A CYBERGUERRA BATE EM NOSSA PORTA.

ESTRATÉGIAS DE DEFESA USANDO A NORMA ANSI/ISA-99.

Marcelo Ayres Branquinho (marcelo.branquinho@tisafe.com),
Diretor Executivo da TI Safe Segurança da Informação.

A atividade de *hackers* do mundo inteiro em sites de entidades governamentais brasileiras e chamou a atenção da imprensa e do público em geral. O FBI (nos EUA) e órgãos governamentais brasileiros como a Receita Federal e o IBGE sofreram ataques que levaram à indisponibilidade de serviços e pichações de seus websites. Estes ataques chamam a atenção principalmente porque mostram como os *hackers* e suas ferramentas de ataque estão cada vez mais poderosas a ponto de conseguir burlar a segurança de sites tão bem protegidos como estes.

O fato dos ataques terem sido amplamente divulgados na mídia expôs ao mundo que não existe um site 100% seguro, e os *hackers* sabem muito bem disto. Sem pretender minimizar a gravidade destes ataques que mancham a imagem dos órgãos e expõem dados confidenciais, afirmo que infelizmente eles estão longe de ser a pior coisa que poderia nos acontecer no cenário mundial de cyberguerra [1]. Existem coisas piores, muito piores...

Se imaginarmos que a água que bebemos, a eletricidade que chega às nossas casas, a sinalização dos transportes de massa (inclusive aéreos), o controle de usinas hidroelétricas e nucleares, todos estes serviços são controlados por sistemas de computação que podem ser potenciais alvos de *hackers* do mundo inteiro, temos um cenário com um risco potencial muito maior. Imagine se ocorresse uma invasão em um sistema de controle de uma estação de tratamento de águas responsável pelo controle dos reagentes químicos que são misturados para purificar a água que é consumida pela população? E se um ataque hacker fosse capaz de desabilitar, mesmo que temporariamente, usinas hidroelétricas e nucleares causando blecautes nas cidades? Todas estas ameaças à infraestrutura crítica são hoje bastante reais.

Eventos recentes como o aparecimento do Worm Stuxnet [2] no ano passado (este *malware* ficou bastante famoso por ter paralisado o programa nuclear iraniano destruindo centrífugas em duas das principais usinas nucleares daquele país) representam uma virada no modo como as empresas e os governos devem enxergar a segurança, pois hoje os atacantes não são mais garotos que viram a noite tentando fazer uma pichação em uma página, e sim grupos de profissionais muito competentes e bem pagos bancados por organizações para o desenvolvimento de Cyber armas [3].

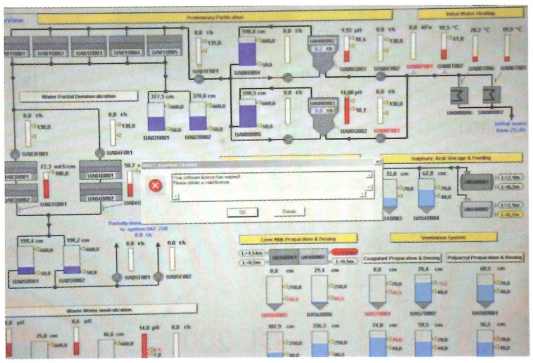

FIGURA 1 – Software SCADA de planta Nuclear Iraniana afetada pelo Stuxnet.

Fonte: http://www.computerworld.com/s/article/9188147/Iran_admits_Stuxnet_worm_infected_PCs_at_nuclear_reactor

O Stuxnet é um divisor de águas e mostra claramente que os sistemas de automação provavelmente serão os próximos alvos dos atacantes cibernéticos.

Em meu trabalho diário me deparo com diversas indústrias que estão bastante preocupadas com este tema, pois tem consciência que estão muito aquém do desejado no que diz respeito à segurança de suas plantas de automação. Algumas delas inclusive já sofreram infecções por *malware* que levaram à paralisação de áreas inteiras causando grandes prejuízos financeiros e risco de vidas humanas. Infelizmente as empresas que já acordaram para este tema no Brasil ainda são a exceção, quando deveriam ser a regra. A grande maioria das empresas ainda continua acreditando que nada vai lhes acontecer, e neste ponto podem estar cometendo um grande erro e comprometendo os sistemas que controlam as principais atividades produtivas de seus negócios.

A preocupação com ataques em plantas de automação não é recente. Já em 2004 a ISA (*International Society of Automation*) lançou 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 em todo o mundo [4].

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. Ela é composta de dois relatórios técnicos escritos em língua inglesa e pode ser obtida no website da ISA (www.isa.org):

- Relatório Técnico ANSI/ISA-TR99.00.01-2007 – "*Security Technologies for Industrial Automation and Control Systems*": este relatório técnico fornece métodos para avaliação e auditoria de muitos tipos de tecnologias de cyber segurança, 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, implantação, 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 cyber ataques.
- Relatório Técnico ANSI/ISA-TR99.00.02-2004 – "*Integrating Electronic Security into the Manufacturing and Control Systems Environment*": 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.

A norma ANSI/ISA-99 detalha uma estratégia para defesa em profundidade denominada modelo de zonas e conduítes. Este modelo é usado para descrever os grupos lógicos de ativos dentro de uma instalação industrial. 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 baseada 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. Na especificação das zonas de segurança deverá ser usada 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 executados dentro de um dispositivo físico, uma organização pode mapear este dispositivo físico para os mais rigorosos requisitos de segurança, ou criar uma zona separada com política de segurança própria que 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.

Assim como as zonas de segurança, os conduítes 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.

Fisicamente um conduíte pode ser um cabo que conecta zonas para fins de comunicação. O conduíte é um tipo de zona que não pode ter subzonas, isto é, um conduíte não é feito 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 é aplicado para zonas de segurança em vez de dispositivos individuais. Normalmente um sistema de automação e controle consiste em dispositivos e sistemas de múltiplos fornecedores integrados para fornecer as funcionalidades desejadas. 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.

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 passará 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 usada para selecionar os dispositivos e contramedidas a serem utilizadas 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.

Tomaremos como exemplo uma grande refinaria com múltiplas áreas operacionais em suas instalações como destilação, hidrotratamento, reformadores catalíticos e utilitários. A empresa escolheu seguir os conceitos das normas ANSI/ISA-95.00.01-2000 e ANSI/ISA–99.02.01, dividindo seus processos operacionais em níveis que variam de 0 (zero) a 4 (quatro).

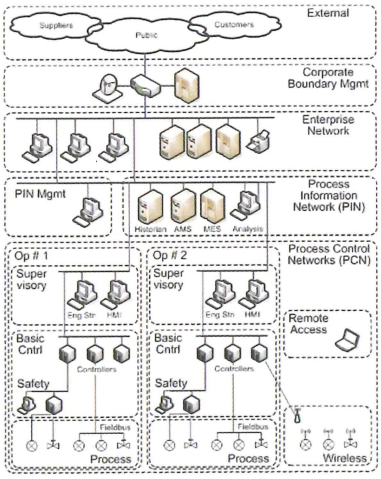

FIGURA 2 – Topologia da rede de automação da refinaria.

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 fabricantes de sistemas de controle, por exemplo) e clientes precisam trocar dados com estes sistemas de controle a partir de redes externas.

Adotando o modelo de zonas e conduítes, 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 subzonas baseado no nível em que elas operam, conforme mostra a Figura a seguir.

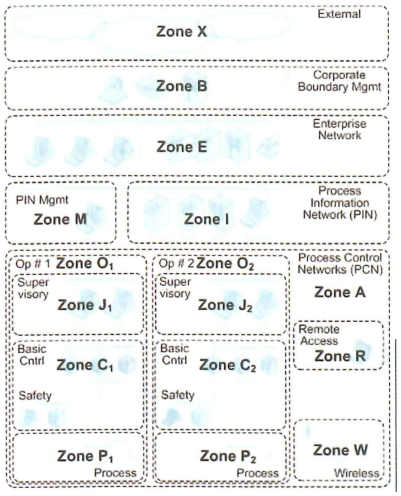

FIGURA 3 – Rede de automação da refinaria dividida em zonas de segurança.

Cada zona foi definida com as seguintes características de zona (atributos) baseados na norma ANSI/ISA–99, com algumas pequenas adições, conforme apresenta o quadro a seguir, relativo à zona de segurança C1.

QUADRO 1 – Descritivo das características de uma zona de segurança.

ZONA: C1 / 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 são permitidas para a zona P1 (processo da unidade de recirculação de águas 1). Acesso de leitura aos dados publicados é permitido 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. Todas 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 é possível notar neste quadro, 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 (*Access Control*

Lists – Listas de Controle de Acesso) 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 definir 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 o 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 entre as zonas PIN e corporativa) 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.

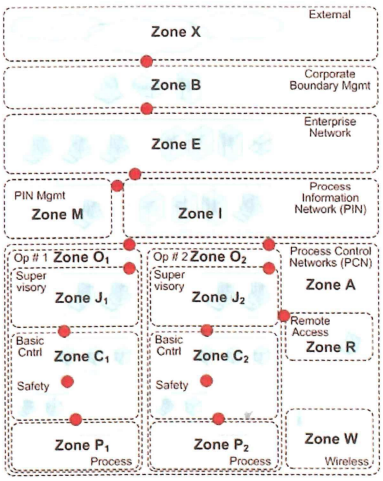

FIGURA 4 – Conduítes apresentados entre as zonas de segurança.

Finalmente, entender 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 equipamentos de segurança com capacidades de *firewall* deveriam ser instalados em cada conduíte que havia sido identificado na rede. Uma vez instalados os *firewalls*, cada um deles deveria ser ativado para filtrar todo o tráfego passando pelo conduíte. Para isto os engenheiros de controle da refinaria deveriam configurar 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 C1

A Análise de Riscos realizada durante a análise de zonas indicou que existia potencial para falhas comuns de rede entre a zona do supervisório (J1) e a zona de sistemas integrados de segurança (C1). Desta forma era necessário aumentar a integridade das operações, limitando o tipo e as taxas de tráfego no conduíte entre as zonas.

A solução foi definir um conduíte entre as zonas J1 e C1 e utilizar um *firewall* Industrial para MODBUS entre as duas zonas para aumentar os controles de tráfego entre elas, como está apresentado na Figura a seguir.

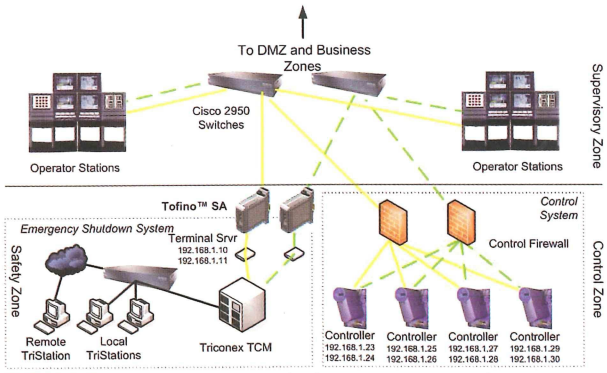

FIGURA 5 – Arquitetura ilustrada da zona C1 protegida.

Além disso, para garantir a alta disponibilidade da 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 tradicional. Esta configuração aumentou a confiabilidade e diminuiu o custo de configuração, reduzindo consideravelmente o TCO da solução.

A escolha das soluções tecnológicas a serem aplicadas em cada conduíte pode 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.

A aplicação da norma ANSI/ISA-99 em plantas de automação é a mais efetiva estratégia de defesa disponível e deve ser considerada pelas indústrias em seus planejamentos estratégicos. O cenário futuro que se desenha é bastante perigoso e os ataques tendem a aumentar e se tornar cada vez mais sofisticados, inclusive com o aparecimento de uma segunda geração de cyber armas que sucederão o Stuxnet. Chegou a hora de nossas indústrias atentarem para este cenário e começarem a adotar estratégias de segurança mais rígidas e baseadas em normas internacionais para seus sistemas e redes industriais, uma vez que estas redes e sistemas são parte fundamental do core business destas empresas.

REFERÊNCIAS

1. Palestra Técnica "Cyber-Terrorismo e a Segurança das Infraestruturas críticas" disponível na seção de segurança da automação no site da TI Safe Segurança da Informação, link http://www.tisafe.com/recursos/palestras/
2. Reportagem sobre o Stuxnet no site do Jornal Nacional, disponível em http://g1.globo.com/jornal-nacional/noticia/2010/11/supervirus-que-ataca-computadores-preocupa-servicos-secretos.html
3. CLARKE,R.A., KNAKE,R.K. Cyber War, Nova Iorque, EUA. 2010.
4. 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.
5. Palestra Técnica "O Uso de padrões abertos para segurança SCADA" disponível na seção de segurança da automação no site da TI Safe Segurança da Informação, link http://www.tisafe.com/recursos/palestras/

SOBRE O AUTOR

Engenheiro eletricista, com especialização em sistemas de computação com MBA em gestão de negócios, é membro da ISA Internacional, atualmente é diretor executivo da TI Safe Segurança da Informação onde atua como chefe do departamento de segurança para sistemas de automação industrial. Com larga experiência adquirida ao longo de 12 anos de atuação na área, coordenou o desenvolvimento da Formação de Analistas de Segurança de Automação, primeira formação brasileira no segmento e ministrada em infraestruturas críticas e organismos governamentais brasileiros. Atualmente participa do grupo internacional de estudos da ISA para revisão da norma ANSI/ISA-99.