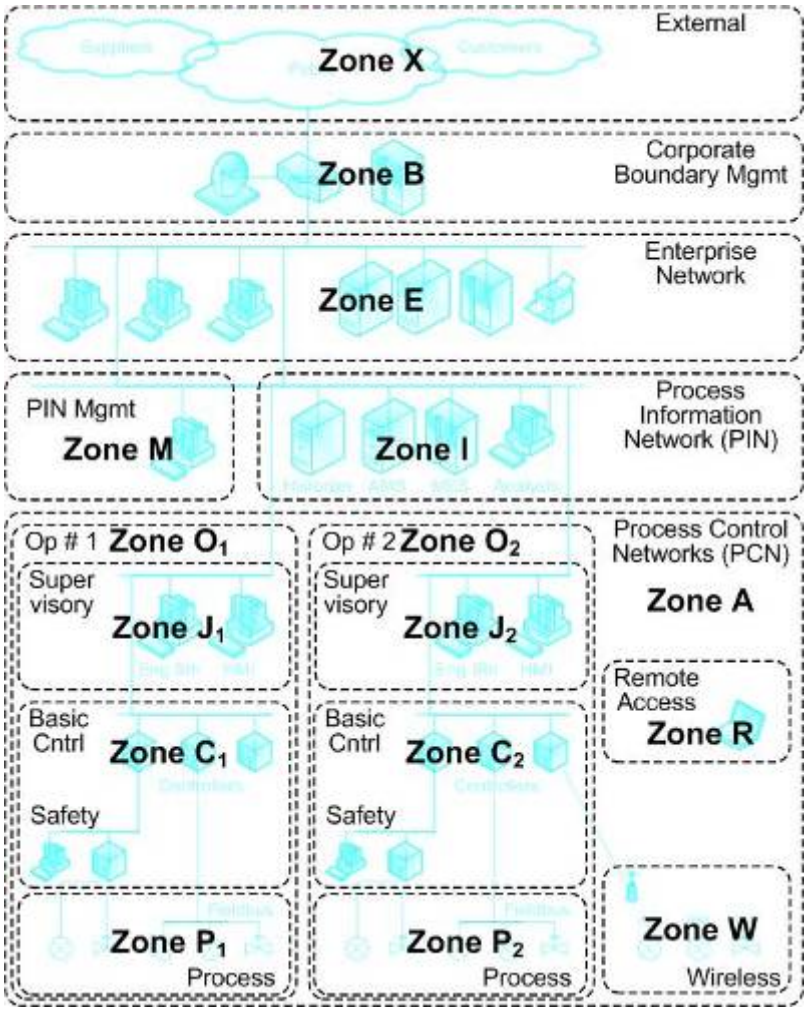

Figura 2. Rede de automação da refinaria dividida em zonas de segurança.

Cada zona foi definida com as seguintes caracterísitcas de zona (atributos) baseados na norma ANSI/ISA–99, com algumas pequenas adições, conforme apresenta o quadro abaixo, relativo à zona de segurança S1:

Quadro 1. Descritivo das características de uma zona de segurança.

ZONA: S1	**Nome da Zona:** Sistema de Segurança da unidade de recirculação de águas 1
Definição da Zona: Esta zona inclui todos os sistemas integrados de segurança da unidade de recirculação de águas 1.	
Agência Controladora: Departamento de automação de processos, equipe SIS.	
Função da zona: Os Sistemas nesta zona fornecem as funções de segurança da unidade de recirculação de águas 1.	
Perímetro da zona: O sistema integrado de segurança, como definido pelos estudos de periculosidade da área.	
Ativos típicos: O controlador do sistema integrado de segurança, estações de engenharia e equipamentos de comunicações.	
Heranças: Esta zona herda os atributos da zona C1 (controle básico da unidade de recirculação de águas 1).	
Análise de riscos da zona: Esta é uma zona moderadamente segura com consequências extremas se invadida.	
Recursos de Segurança dos ativos da zona: Assumimos que todos os ativos são incapazes de sobreviver a ataques de baixo nível (ou seja, aqueles lançados por malware e hackers sem sofisticação) contra sua disponibilidade e confidencialidade. Este é o resultado dos protocolos em uso e do projeto dos sistemas.	
Ameaças e vulnerabilidades: As vulnerabilidades desta zona são típicas de equipamentos de controle industriais usando MODBUS para suas comunicações. As principais ameaças são:	
• Ataques de negação de serviço (DoS) contras as comunicações do sistema.	
• Acesso interno ou externo não autorizado às estações de engenharia.	
• Spoofing de comandos de controle MODBUS/TCP.	
• Spoofing de respostas MODBUS/TCP aos processos do sistema.	
• Reprogramação de funções de segurança.	
Consequências das brechas de segurança:	
• Parada na produção superior a 6 horas caso o sistema de desligamento de emergência não funcione.	
• Parada na produção inferior a 6 horas dada a perda da visibilidade do sistema de segurança.	
• Desabilitação/manipulação de desligamento de emergência resultando em fatalidade ou incidentes ainda maiores.	
Consequências ao negócio: Extremas	
Objetivos de segurança: Proteger a integridade/disponibilidade do sistema de segurança da unidade de recirculação de águas 1.	
Políticas aceitáveis para o uso: Comunicações de I/O e Fieldbus é permitida para a zona P1 (processo da unidade de recirculação de águas 1). Acesso de leitura aos dados publicados é permitida para sistemas aprovados na zona C1 (sistema básico de controle da unidade de recirculação de águas 1). Todos os acessos de escrita a esta zona são proibidos. Todos as funções de gerência e programação devem ser internas a esta zona.	
Conexões entre zonas: Conduítes para esta zona devem ser estabelecidos desde a zona C1 (sistema básico de controle da unidade de recirculação de águas 1) e para a zona P1 (processo da unidade de recirculação de águas 1).	
Estratégias de segurança: Todas as conexões para esta zona devem ser controladas usando conduítes tipo S. Acesso a estes sistemas devem ser aprovados pela agência controladora.	
Processo de gestão de mudanças: Todas as mudanças nesta zona ou em qualquer um dos conduítes que se conectem a ela devem seguir o processo de gestão de aprovação de mudanças de sua agência controladora responsável (veja acima). Isto inclui mas não se limita à instalação ou troca de equipamentos, modificação de políticas de segurança, e exceções às políticas de segurança ou práticas existentes.	

Como ilustrado no exemplo acima, cada zona é definida não somente pelo seu perímetro, ativos e análise de riscos, mas também por seus recursos de segurança. Os conduítes entre as zonas fornecem as funções de segurança que permitem que duas zonas com diferentes perfis de segurança possam estar conectadas com segurança. Os conduítes não devem ser pensados como uma rede (entretanto eles devem ser baseados em tecnologia de rede com um switch com ACLs ou como um

access point de uma rede sem fio com serviços de criptografia), mas como um ponto no sistema que oferecerá funcionalidades de segurança.

Ao fazer os conduítes baseados em funcionalidades ao invés de baseados em tecnologia, podemos focar nos benefícios de segurança desejados. Da mesma forma, conduítes podem ser agrupados em classes funcionais para simplificar o projeto. Por exemplo, o conduíte tipo S (usado entre os sistema básico de controle e o sistema de Segurança) pode ser definido como capaz de fornecer as funções de controle de acesso e integridade, mas não funções de confidencialidade. Por outro lado, o conduíte tipo A (usado dentre as zonas PIN e corporative) pode ser definido como capaz de fornecer as funções de controle de acesso, integridade e confidencialidade. O tipo de tecnologia a ser usada no conduíte é irrelevante, o que importa é que ela forneça as funções de segurança requeridas pelo conduíte.

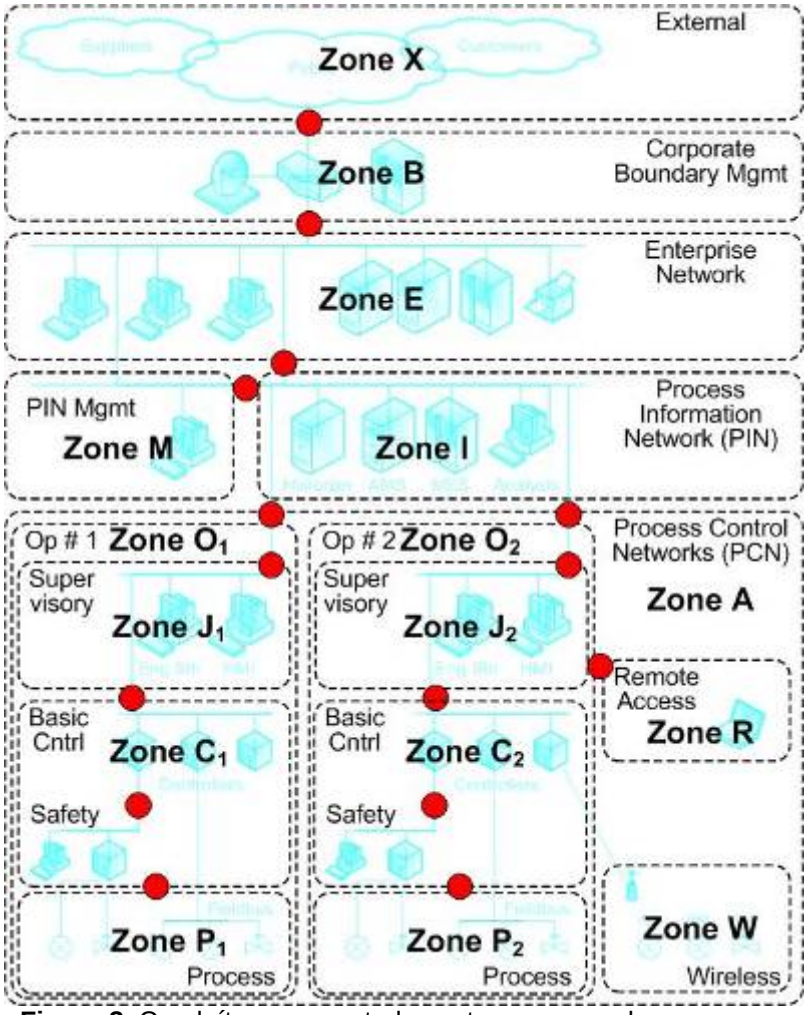

Figura 3. Conduítes apresentados entre as zonas de segurança.

Finalmente, entendendo os recursos de segurança dos equipamentos de uma zona é fundamental para assegurá-la. A apuração dos recursos de segurança deve ser baseada no menor denominador comum, e não na média. Por exemplo, uma zona contendo dez servidores windows 2003 com todos os patches em dia e um servidor windows NT sem nenhum patch instalado deve ser categorizada como uma zona com baixos recursos de segurança. Ao aplicar controles compensatórios ao servidor

NT (como um firewall dedicado na frente do servidor), então teremos uma melhoria no nível de segurança de toda a área.
Aplicando o modelo de zonas e conduítes determinamos que appliances de segurança com capacidades de Firewall deveriam ser instalados em cada conduítes que havia sido identificado na rede. Uma vez instalados os Firewalls, cada um deles foi ativado para filtrar todo o tráfego passando pelo conduíte. Foi necessário que os engenheiros de controle da refinaria configurassem regras para especificar quais equipamentos na rede seriam permitidos a comunicar através dos conduítes e quais protocolos eles poderiam usar, e os firewalls iriam bloquear qualquer outro tráfego que não se encaixasse nestas regras.

Exemplo: Protegendo a Zona S1

A Análise de Riscos realizadas durante a análise de zonas indicou que existia potencial para falhas comuns de rede entre a zona do supervisório (J1) e as zonas de sistemas integrados de segurança (S1). Desta forma era necessário aumentar a integridade das operações, limitando o tipo e as taxas de tráfego no conduíte (S)
A solução foi definir um conduíte entre as zonas J1 e S1 e utilizar um Firewall Industrial para MODBUS entre as duas zonas para aumentar os controles de tráfego entre elas, como está apresentado na Figura 3.

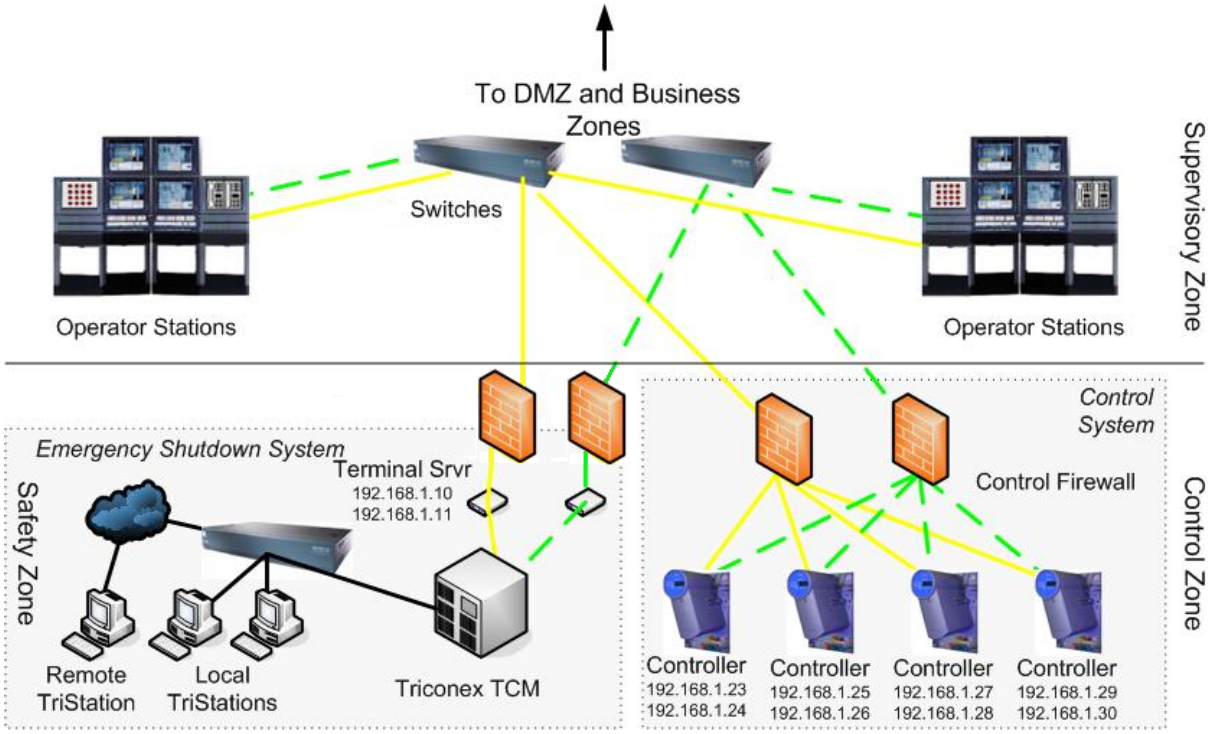

Figura 3. Arquitetura ilustrada da zona S1 protegida.

Além disso, para garantir a alta disponibilidade das zona, foram colocados dois Firewalls conectados entre os servidores terminais do sistema de segurança e os switches Ethernet de nível 2, fornecendo conexões redundantes entre o sistema de segurança e o sistema de controle. Foram escolhidos firewalls capazes de inspecionar o conteúdo MODBUS, oferecer alto MTBF e resistência industrial, suportar alimentação redundante e que fossem possíveis de serem configurados em

modo *bridge* ao invés de roteamento tradicionais. Esta configuração aumentou confiabilidade e diminuiu o custo de configuração, reduzindo consideravelmente o TCO da solução.
A escolha das soluções tecnológicas a serem aplicadas em cada conduíte podem variar dependendo do nível de segurança e de disponibilidade que cada área requer. A participação conjunta de engenheiros de controle e automação juntamente a profissionais de segurança da informação é fundamental para o sucesso de projetos com este perfil.

4 DISCUSSÃO

O retorno obtido em investimentos em segurança da informação nem sempre é tangível e na maioria dos casos ele é notado quando nenhum incidente de segurança ocorre.[9] Esta falta de tangibilidade no retorno destes investimentos é a principal barreira para que as empresas brasileiras façam investimentos mais significativos como o feito pela refinaria norte-americana que citamos neste trabalho.
Existem no mundo diversas iniciativas de catalogar os incidentes de segurança ocorridos em instalações industriais.[10] Dentre estas iniciativas a que mais se destaca é o ISID (*Industrial Security Incident Database*) do qual participam empresas de países como Estados Unidos, Alemanha, Austrália e França, dentre outros. O ISID é um serviço sem fins lucrativos mantido pela Byres Research e o BCIT (*British Columbia Institute of Technology*) para a indústria para registrar incidentes de Cyber-segurança que tenham diretamente afetado sistemas industriais SCADA e sistemas de controle de processos. Este banco de dados possui eventos de incidentes acidentais e também de atos intencionais com invasões externas, ataques DoS, e infiltrações de vírus e worms. Os dados são coletados de relatórios privados através de membros de empresas assim como dados de pesquisas em reportagens de incidentes que se tornaram públicos. Todos os registros feitos ao banco de dados são totalmente confidenciais. A segurança de toda a informação enviada é de crítica importância e todas as referências sensíveis são removidas (e não mascaradas), não havendo riscos para o colaborador ou sua empresa. Além disso, o banco de dados não está disponível online e os dados nunca são vendidos a companhias terceiras – o acesso somente é permitido às empresas colaboradoras.
As empresas brasileiras, por desconhecimento ou por tentativa de preservar suas imagens perante o mercado, não enviaram nenhum registro de incidentes de segurança em automação para estes bancos de dados internacionais como o ISID, o que faz com que o Brasil não figure na lista de países atacados e os gestores das empresas de nosso país pensem “Se aqui no Brasil estes ataques não acontecem, porque fazer caros investimentos nesta área?”.
Em consultorias desenvolvidas no Brasil pela empresa em que trabalho, temos obtido relatos de grandes indústrias nacionais que tem sofrido constantes infecções por malware que levaram inclusive à paralisação de áreas inteiras. Nenhum destes eventos foi registrado em bases de dados de incidentes ou mesmo divulgado internamente e em alguns casos os prejuízos foram enormes.
Fica para reflexão: não seria a hora destas empresas começarem a adotar estratégias de segurança para suas áreas industriais?

5 CONCLUSÃO

Novas tecnologias de redes e computadores introduzidos em sistemas de controle tem fornecido grandes melhorias na performance e produtividade das plantas. Entretanto, estes ganhos não continuarão a ser obtidos no futuro sem que ocorram melhorias correspondentes na segurança e confiabilidades das rede de controle. As melhores práticas especificadas na norma ANSI/ISA-99 fornecem um caminho a ser seguido pelas empresas para atingir e manter estas melhorias de segurança através de uma estratégia que integra projeto, implementação, monitoramento e melhorias contínuas.

Agradecimentos

Agradecemos às equipes técnicas da Byres Security Inc., no Canadá, e da TI Safe Segurança da Informação Ltda no Rio de Janeiro pelo apoio que nos foi prestado na elaboração do trabalho.

REFERÊNCIAS

1 CLARKE,R.A., KNAKE,R.K. Cyber War, Nova Iorque, EUA. 2010.
2 KRUTZ, R.L. Securing SCADA Systems, Indianápolis, EUA, 2006.
3 ISA, The Instrumentation, Systems, and Automation Society, ISA TR99.00.01-2004, Washington, EUA. 2004.
4 ISA, The Instrumentation, Systems, and Automation Society, ISA TR99.00.01-2004- Security Technologies for Manufacturing and Control Systems, Washington, EUA. 2004.
5 ISA, The Instrumentation, Systems, and Automation Society, ISA TR99.00.02-2004- Integrating Electronic Security into the Manufacturing and Control Systems Environment, Washington, EUA. 2004.
6 ISA, The Instrumentation, Systems, and Automation Society, ANSI/ISA-95.00.01-2000, Washington, EUA. 2000.
7 ISA, The Instrumentation, Systems, and Automation Society, ANSI/ISA–99.02.012000, Washington, EUA. 2000
8 KRAMER,F.D., STARR,S.H.,WENTZ,L.K. Cyberpower and National Security, Dulles, EUA. 2009.
9 IGURE, V.M., Security Assessment of SCADA Protocols, Saarbrucken, Alemanha. 2008.
10 CARR, J., Cyber Warfare, California, EUA. 2009.