Mini-Curso de Segurança de Automação Industrial

Versão 1.0
Outubro de 2014

São Paulo Section

TI Safe Segurança da Informação

Introdução ao curso

São Paulo Section

TI Safe Segurança da Informação

Instrutor

Marcelo Branquinho
Marcelo.branquinho@tisafe.com

- Engenheiro eletricista, com especialização em sistemas de computação com MBA em gestão de negócios e membro da ISA Seção RIODJ, atualmente é diretor da TI Safe Segurança da Informação onde também atua como chefe do departamento de segurança para sistemas de automação industrial.
- Com larga experiência adquirida ao longo de 14 anos de atuação na área, coordenou o desenvolvimento da Formação de Analistas de Segurança de Automação, sendo autor do livro "Segurança em Automação Industrial e SCADA", lançado em 2014.
- Atualmente é integrante do comitê internacional que mantém a norma ANSI/ISA-99.
- Possui certificação internacional CSSA (*Certified SCADA Security Architect*).

São Paulo Section

TI Safe Segurança da Informação

Objetivos

- Conscientizar profissionais a respeito dos principais riscos em redes industriais, bem como recomendar as principais contramedidas para os mesmos, de acordo com as principais normas de segurança internacionais.
- Apresentar soluções de segurança para redes industriais e SCADA

São Paulo Section

TI Safe Segurança da Informação

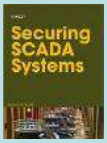
Referência Bibliográfica

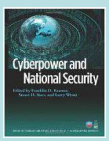
São Paulo Section

TI Safe Segurança da Informação

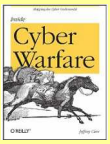
Literatura adicional

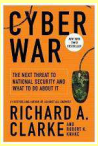
Literatura Básica





Ciberguerra e Ciberarmas





Eng. Social

São Paulo Section

TI Safe Segurança da Informação

Agenda

- Embasamento teórico sobre segurança de automação industrial
- A norma ANSI/ISA-99
- Entendendo os riscos em redes industriais e sistemas SCADA
- Segurança de borda da rede de automação
- Estratégias de defesa em profundidade
- Proteção da rede interna
- Treinamento e conscientização
- Dúvidas

Infraestruturas Críticas e Ciberterrorismo

O que são infraestruturas críticas?

São sistemas de infraestrutura para os quais a continuidade é tão importante que a perda, interrupção significativa ou degradação dos serviços poderia ter graves conseqüências sociais ou à segurança nacional.

Exemplos:

- ⇨ Geração e distribuição de eletricidade;
- ⇨ Telecomunicações;
- ⇨ Fornecimento de água;
- ⇨ Produção de alimentos e distribuição;
- ⇨ Aquecimento (gas natural, óleo combustível);
- ⇨ Saúde Pública;
- ⇨ Sistemas de Transportes;
- ⇨ Serviços financeiros;
- ⇨ Serviços de Segurança (polícia, exército)

Primeiros ataques aéreos – 1ª Guerra Mundial

- Aviões foram usados em combate pela primeira vez na primeira guerra mundial
- Trunfo: podiam bombardear a infraestrutura crítica de nações sem serem atingidos
- Na época, causaram grande terror à população e aos governos

Cyber War

- Cyber War ou Guerra Cibernética é (conceitualmente) apenas uma nova modalidade da guerra convencional.
- Principais diferenças:
  - Silenciosa
  - Anônima
  - Sem território definido
  - Sem reação
  - Quem? Como? De onde?

Guerra Convencional X Guerra Cibernética

Quanto custa um bombardeiro Stealth — **$1.5 a $2 bilhões**

Quanto custa um caça Stealth? — **$80 a $120 milhões**

Quanto custa um míssil de cruzeiro — **$1 a $2 milhões**

Quanto custa uma cyber arma? — **$300 a $50,000**

Encontre as armas de destruição em massa:

Fábricas de armas nucleares | **Fábricas de cyber-armas**

Onde estão as fábricas de cyber armas?

ISA São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

Antigamente...

Objetivo: Destruir

Chen-Ing Hau, 24
(Autor do vírus CIH)

ph McElroy, 16
o laboratório de pesquisas nucleares dos EUA)

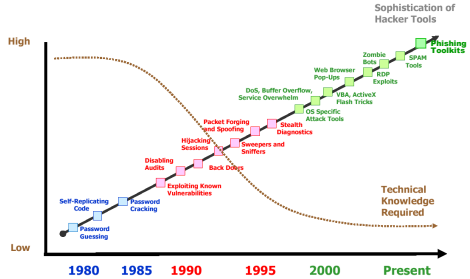
ISA São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

Os tempos mudaram...

"Script Kiddies", usando toolkits baixados da internet precisam de muito pouco conhecimento técnico para lançar um ataque!



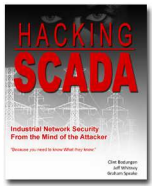
ISA São Paulo Section

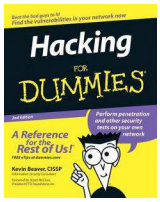
TI Safe Segurança da Informação

www.tisafe.com

Literatura Hacker

- A criticidade do uso e o impacto provocado por ataques a redes de automação aumentou o interesse de *hackers* em realizar ataques. Já existem livros ensinando como atacar uma rede industrial.





O que movimenta esse mercado?

Phishing

Pop ups & BOs

Sequestro de browser

Espionagem Industrial

É um negócio!

SPAM

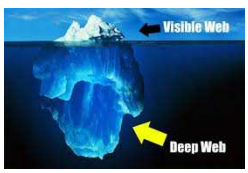
Roubo de identidades

Roubo de dados corporativos

Roubo de Dados pessoais

O Mercado do Cibercrime – Dark Web

- Duração: 4:18
- Este vídeo apresenta o mercado do crime cibernético movimentado na dark web (ou deep web).
- Áudio: Inglês (legendado em português)

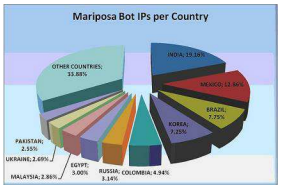


Venda de kits para Malware/Phishing

- "Fornecedores de armas"
- Venda de malware "somente para pesquisa"
- Tradução de manuais
- Suporte / Fóruns para usuários
- Linguagem específica,
- Referências para as empresas de hospedagem
- Geralmente não é ilegal
- Operam em países que os protegem de ações civis
- Torna mais fácil para entrar no mercado de cibercrime

Botnets

- Uma **botnet** é uma coleção de agentes de software ou bots que executam autonomamente e automaticamente.
- As principais motivações para levar alguém a criar e controlar botnets são o reconhecimento e o ganho financeiro.
- Quanto maior a botnet, mais admiração seu criador pode reivindicar entre a comunidade *underground*. Este poderá alugar os serviços da botnet para terceiros, usualmente mandando mensagens de *spam* ou praticando ataques de negação de serviço (DDOS) contra alvos remotos.



Crime de extorsão por DDOS

- "Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us. The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.
- **You will also receive several bonuses.** 1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about $ 100 per night, for you it will cost only 70 $ per day. 2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them."

Os novos atacantes

- Silenciosos
  - ⇨ Sem alarmes, sem vestígios
- Precisos
  - ⇨ Personalização, códigos específicos
  - ⇨ Tomam vantagem sobre fraquezas tecnológicas e humanas
- Patrocinados
  - ⇨ Por governos
  - ⇨ Por empresas concorrentes
  - ⇨ Por empresas de hacking
  - ⇨ Por grupos terroristas

ISA São Paulo Section

TI Safe Segurança da Informação

Ciberterroristas

- Grupos organizados custeados por governos de países ou organizações terroristas para promover o terrorismo ao redor do mundo.
- A infraestrutura crítica dos países é o alvo preferido destes grupos.
- Enquanto hackers se preocupam em roubar ativos da empresa, Ciberterroristas se dedicam a promover atos de destruição.
- Cyber-Jihad e Cyber Al-Qaeda são exemplos.

ISA São Paulo Section

TI Safe Segurança da Informação

Ciberespiões

- Ciberespionagem é a prática de usar computadores e tecnologia da informação para conseguir informação confidencial de um adversário.
- Diferentemente das técnicas tradicionais de espionagem, como plantar escutas telefônicas, as escutas cibernéticas são bem mais difíceis de serem detectadas.
- Uma vez que o espião tenha desenvolvido ou comprado uma escuta cibernética, a técnica mais comum de plantá-la é por email. Entretanto deve ser notado que já foram encontrados códigos espiões no firmware de equipamentos eletrônicos fornecidos por empresas estrangeiras, principalmente chinesas.

ISA São Paulo Section

TI Safe Segurança da Informação

Hacktivistas

- Hacktivismo é o ato de invadir sistemas de computação por motivos políticos ou sociais.
- O indivíduo que realiza atos de Hacktivismo é denominado Hacktivista.
- Alguns grupos hacktivistas famosos:
  - ⇨ Anonymous: http://anonymous.pysia.info/
  - ⇨ Lulzsec: http://lulzsecbrazil.net/
  - ⇨ Team Web Ninjas: http://hackmageddon.com/tag/web-ninjas/

ISA São Paulo Section

TI Safe Segurança da Informação

Guerreiros cibernéticos (Cyber Warriors)

- São pessoas que se engajam na guerra cibernética, seja por razões pessoais, patriotismo ou crenças religiosas.
- Ciberguerreiros podem atacar computadores ou sistemas de informação através de hacking ou outras estratégias relacionadas, ou defendê-los dos seus inimigos.
- Eles também podem encontrar melhores maneiras de proteger um sistema ao encontrar vulnerabilidades por meio de técnicas de hacking e anulando estas vulnerabilidades antes que os inimigos a explorem.
- Ciberguerreiros são frequentemente contratados por governos de países e organizações militares.

ISA São Paulo Section

TI Safe Segurança da Informação

A Ameaça Interna

- Grande parte das invasões realizadas em sistemas de tecnologia corporativos têm participação de funcionários ou ex-funcionários das empresas. A afirmação feita há alguns meses pelo detetive britânico Chris Simpson - da unidade de crimes de computação da polícia metropolitana londrina - é reforçada no Brasil pelo IPDI (Instituto de Peritos em Tecnologias Digitais e Telecomunicações).
- Segundo o IPDI, 80% dos golpes realizados no ambiente corporativo, sejam on-line ou off-line, contam com colaboração interna.
- Esta tendência, aliada à popularização do uso da tecnologia, facilita o roubo de informações, espionagem industrial, sabotagem, entre outros tipos de crime.

Fonte: http://www1.folha.uol.com.br/folha/informatica/ult124u19452.shtml

TI Safe Segurança da Informação

Ataques a redes e sistemas industriais no exterior

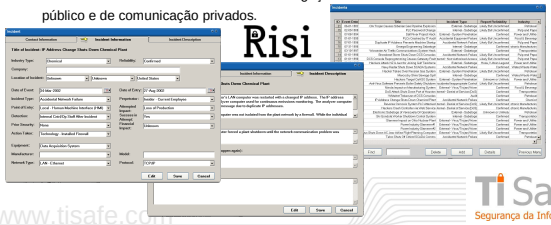
Shodan

SHODAN Computer Search Engine http://www.shodanhq.com

- Hackers estão usando o site de busca Shodan para encontrar computadores de sistemas SCADA que utilizam mecanismos potencialmente inseguros para autenticação e autorização.

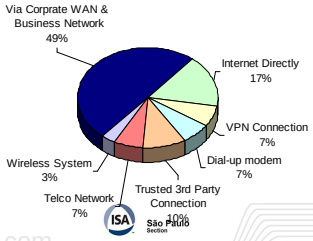
Repository for Industrial Security Incidents

- http://www.securityincidents.org/
- O Repositório de Incidentes de Segurança Industrial é um banco de dados de incidentes que têm (ou podem ter) afetado controle de processos e sistemas SCADA.
- O objetivo da RISI é coletar, investigar, analisar e compartilhar importantes incidentes de segurança industrial entre as empresas associadas para que elas possam aprender com as experiências dos outros.
- Os dados são recolhidos através da investigação sobre incidentes de conhecimento público e de comunicação privados.



Como os atacantes entram...

a) Laptops de terceiros infectados com Malware e conectados diretamente à rede de automação
b) Conexões 3G não autorizadas e redes sem sem fio, ou através da rede corporativa
c) Atos intencionais de funcionários insatisfeitos
d) Conexões via modem
e) VPNs

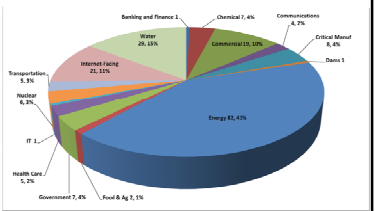


Segurança em sistemas SCADA é preocupante

ICS-CERT MONITOR

Vulnerability Type	
Buffer Overflow	44
Input Validation	13
Resource Exhaustion	8
Authentication	8
Cross-site Scripting	8
Path Traversal	8
Resource Management	8
Access Control	7
Hard-coded Password	7
DLL Hijacking	6
SQL Injection	4
Credentials Management	3
Cryptographic Issues	3
Insufficient Entropy	3
Use After Free	3
Use of Hard-coded Credentials	2
Cross-Site Request Forgery	2
Privilege Management	2
Write-what-where Condition	2
Integer Overflow or Wraparound	2
Inadequate Encryption Strength	2
Missing Encryption of Sensitive Data	1
Code Injection	1
Forced Browsing	1
Miscellaneous	15
Total	171

ICS-CERT Incidents by Sector – Fiscal Year 2012



Incidentes SCADA na ficção – Die Hard 4

Bomba lógica destrói oleoduto na Sibéria

- Em 1982, durante a guerra fria, os planos de um sofisticado sistema SCADA para controle de oleoduto foram roubados pela KGB de uma empresa canadense.
- A CIA alega que esta empresa detectou o ataque e inseriu uma bomba lógica no código roubado para sabotar e explodir o oleoduto.
- A explosão foi equivalente a um poder de 3 Quilotons de TNT. A explosão foi tão poderosa que satélites americanos enviaram alertas nucleares aos centros de controle nos EUA.

Oleoduto explode em Bellingham (EUA)

01/06/1999

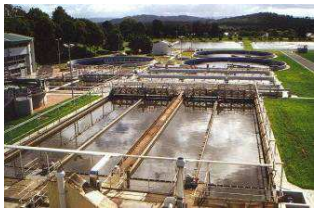
- Falhas no SCADA resultaram na explosão do oleoduto.
- Gasolina atingiu dois rios nas cidades de Bellingham e Washington.
  - ⇨ Explosão matou 3 pessoas e feriu 8.
  - ⇨ Aproximadamente 26 hectares de árvores e vegetação foram queimados durante o incidente.
  - ⇨ Liberou aproximadamente 236.000 galões de gasolina, causando danos substanciais ao meio ambiente.

É possível quantificar o prejuízo de um incidente como estes?

Ataque à ETR de Maroochy Shire

31/10/2001

- Ataque ao sistema de controle de tratamento de resíduos de Maroochy Shire em Queensland, Austrália.
- A Planta passou por uma série de problemas: bombas não acionavam quando comandadas, alarmes não estavam sendo reportados, e havia uma perda de comunicações entre o centro de controle e as estações de bombas.
- Estes problemas causaram o alagamento do terreno de um hotel próximo, um parque, e um rio com mais de 7 milhões de litros de esgoto bruto.



Ataque à Usina Nuclear de Davis-Besse

- Em 25/01/2003, a usina nuclear Davis-Besse usina nuclear em Oak Harbour, Ohio, foi infectada com o worm "Slammer" do MS SQL.
- A infecção causou sobrecarga de tráfego na rede local. Como resultado, o Sistema de Segurança de Display de Parâmetros (DOCUP) ficou inacessível por quase 5h, e o computador de processos da planta por mais de 6h.

- Um firewall estava no local para isolar a rede de controle da rede da empresa, no entanto, havia uma conexão T1 a partir de uma empresa de consultoria de software, que entrou na rede de controle por trás do firewall, ignorando todas as políticas de controle de acesso impostas pelo firewall corporativo.
- O worm infectou servidor do consultor e foi capaz de entrar na rede Davis-Besse através da linha T1.

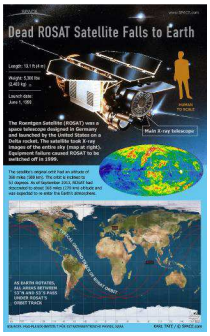
Transporte Ferroviário – Ataque à CSX

20/08/2003

- Sistema de sinalização ferroviário da CSX
- Virus Sobig causa desligamento dos sistemas de sinalização da costa leste dos EUA
- Virus infectou a base de controle da Flórida, desligando sinalização e outros sistemas de controle ferroviário
- Trens que fazem percursos de longas distâncias foram atrasados entre 4 a 6 horas

Ataque a centro de comando derruba satélite

- Em 2008 investigadores da NASA reportaram que uma falha no ROSAT estava ligada à uma cyber invasão no Goddard Space Flight Center, centro de comando do satélite.
- Segundo o relatório da NASA: "Atividades hostis comprometeram sistemas de computadores que direta ou indiretamente lidam com o controle do ROSAT"
- Após sucessivas falhas nos meses seguintes, em 23/10/11 o satélite alemão ROSAT explodiu ao reentrar na atmosfera terrestre. Seus destroços caíram em áreas inabitadas do planeta não causando vítimas.



Ataque à ETA de South Houston (EUA)

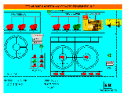
18/11/2011

- Hacker invadiu e publicou em blog imagens dos supervisórios do SCADA da ETA de South Houston, provando que poderia ter operado a planta
- http://pastebin.com/Wx90LLum

Hacker penetrates South Houston's water supply network

'pr0f' posts proof-of-concept attack results

Written by Gareth Halfacree on 18 November, 2011 NEWS > SECURITY



Fears that digital ne'er-do-wells could gain illicit access to a nation's electricity, gas or water infrastructure via the internet have proven well-founded as a hacker known as 'pr0f' posts proof of an attack on South Houston's water supply.

The attack was born when 'pr0f' read a quote from Department of Homeland Security's Peter Boogaard made in response to an article on The Register claiming that an electronic attack had damaged water pump in Illinois. "DHS and the FBI are gathering facts surrounding the report of a water pump failure in Springfield Illinois," Boogaard stated. "At this time there is no credible corroborated data that indicates a risk to critical infrastructure entities or a threat to public safety."

"This was stupid," 'pr0f' writes in a missive posted to hacker hangout Pastebin. "You know. Insanely stupid. I dislike, immensely, how the DHS tend to downplay how absolutely F****D the state of national infrastructure is. I've also seen various people doubt the possibility an attack like this could be done."

ISA São Paulo Section

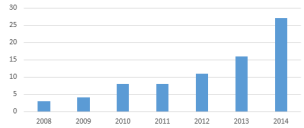
TI Safe Segurança da Informação

www.tisafe.com

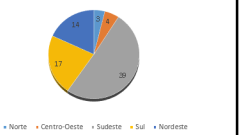
Incidentes de segurança em industrias no Brasil

- Fonte: 1º Relatório Anual TI Safe sobre incidentes de segurança em redes de automação brasileiras
- Incidentes computados de Setembro de 2008 a Abril de 2014
- Dados obtidos somente de clientes da TI Safe no Brasil

Evolução dos incidentes de segurança em redes de automação de clientes da TI Safe no Brasil - dados de 09/2008 a 04/2014



Incidentes de segurança em redes de automação brasileiras por região geográfica, de 2008 a 2014



ISA São Paulo Section

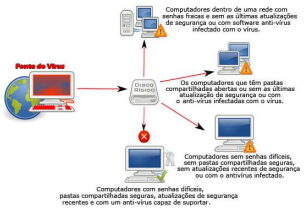
TI Safe Segurança da Informação

www.tisafe.com

Malware – O principal vilão

- O DOWNAD, mais conhecido como "Conficker", dominou a contagem de malware em plantas industriais no Brasil.
- Dos 27 casos documentados em nosso estudo, 14 foram derivados de infecções do Conficker.
- Isso acontece porque plantas de automação não são atualizadas com os últimos *patches*, deixando-as expostos a malwares como o Conficker.
- Além disso, boa parte das plantas industriais brasileiras não possui política de segurança adequada, medidas para controle de acesso à rede de automação e proteção de portas USB.

Vírus Conficker Win32



ISA São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

Estudo de Caso – Grande Siderúrgica Nacional

- **Malware e sua variante**: Conficker Win32
- **Número de máquinas infectadas:** toda a rede, mais de 30 computadores entre eles servidores, estações de engenharia, estações de operação e gateway. "Não estou mencionando os problemas do complexo siderúrgico. Apenas relatei a Termelétrica. Houveram outras infecções nas demais unidades como Alto Forno, Sinter, Coqueria e Distribuição de Energia".
- Existia anti-virus na planta, porém **estava com as assinaturas desatualizadas**.
- **Principais consequências da infecção:** operação as cegas até o isolamento total do problema. Entre 2 e 4 horas correndo risco.
- **Houve prejuízos financeiros quantificáveis?** Não, mas tivemos que explicar o ocorrido para o O.N.S.
- **Como foi o processo de desinfecção e quanto tempo levou?** A desinfecção para retornar a operação segura 4 horas, mas no total levaram mais de 30 dias até podermos estabelecer todas as interfaces. A última interface estabelecida foi com a rede corporativa até obtermos total segurança da rede.
- **Foi descoberta a origem da infecção?** Não. Na época era difícil porque a planta estava em comissionamento e havia muitas interfaces trabalhando nessas redes.

ISA São Paulo Section

TI Safe Segurança da Informação

Hackers causaram blecautes no Brasil?

- Duração: 3:58
- Este vídeo mostra reportagem da CBS onde o presidente norte-americano, Barack Obama, afirma saber de blecautes em outros países devido a ataques
- A CBS atribui os ataques aos blecautes Brasileiros ocorridos no Rio de Janeiro (Jan/05) e no Espírito Santo (Set/07)
- Áudio: Inglês (legendado em português)

ISA São Paulo Section

TI Safe Segurança da Informação

A norma ANSI/ISA 99

- Norma elaborada pela ISA (*The Instrumentation Systems and Automation Society*) para estabelecer segurança da informação em redes industriais
- É um conjunto de boas práticas para minimizar o risco de redes de sistemas de controle sofrerem Cyber-ataques
- Atualmente sendo revisada em função do surgimento do Stuxnet

TECHNICAL REPORT

ANSI/ISA—TR99.00.02—2004
ANSI Technical Report prepared by ISA

Integrating Electronic Security into the Manufacturing and Control Systems Environment

Approved 19 October 2004

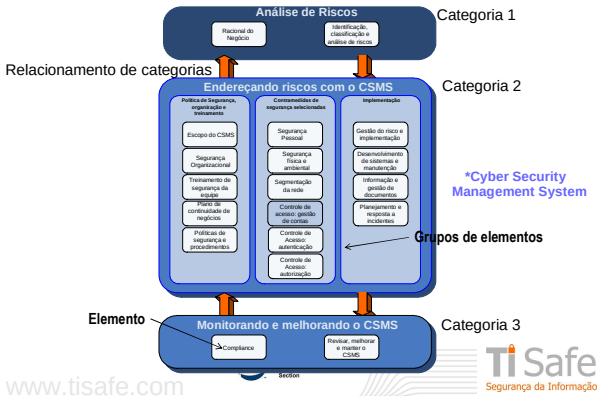
ISA São Paulo Section

TI Safe Segurança da Informação

Relatórios Técnicos da ISA 99

- **ANSI/ISA-TR99.00.01-2007** – "Security Technologies for Industrial Automation and Control Systems"
  - ⇨ Fornece métodos para avaliação e auditoria 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.
- **ANSI/ISA-TR99.00.02-2004** – "Integrating Electronic Security into the Manufacturing and Control Systems Environment"
  - ⇨ Framework para o desenvolvimento de um programa de segurança para sistemas de controle
  - ⇨ Fornece a organização recomendada e a estrutura para o plano de segurança.
  - ⇨ O Framework está integrado no que é chamado de CSMS (*Cyber Security Management System*)
  - ⇨ Os elementos e requerimentos estão organizados em 3 categorias principais:
    - Análise de Riscos
    - Endereçando os riscos com o CSMS
    - Monitorando e melhorando o CSMS

ANSI/ISA-TR99.00.02-2004: Estabelecendo um programa de segurança de sistemas de controle e automação industrial



As Etapas para a implementação do CSMS

1. Análise de Riscos
   - Racional do negócio, identificação de riscos, classificação e análise
2. Endereçando riscos com o CSMS
   - Política de Segurança, Organização e Treinamento
     - Definir escopo, segurança organizacional, treinamento da equipe, plano de continuidade de negócios, políticas e procedimentos
   - Selecionar contramedidas de segurança
     - Segurança pessoal, segurança física, segmentação de rede, controle de acesso, autenticação e autorização
   - Implementação
     - Gerência de riscos e implementação, desenvolvimento e manutenção de sistemas, gestão da informação e documentos, planejamento de incidentes
3. Monitorando e melhorando o CSMS
   - Compliance
   - Revisar, melhorar e manter o CSMS

Entendendo os riscos em redes industriais e sistemas SCADA

São Paulo Section

TI Safe Segurança da Informação

Análise de riscos em redes industriais

- Segue basicamente o mesmo fluxo que as análises de riscos de sistemas convencionais
- O que muda são as ameaças e os riscos aos quais os sistemas SCADA estão submetidos
- A Análise de Riscos em redes industriais e sistemas SCADA é parte integrante da norma ANSI ISA-99 e é a primeira etapa na implementação do CSMS

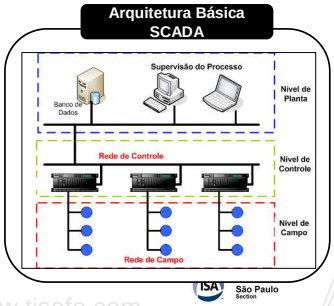
São Paulo Section

TI Safe Segurança da Informação

As Ilhas de automação

Sistemas SCADA, algumas décadas atrás:

- Sistemas proprietários, totalmente dependente de fabricantes.
- Sistemas isolados com arquiteturas fechadas - "Ilhas de automação".

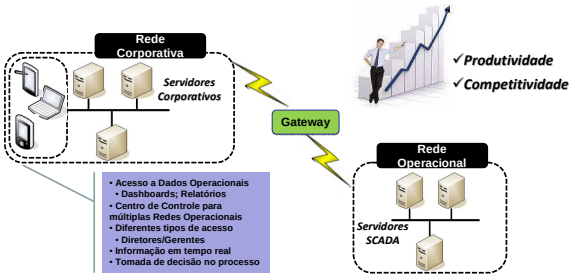


São Paulo Section

TI Safe Segurança da Informação

A evolução dos sistemas SCADA

- Sistemas abertos com arquitetura centrada em conectividade.
- Integrações cada vez mais freqüentes com a Intranet corporativa e Internet.

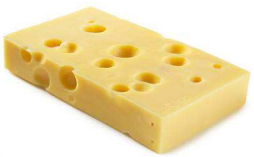


A evolução dos sistemas supervisórios

- No início os sistemas supervisórios eram desenvolvidos em plataformas operacionais caríssimas, baseadas em sistemas Unix like e máquinas poderosas como os Digital Vax e Alpha.
- Desenvolver aplicativos para estas plataformas era algo extremamente caro.
- Com isto, supervisórios passaram a ser desenvolvidos para plataformas Windows, cujo processo de desenvolvimento era muito mais rápido e os custos globais do projeto eram bastante reduzidos.

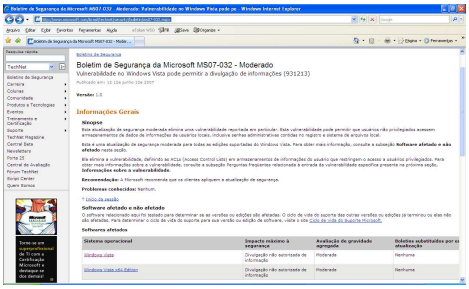
Tipos de Vulnerabilidades

- Vulnerabilidades dos Sistemas Operacionais e Protocolos.
- Vulnerabilidades no Projeto dos Produtos.
- Vulnerabilidades das Implementações.
- Vulnerabilidades de Configurações Inadequadas.



Vulnerabilidades no Windows

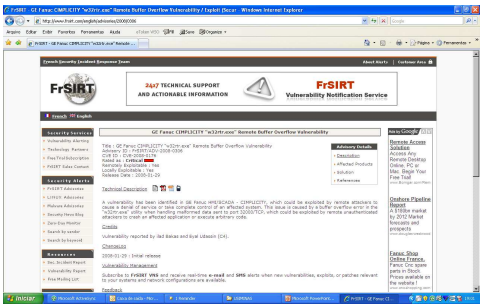
A Microsoft libera boletins periódicos e atualizações de segurança para seus sistemas operacionais e aplicativos - http://technet.microsoft.com/pt-br/security/bulletin/



São Paulo Section

TI Safe Segurança da Informação

Vulnerabilidades e Exploits para SW SCADA



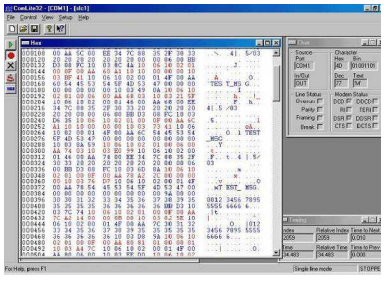
http://www.frsirt.com/english/advisories/2008/0306

São Paulo Section

TI Safe Segurança da Informação

Cracking de senhas em PLCs

É possível monitorar a comunicação entre o Supervisório e o PLC através da porta COM e obter as senhas (Principal e Master) do PLC.



São Paulo Section

TI Safe Segurança da Informação

Injeção de código em PLCs

- Ataque de injeção de código: uma bomba relógio com 14 bytes
- Desenvolvido por Ralph Langner, este ataque não necessita de informação interna e nenhuma programação ao nível da controladora para ser executado
- É inspirado no ataque do Stuxnet contra sistemas de controle
- O ataque consiste em injetar o código ao lado no início da varredura principal (OB1), na frente do código legítimo
- Para cada chamada do OB1, o ambiente de execução passa a data/hora atual como um parâmetro para a pilha, então nenhuma chamada de função de sistema é necessária.
- No exemplo ao lado, a data/hora programada é o natal de 2011, que é simplemente carregada no acumulador ao lado da data hora atual.
- A partir daí, é feita uma comparação. Assim que o relógio interno do controlador vai para 25 de dezembro, as saídas são congeladas, porque a directiva BEC salta execução da lógica de controle legítimos.

Código do ataque (Step7 STL)

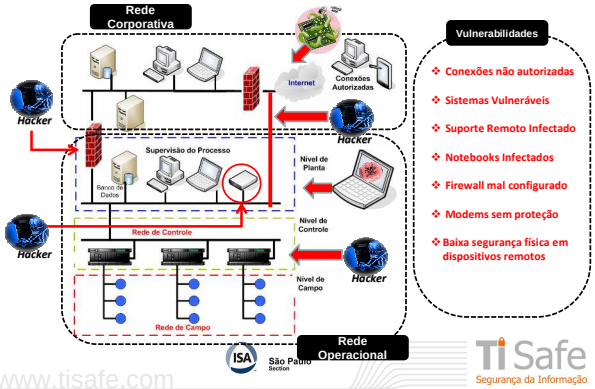
```
L    LD   12
L    DW#16#11122500
>=D
BEC
```

http://www.langner.com/en/2011/07/21/a-time-bomb-with-fourteen-bytes/

Vulnerabilidades no Protocolo OPC

Vulnerabilidade	Boa Prática
Atualizações e patches inadequados no servidor	Siga a orientação do vendedor OPC e diretrizes organizacionais.
Serviços de sistema desnecessários	Desative serviços desnecessários e garanta que os servidores OPC são plataformas para este único propósito.
Acesso desnecessário ao servidor, proveniente de outros dispositivos	Use o Windows IP Filtering
Enumeração do sistema e seus perfis	Desative serviços desnecessários e confirme através de escaneamentos de vulnerabilidades programadas
Senhas fracas e vulneráveis	Siga as bos práticas da indústria e a política estabelecida na empresa.
Navegação remota na Registry	Desative a edição remota da Registry.
Segurança inadequada no Login	Habilite a auditoria do sistema para objetos OPC e DCOM para identificar tentativas de acesso não autorizado.

Vulnerabilidades em redes industriais



Vulnerabilidades

- Conexões não autorizadas
- Sistemas Vulneráveis
- Suporte Remoto Infectado
- Notebooks Infectados
- Firewall mal configurado
- Modems sem proteção
- Baixa segurança física em dispositivos remotos

Vulnerabilidades comuns em SCADA

Arquitetura de rede insegura

- Configuração de servidores de FTP, web e e-mail de maneira inadvertida ou sem necessidade fornecem acesso à rede interna da empresa.
- Conexões de rede com parceiros de negócios não protegidas por Firewalls, IDS ou VPN são portas de entrada para invasões.
- Modems habilitados, sem mecanismos fortes de controle de acesso.
- Firewalls e outros dispositivos de segurança de rede não implementados internamente, deixando pouca ou nenhuma separação entre as redes corporativa e de automação.
- Redes sem fio configuradas sem segurança adequada.
- PLCs não requerem autenticação para serem usados.
- Softwares de supervisórios possuem vulnerabilidades publicadas na Internet.
- Pontos de rede de dispositivos no campo como CLPs e remotas estão diretamente conectados à rede de automação e podem ser porta de entrada para ataques.

Vulnerabilidades comuns em SCADA (Cont.)

Falta de monitoramento em tempo real

- LOGs de equipamentos de segurança não são analisados, impedindo o pessoal de segurança de redes de reconhecer ataques individuais
- Empresas não utilizam software especialista para gestão de logs e incidentes

Bombas Lógicas

- Pedaços de código intencionalmente inseridos em um sistema de software que irá executar uma função maliciosa quando condições específicas forem atingidas.

Falta de Conhecimento e crença em mitos

- "Nossa rede de automação não está conectada à Internet, então não temos nenhum problema"
- "Nossos funcionários são 100% confiáveis"

Segurança de Borda da Rede de Automação

Firewalls

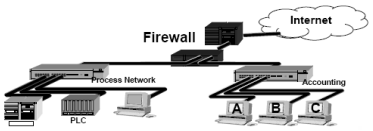
São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

Firewall

- Um firewall é um mecanismo usado para controlar acesso de e para uma rede com o objetivo de protegê-la.
- Os firewalls devem ser postos entre duas entidades de rede que estejam em diferentes níveis de confiabilidade.
- Evoluíram de simples filtros de pacotes a sofisticadas ferramentas de controle pró-ativo.
- Podem trabalhar junto a sistemas de detecção de intrusos e anti-vírus.



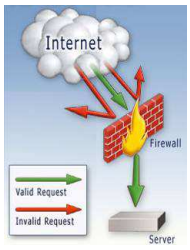
São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

Tipos de firewall usados em redes de T.I.

- Existem dois tipos básicos de firewalls e cada um atua em uma camada diferente.
- Camada de Aplicação
  - Operam através de regras pré-estabelecidas. Nesse sistema de filtros podem de maneira simples bloquear serviços como: Troca de mensagens instantâneas, troca de arquivos, telnet, entre outros, como também liberar o acesso HTTP e POP, por exemplo.
- Camada de Rede
  - Tomam suas decisões baseados nas portas e nos endereços de origem e destinos dos pacotes.

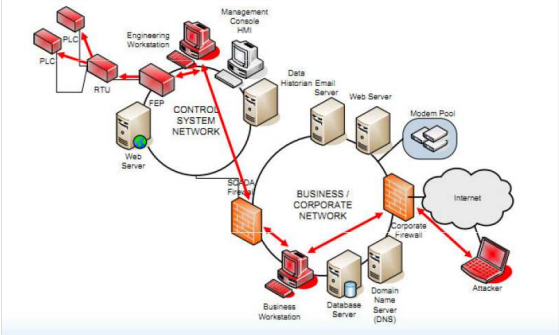


São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

Típico ataque a sistemas SCADA



Arquiteturas de Firewall

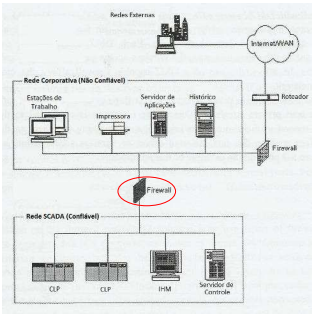
Zonas de segurança em redes industriais

- **Confiáveis**
  - Dispositivos SCADA dedicados e rede de automação.
  - Dispositivos de campo.

- **Não Confiáveis**
  - Internet.
  - Rede Corporativa.
  - Redes de Parceiros e Fabricantes.

a) Firewall separando as redes

- É recomendado o uso de um Firewall entre a rede de automação e a rede corporativa da empresa.
- Arquitetura mais básica e frequentemente encontrada em indústrias brasileiras.
- Regras diretas de comunicação entre rede SCADA e corporativa:
  - ⇨ Baixo nível de segurança.
  - ⇨ Susceptível a ataques de baixa complexidade.



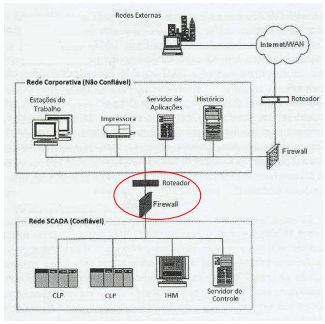
São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

b) Firewall e roteador separando redes

- Arquitetura um pouco mais sofisticada.
- Roteador é mais rápido e filtra pacotes indesejáveis antes que eles cheguem ao firewall.
- A redução do número de pacotes melhora o desempenho da rede.
- Maior segurança pois um atacante terá que desabilitar dois equipamentos.



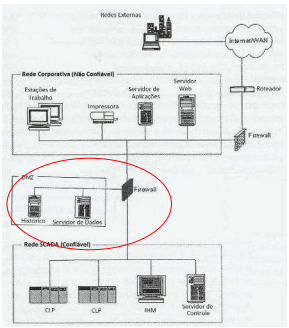
São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

c) Firewall com DMZ entre as redes

- Arquitetura que cria uma zona semi-confiável (DMZ) para a colocação de equipamentos que tenham que ser acessados pela rede corporativa e de controle.
- Nenhuma comunicação direta entre a rede corporativa e de automação passa a ser necessária.
- Cada caminho de comunicação terminará sempre na DMZ.
- Risco: um computador comprometido na DMZ poderá atacar a rede de controle usando tráfego de rede válido de aplicativos.



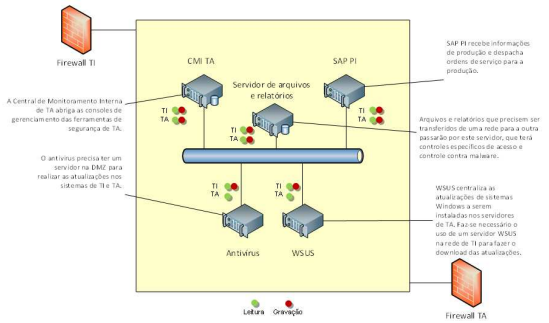
São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

DeMilitarized Zone – DMZ

Segmento onde há acesso tanto interno quanto externo, a DMZ é considerada uma rede semi-confiável.



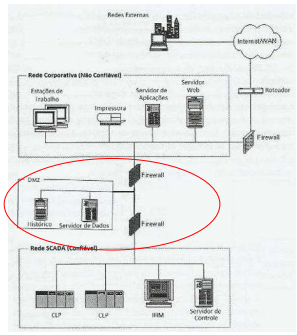
São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

d) Par de firewalls com DMZ entre as redes

- O uso de 2 firewalls para a criação da DMZ permite que cada rede controle sua segurança.
- Melhor configuração para evitar conflitos políticos entre TI e TA sobre quem é o administrador do firewall.
- Cada gestor de rede cria e administra suas próprias regras.
- Ter firewalls de diferentes fabricantes aumenta a segurança.



São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

Firewall de perímetro de próxima geração

- A Plataforma de segurança de próxima geração da Palo Alto Networks pode ser usada para proteger redes de infraestruturas críticas e sistemas SCADA em segmentos de mercado tais como energia, águas e resíduos, transportes e manufatura.
- Sua plataforma de próxima geração oferece funcionalidades tais como:
  - ⇨ Inspeção profunda do tráfego da rede que provê informação intuitiva e inteligência para a tomada de decisão
  - ⇨ Controle granular sobre as aplicações, os usuários, o conteúdo e o tráfego WAN ou web.
  - ⇨ Proteção nativa tanto contra ameaças conhecidas como para ameaças desconhecidas
  - ⇨ Gerenciamento centralizado que facilita a forense digital e recuperação em caso de incidentes

paloalto networks.

São Paulo Section

www.tisafe.com

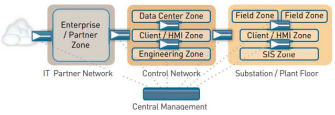
TI Safe Segurança da Informação

Funcionalidades da plataforma

- No coração da plataforma Palo Alto existem funcionalidades únicas tais como *App-Id*, *User-Id* e *Content-Id*.

- Estas funcionalidades permitem ao sistema Palo Alto classificar o tráfego de acordo com a aplicação, o usuário e o tipo de conteúdo:
  - ⇨ **App-Id**: Identifica todas as aplicações em todas as portas o tempo todo (ao contrário do comum em firewalls porta/protocolo)
  - ⇨ **User-Id**: Identifica usuários ou grupos de usuários (ao contrário do comum endereço IP)
  - ⇨ **Content-Id**: Escaneia o conteúdo do tráfego buscando dados estruturados, arquivos, ameaças, URL´s

Assinaturas de aplicativos para SCADA



- A solução Palo Alto permite a configuração da arquitetura estendendo a proteção desde pontos remotos (estações remotas, plantas remotas, UTRs, etc.), passando pela rede de campo (com ou sem fio), centro de controle e integrando-se com a rede de T.I. em uma configuração distribuída com gerenciamento central.

- Os sistemas Palo Alto apresentam reconhecimento de assinaturas nos seguintes protocolos industriais:

▪ Modbus	▪ OPC
▪ DNP3	▪ OSIsoft PI
▪ Ethernet IP	▪ Cygnet
▪ IEC 60870-5-104	▪ FactoryLink
▪ Synchrophasor	▪ ICCP

- Além destas assinaturas, a plataforma apresenta capacidade de controle de funções que permitem o monitoramento e o controle de sub-funções (tais como leitura e escrita) em protocolos industriais tais como o Modbus e o IEC 60870-5-104.

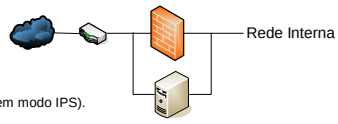
Principais benefícios das VLANs

- Segmentação da rede, aumentando a segurança e implementando o conceito de defesa em camadas.
- Segurança:
  - ⇨ Quando os usuários são agrupados em uma VLAN nenhum usuário fora desta VLAN consegue comunicar-se com os membros desta VLAN.
  - ⇨ A comunicação entre membros de diferentes VLAN é possível através de um roteador, e neste podemos implementar regras (filtragem de pacotes) que permitirão/bloquearão a comunicação.
- Facilidade de movimentação em redes IP.
- Gerenciamento: O software do Switch permite o assinalamento de um usuário para uma VLAN e mais tarde, mover o mesmo usuário para uma outra VLAN. Quando o usuário é movido de lugar, em um ambiente de Switch não será necessário um recabeamento para garantir a conectividade no grupo. O software de gerenciamento permite a reconfiguração da LAN em segundos.

Sistemas de Detecção e Prevenção de Intrusos (IDPS)

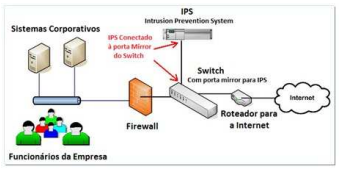
Intrusion Detection and Prevention System

- Equipamentos dedicados ou componentes baseados em *software* que monitoram o tráfego da rede com o objetivo de identificar ações maliciosas, mal uso da conexão, tentativas de ganho de acesso desautorizados e ataques.
- Tipos de IDPS
  - ⇨ Baseados em equipamentos e rede.
  - ⇨ Baseados em assinaturas.
- Composição básica
  - ⇨ Sensores.
  - ⇨ Sistemas de decisão.
  - ⇨ Sistema de armazenamento.
  - ⇨ Módulo de reação (somente em modo IPS).

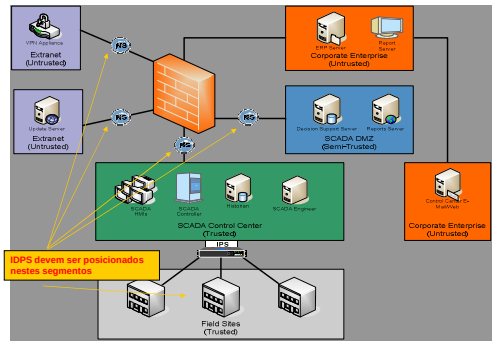


Como funciona um IDPS

- Os sensores detectam os eventos para análise.
- O sistema de decisão determina se houve comportamento intrusivo.
- Caso o equipamento esteja em modo de prevenção, o comportamento intrusivo será bloqueado.
- Ocorre o armazenamento de log com o evento associado à decisão tomada para futura análise.



Onde os IDPS devem ser posicionados?



São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

Cenários de uso de IDPS em SCADA

Aplicação do IDPS	Funcionalidade
IDPS baseados em rede conectam à estação central de controle SCADA para monitorar a IHM e conexões a outras redes da empresa.	Monitoram logs de auditoria de sistemas operacionais para servidores centrais e outros sistemas principais.
IDPS baseados em rede monitoram a DMZ e lêem informações de ataque provenientes de logs de firewall e servidores.	Detectam ataques à DMZ e determinam o combate ao ataque.
IDPS baseados em rede monitoram o log de firewalls.	Detectam e combatem ataques ao firewall.
IDPS baseados em rede monitoram *port-scans* e ataques potenciais como os de DOS e DDOS, dentre outros.	Enviam comando de TCP-Reset para as conexões dos atacantes, combatendo os ataques.
Equiparar o nível de segurança dos servidores da rede aos de uma rede com *patches* atualizados.	Funcionalidade Virtual Patch, presente em alguns IDPS de mercado.

São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

IDPS para uso em redes SCADA

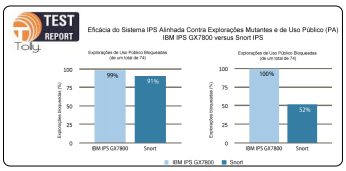
São Paulo Section

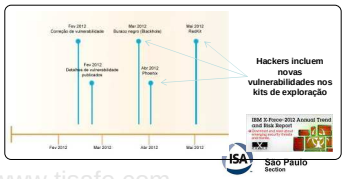
www.tisafe.com

TI Safe Segurança da Informação

IBM Security Network IPS

Protege ambientes bloqueando ameaças mutantes e ataques 0 Day.





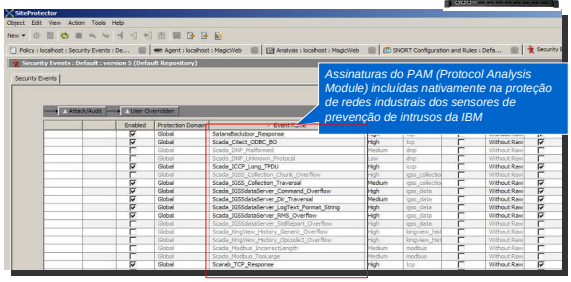
Principais funcionalidades

- Utiliza abordagem baseada em protocolo para capturar muitos ataques "dia-zero" e ameaças mutantes.
- Oferece proteção contra vulnerabilidades conhecidas quando uma correção está indisponível ou implementado usando uma "correção virtual".
- Patch virtual protege os sistemas SCADA uma vez que os sistemas e controladoras não podem receber correções.

ISA São Paulo Section

IBM Security Network IPS

Proteção de ataques específicos de redes SCADA



- Assinaturas nativas dos IDPS da IBM protegem os segmentos de redes industriais inspecionando tráfego e bloqueando o conteúdo malicioso.

ISA São Paulo Section

IBM Security Network IPS

Permite a fácil criação de assinaturas específicas para detecção de ataques a autômatos programáveis.

```
alert tcp !$ENIP_CLIENT 44818 -> $ENIP_SERVER any
(msg:"SCADA_IDS: ENIP/CIP – Reboot or Restart from
Unauthorized Client"; flags:PA; cip_service:5;
reference:scada,1111501.htm, classtype:attempted-dos;
sid:1111501; rev:1; priority:1;)
```

Exemplo de criação de assinatura personalizada SNORT para monitoração da condição de Reboot ou Restart de um PLC a partir de um cliente não autorizado.

ISA São Paulo Section

IBM Virtual Patch® Technology

- Protege vulnerabilidades contra ataques mesmo que a máquina não tenha o patch instalado.
- Permite um processo de gerenciamento de patches sem o medo de falhas.
- Muito útil para redes industriais onde a instalação de patches em servidores SCADA é quase sempre um problema.

Estratégias de defesa em profundidade

Porque as soluções de segurança falham?

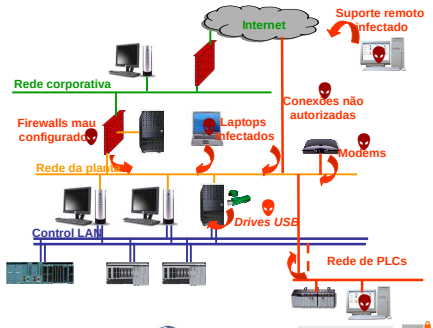
- Uma solução popular para a segurança industrial é instalar um firewall entre as redes de negócios e de controle.
- Conhecido como o ***Bastion Model*** , uma vez que ele depende de um ponto único de segurança.
- Exemplo: Muralha da China.

Proteger o perímetro não é suficiente

- Não se pode somente instalar um firewall para controle de sistemas e esquecer do resto da segurança.
- Os invasores normalmente entram.
- É necessário proteger o chão de fábrica com uma estratégia de defesa em profundidade.
- Um Worm infiltrou-se em*:
  - Uma planta nuclear através de uma conexão 3G.
  - Um sistema SCADA de energia através de uma VPN.
  - Um sistema de controle de Oil&Gas através do sistema do laptop de um terceirizado.
- Firewalls existiam em todos estes casos.

* Dados obtidos do RISI

Caminhos dentro da rede de controle



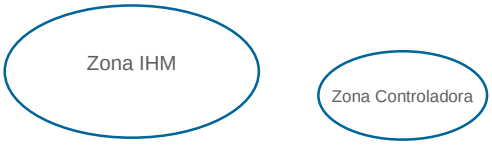
Modelo de Zonas e Conduítes

O que torna um sistema seguro?

- Na maioria dos incidentes reportados, havia uma falha em conter as comunicações em áreas apropriadas ou sub-sistemas.
- Problemas em uma área eram permitidos de migrar para outra área devido à uma estratégia de separação pobre ou inexistente.
- A Solução é o uso de zonas de segurança, como definido na ANSI/ISA-99.
- ELEMENTO 4.3.2.3 – Segmentação de rede:
  - ⇨ Objetivo:
    - Agrupar e separar sistemas de controle de infraestruturas críticas chave em zonas com níveis de segurança comuns de maneira a gerenciar os riscos de segurança e atingir um nível de segurança desejado para cada zona.
  - ⇨ Requerimento 4.3.2.3.1:
    - Uma estratégia de contramedida baseada na segmentação de rede deve ser desenvolvida para os elementos de uma rede crítica de acordo com o nível de riscos desta rede.

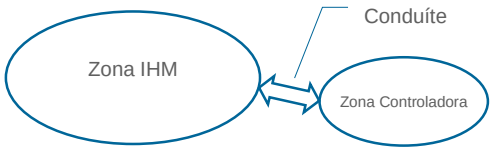
Definição de zona de segurança

- "Zona de segurança: agrupamento de ativos físicos e lógicos que dividem os mesmos requerimentos de segurança". [ANSI/ISA–99.00.01–2007- 3.2.116].
- Uma zona deve ter uma borda claramente definida (seja lógica ou física), que será a fronteira entre elementos incluídos e excluídos.



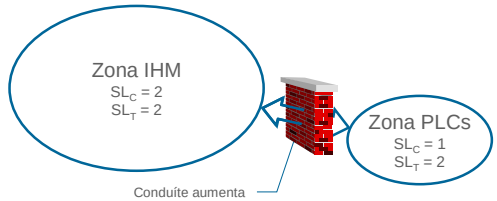
Conduítes

- Um conduíte é um caminho para o fluxo de dados entre duas zonas:
  - ⇨ Pode fornecer as funções de segurança que permitem diferentes zonas a se comunicar com segurança.
  - ⇨ Todas as comunicações entre zonas devem passar por um conduíte.



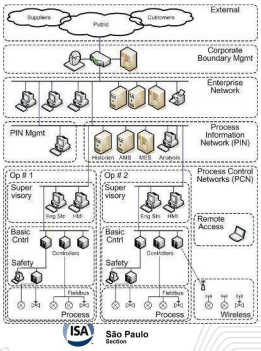
Níveis de Segurança

- Uma zona terá de um nível de segurança alvo (SL_T) baseado em fatores como sua criticidade e consequências.
- Equipamentos em uma zona terão uma capacidade para o nível de segurança (SL_C).
- Se eles não forem iguais, então será necessário adicionar tecnologias de segurança e políticas para torná-las iguais.



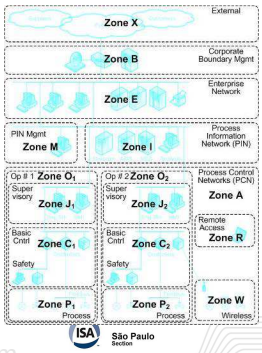
Usando zonas: o exemplo da refinaria

Topologia da rede de automação da refinaria.



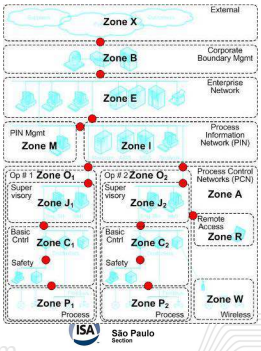
Especificando as zonas (1º Passo)

Rede de automação da refinaria dividida em zonas de segurança.



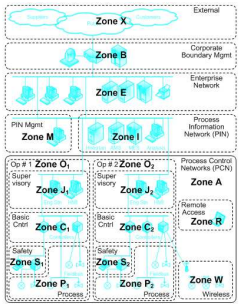
Adicionando os conduítes (2º Passo)

Conduítes são adicionados entre as zonas de segurança.



Protegendo as Zonas (3º Passo)

- A solução foi separar algumas zonas que estava em desequilíbrio entre o SLC e o SLT.
- E então colocar firewalls industriais entre estas zonas para atingir o nível de segurança desejado.



Proteção da Rede Interna

- Segmentação segundo o modelo de zonas e conduítes
- Domínio de segurança para redes de automação
- Framework para controle de malware
- Firewall industrial - Suite Tofino
- Firewall industrial - Siemens SCALANCE S
- Gateways de segurança unidirecionais

VLANs

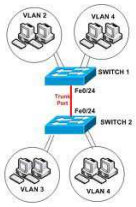
São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

Segmentação da rede de automação

- É necessário proteger não somente o perímetro como também a rede interna.
- A norma ANSI/ISA-99 define o modelo de zonas e conduítes onde a rede interna é dividida logicamente em zonas de segurança interligadas por segmentos de rede denominados conduítes.
- A norma também orienta que nos conduítes devem ser implantadas soluções de segurança para as zonas da rede interna.
- Para este propósito a TI Safe oferece os seguintes serviços:
  - ⇨ Inventário de ativos da rede de automação.
  - ⇨ Especificação da arquitetura da rede de acordo com o modelo de zonas e conduítes.
  - ⇨ Segmentação da rede interna através de configuração de VLANs (Redes Locais Virtuais).
  - ⇨ Especificação de modelos de firewalls industriais específicos para uso nos conduítes.



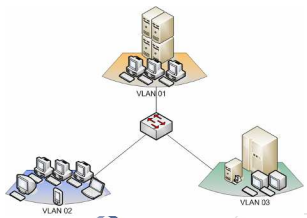
São Paulo Section

www.tisafe.com

TI Safe Segurança da Informação

Virtual Local Area Networks (VLANs)

- As VLANs são segmentações virtuais de uma rede real em setores específicos e isolados entre si.
- Implementam um método de "etiquetar" pacotes para identificar quem pode falar com quem.
- O Padrão usado para VLANs é o IEE802.1Q



São Paulo Section

www.tisafe.com

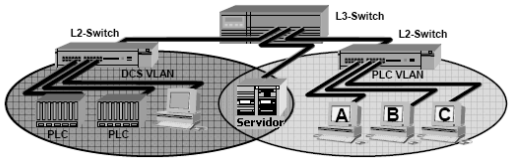
TI Safe Segurança da Informação

Definição de VLANs

- Grupo de computadores, servidores e outros recursos de redes que estão localizados em qualquer parte da rede, mas comunicam-se como se estivessem conectado a um mesmo segmento de rede.
- Com VLANs podemos segmentar uma rede sem restrições de conexões físicas.
- Formas sugeridas para implementação de VLANs:
  - Grupos Departamentais (Contabilidade, RH, Secretaria, Automação).
  - Grupos Hierárquicos (Gerência, Diretoria, Chefia, Supervisão).
  - Grupo de usuários (Supervisores, Operadores, etc).

Separação da rede interna usando VLANs

- Na figura abaixo, ambas as VLANs contém o servidor de informações de processos, permitindo que os dois grupos acessem o servidor, mas ainda formando uma separação segura entre as diferentes redes de processos.



VLANs podem ser usadas para criar zonas de segurança dentro da rede de automação, mas nunca para separar a rede corporativa da rede de automação.

Domínio para redes de automação

- Especificação de política de controle de acesso para a rede de automação.
- Implantação de domínio para área de automação baseado no Microsoft Active Directory (esquema de autenticação centralizada ou distribuída).
- Integração com login de plataformas UNIX like e login transparente.
- Estabelecimento de relação de confiança com domínio corporativo.
- Integração com fabricantes para ativação de GPOs específicas para segurança de redes industriais.
- Registros (Logs) de atividades de usuários na rede de automação.

Framework para Controle de Malware

TREND MICRO

ISA São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

Framework para controle de malware

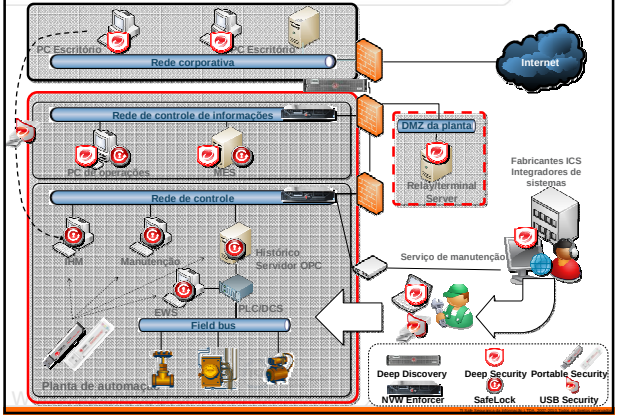
①② Gateway/ Rede	③ DMZ ④ Autenticação de rede	⑤ Controle de rede	⑥⑦ Mídia Externa/PC
	Não Missão Crítica Uso geral	Missão Crítica Uso específico	
Trend Micro Network VirusWall Enforcer	Trend Micro Deep Security "Proteção modular compreensiva, para servidores, PCs e laptops"	Trend Micro Safe Lock "Multi-layer LOCKDOWN"	Trend Micro USB Security "Armazenamento USB protegido"
Trend Micro Deep Discovery "Controle, análise e visibilidade da rede"			
N/A		Trend Micro Portable Security "Escaneamento de Malware / ferramenta de limpeza para PC isolados ou em rede	Trend Micro Deep Security

ISA São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

Pontos de contramedidas em ICSs



Deep Discovery
Trend Micro Deep Security
Trend Micro Network Virus Wall Enforcer

São Paulo Section

www.tisafe.com

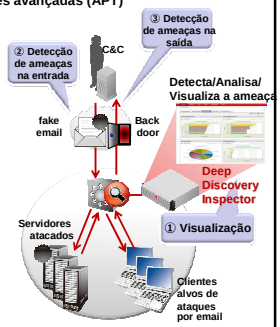
TI Safe
Segurança da Informação

Deep Discovery – Visão Geral

Monitora a rede e protege de ameaças persistentes avançadas (APT)

Características

1. **Total visibilidade de ameaças à rede**
   - ⇨ Cenário de situações via widget gráfico
   - ⇨ Fácil detecção das últimas ameaças sem análise baseada em relatórios que permite rápida tomada de decisão
2. **Detecção de ameaças de entrada**
   - ⇨ Provê regras de detecção baseadas a partir da base da Trend Micro e realiza análise dinâmica através de virtualização
   - ⇨ Proteção independente para vários protocolos de rede usados.
3. **Detecção de ameaças de saída**
   - ⇨ Detecta via monitoramento as trasmissões de dados não autorizadas
   - ⇨ Determina situações críticas basedas em servidores de commando e controle, endereços IP cadastrados na base de reputação, dentre outros.



São Paulo Section

www.tisafe.com

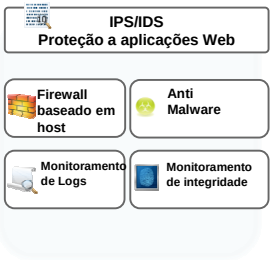
TI Safe
Segurança da Informação

Trend Micro Deep Security

Proteção modular para servidores, desktops e laptops

Características

1. Proteção contra vulnerabilidades do Sistema operacional e de aplicações
2. Proteção contra ataques de SQL Injection em aplicações Web
3. Monitoramento Centralizado de eventos de segurança do Sistema Operacional e middleware
4. Escaneamento em tempo real
5. Monitora mudanças nos arquivos e registros



São Paulo Section

www.tisafe.com

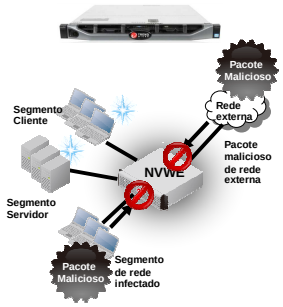
TI Safe
Segurança da Informação

Trend Micro Network Virus Wall Enforcer

Proteção para segmentos de rede

Características

1. **Protege o PC de controle e terminais**
   - ⇨Distribui no mesmo segmento de rede as demandas de proteção contra ataques de vulnerabilidades
2. **Proteção a Segmentos de Rede**
   - ⇨ Protege segmentos de rede em legados cliente/servidor distribuindo demandas de proteção.
3. **Quarantena de Rede**
   - ⇨ Protege contra infecções secundárias causadas por dispositivos não autorizados trazidos por terceiros e conectados em meio externo.



ISA São Paulo Section

TI Safe Segurança da Informação

Firewall Industrial – Suite Tofino

TOFINO SECURITY
A BELDEN BRAND

ISA São Paulo Section

TI Safe Segurança da Informação

Firewall Industrial - Suite Tofino

- Completa solução para segurança de plantas de automação indicada para empresas que desejam atingir o *compliance* com a norma ANSI/ISA-99 sem a necessidade de paradas de produção nem configurações complicadas.
- A solução é controlada e monitorada em tempo real por uma console de gerência que armazena trilhas de auditoria para os eventos de segurança.

Suite Tofino
Segurança de Redes Industriais

- A TI Safe é o único VAR da Belden autorizado para prestar consultoria e serviços no Brasil.
- Serviços prestados:
  - Certificação oficial da Suíte Tofino (12h)
  - Implantação e configuração da Solução
  - Monitoramento 24 X 7 X 365
  - Suporte de Segurança da solução implantada

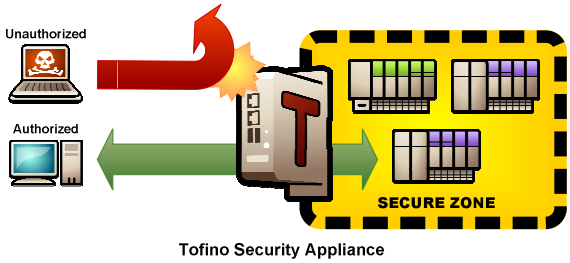
ISA São Paulo Section

TI Safe Segurança da Informação

Componentes da Suite Tofino

- *Appliance* de Segurança Tofino™:
  - ⇨ Nível de segurança para sua rede de controle.
- Módulos de segurança carregáveis (LSM):
  - ⇨ Módulos em *Firmware* que customizam os itens de segurança nos *appliances* de segurança Tofino.
- Plataforma de Gerência Centralizada (CMP):
  - ⇨ Gerência de segurança centralizada.

Suite Tofino: Segurança da rede interna



Tofino Security Appliance

Appliance de segurança Tofino™

- Equipamentos em hardware reforçado para uso em indústrias.
- Instalados em frente de redes de IHM, DCS, PLC e RTUs que necessitem de proteção.
- Simples instalação, não requer conhecimentos de rede nem nenhuma pré-configuração.
- Instalação e configuração sem parada da rede de controle.
- Modo de testes que não oferece riscos para a planta.

Módulos de segurança carregáveis (LSM)

- Os LSMs são plug-ins que fornecem serviços de segurança tais como:
  - ⇨ Firewall.
  - ⇨ Gerência segura de ativos.
  - ⇨ Inspeção de conteúdo.
  - ⇨ VPN Criptografada.
  - ⇨ Modbus Enforcer.
  - ⇨ OPC Enforcer.

- Cada LSM é baixado no appliance Tofino para permitir que ele ofereça funções de segurança customizáveis, dependendo dos requerimentos do sistema de controle.

LSM para Firewall

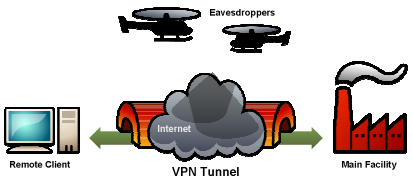
- Engenheiro de controle define lista de regras de tráfego.
- Automaticamente bloqueia e reporta qualquer tráfego que não obedeça a suas regras.
- Definição simples de regras usando um editor gráfico baseado em *drag-and-drop*.

LSM para gerência segura de ativos

- Processo de *discovery* passivo localiza os dispositivos de rede sem qualquer parada no processo.
- Geração de regras baseada em *wizards* ajuda os usuários a criar regras de firewall a partir de relatórios de tráfegos bloqueados.
- Dispositivos novos na rede são reportados para a plataforma de gerência centralizada (CMP) como um alerta de segurança.
- Armazena inventário detalhado para compatibilidade com os padrões ANSI/ISA-99 e NERC CIP.

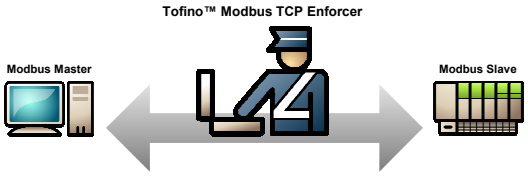
Túneis seguros sobre redes não confiáveis

- Cria túneis seguros entre *Appliances* Tofino; entre Tofinos e PCs; e entre Tofino e dispositivos de terceiros suportados.
- Fácil instalação e gerência.
- Interoperabilidade com outros LSMs (eg Firewall, Modbus TCP Enforcer) para combinar itens de segurança.



LSM para análise de Modbus TCP

- Engenheiro de controle define lista de comandos Modbus permitidos, registros e bobinas.
- Bloqueia automaticamente e reporta qualquer tráfego que não se encaixe nas regras.
- Protocolo '*Sanity Check*' bloqueia qualquer tráfego que não esteja em conformidade com o padrão Modbus.



LSM para segurança de conexões OPC

- Assegura OPC DA, HDA e A&E.
- Monitora conexões de dados criadas pelos servidores OPC para clientes autorizados, e abre dinâmicamente o mínimo requerido de portas no Firewall.
- O protocolo '*Sanity Check*' bloqueia quaisquer pedidos OPC que não estejam em conformidade com o padrão DCE/RPC.

Plataforma de Gerência Centralizada (CMP)

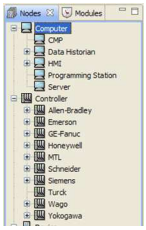
- Configura, gerencia e monitora todos os *appliances* de segurança Tofino a partir de uma estação de trabalho.
- Editor gráfico para rapidamente modelar sua rede de controle.
- Editores drag-and-drop visuais para rápida e fácil configuração de regras de segurança.

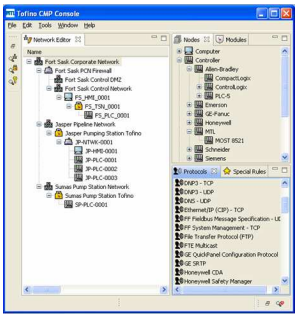
São Paulo Section

TI Safe Segurança da Informação

Monitoramento centralizado

- Tofino CMP (Plataforma Central de Gerência).
- Configura, gerencia e monitora a segurança das redes de automação.





São Paulo Section

TI Safe Segurança da Informação

Firewall Industrial - Siemens SCALANCE S

SIEMENS

São Paulo Section

TI Safe Segurança da Informação

Firewall industrial - Siemens SCALANCE S

Scalance S602
- Autenticação
- Encriptação de dados
- Controle de acesso
- NAT/NAPT
- DHCP Server
- Syslog

Scalance S612
- Scalance 602+
- NAT/NAPT
- DHCP Server
- Syslog
- Proteção de 32 Elementos em rede
- Até 64 VPN's

Scalance S623
- DMZ
- Portas Gigabit ethernet
- NAT/NAPT
- DHCP Server
- Dyn DNS
- Syslog
- Proteção de 64 elementos em rede
- Até 128 VPN's
- Temperaturas de -20 a +70.°

SOFTNET Security Client
- Acesso via internet /intranet de celulas de automação protegidos pelo Scalance S
- Autenticação
- Encriptação de dados
- Performance da Segurança em rede
- Configuração dos equipamentos

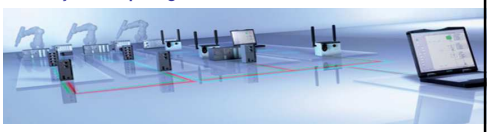
SIEMENS

São Paulo Section

TI Safe Segurança da Informação

Células de proteção com o SCALANCE S

- **"Células de automação" são protegidas**



- ⇨ Uma "célula" é um segmento de rede com um sistema de segurança separado
- ⇨ Controle de acesso na "entrada da célula" através de funcionalidades de componentes de segurança
- ⇨ Mesmo equipamentos sem funcionalidades de segurança estarão protegidos dentro da célula
- ⇨ Comunicações em tempo-real não são afetadas dentro da célula
- ⇨ Canais seguros para comunicação entre as células

A "Célula de Segurança" da Siemens é equivalente à Zona de Segurança da norma ANSI/ISA-99 (Modelo de Zonas e Conduítes)

São Paulo Section

TI Safe Segurança da Informação

Segurança abrangente com SCALANCE S

SCALANCE S602
Para a proteção de redes de automação por firewall

SCALANCE S612

SCALANCE S613
SCALANCE S612 and S613 para a proteção de redes de automação (S613 para mais nós)

Sofware Cliente de segurança para VPN SOFTNET
Para o estabelecimento de conexões seguras entre PCs, notebooks ou dispositivos protegidos por SCALANCE S

Para a segurança da rede e de dados.

São Paulo Section

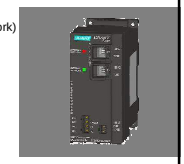
TI Safe Segurança da Informação

Módulos de segurança

- **SCALANCE S602**
  - ⇨ Protege a rede interna através Firewall de pacotes com inspeção de estado (*Stateful*)
  - ⇨ Filtra o tráfego de dados tanto baseado em endereços IP ou MAC
  - ⇨ Além de operar no modo bridge, também pode ser operado no modo roteador e, portanto, ser usado diretamente nas fronteiras das sub-redes IP
  - ⇨ NAT e NAPT (Network Address Translation e Port) permitem o uso de endereços IP privados na rede interna, e os endereços IP públicos podem ser salvos
  - ⇨ Nós da rede interna podem obter seus endereços IP do servidor DHCP integrante
  - ⇨ Diagnósticos remotos possíveis ao longo de um canal seguro com a ferramenta de configuração do SCALANCE S; arquivos de log podem ser avaliados com o servidor Syslog
    Configuração simples e rápida do firewall usando regras de firewall globais e nomes simbólicos para endereços IP
  - ⇨ Ferramenta simples para configuração central do SCALANCE S e do cliente SOFTNET
  - ⇨ C-PLUG: meio de armazenamento para rápida substituição, sem dispositivo de programação

Módulos de segurança

- **SCALANCE S612**
- **Em adição às funcionalidades do S602:**
  - ⇨ Protege a rede interna através do túnel VPN (Virtual Private Network) por meio de IPSec e / ou Firewall de inspeção de pacotes por estado
  - ⇨ Protege a transmissão de dados a partir do monitoramento e manipulação, com a verificação do fluxo de dados de e para a rede interna
  - ⇨ 64 túneis de VPN para segurança de outros módulos atuando simultâneamente
  - ⇨ Proteção do tráfego de dados na camada 2 do modelo IP
  - ⇨ Ferramenta simples para configuração central do SCALANCE S e do cliente SOFTNET
  - ⇨ C-PLUG: meio de armazenamento para rápida substituição, sem dispositivo de programação



Módulos de segurança

- **SCALANCE S613**
- **Em adição às funcionalidades do S612:**
  - ⇨ Duas vezes a quantidade em relação ao framework do S612: até 64 nós ou dispositivos na rede interna e 128 túneis VPN para outros módulos de segurança de forma simultânea
  - ⇨ Faixa de temperatura ampliada: temperatura de funcionamento de -20 ° C a +70 ° C (<95% de umidade relativa a 30 ° C)

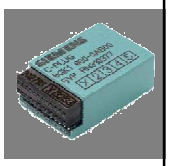
Software

- **Cliente de Segurança SOFTNET**

- Cliente de VPN para PCs e notebooks em um ambiente industrial
- Permite acesso VPN IPSec a sistemas de automação protegidos pelo SCALANCE S
- Proteção na transmissão de dados contra erros operacionais, monitoramento e manipulação
- Conceito de segurança uniforme para plantas de automação usando o SCALANCE S e o cliente SOFTNET
- Ferramenta simples de configuração centralizada para o SCALANCE S e o cliente SOFTNET

Plug de Configuração

- **C-PLUG**



- Meio intercambiável para salvar os dados de configuração do SCALANCE S
- Utilizado para a rápida substituição do módulo, sem ter que reprogramar o dispositivo

Gateways de Segurança Unidirecionais

WATERFALL
One Way to Connect

Gateways de segurança unidirecionais

- Laser em TX, fotocélula em RX, cabo de fibra ótica – você pode enviar dados para fora, mas nada consegue retornar no sentido contrário para a rede protegida.
- TX usa protocolos em duas vias para reunir dados de redes protegidas.
- RX usa protocolos em duas vias para publicar dados em redes externas.
- Derrota ataques de controle avançado / remoto.
- Casos típicos de uso:
  - ⇨ Replicação de bases de dados / históricos;
  - ⇨ Replicação de servidores OPC;
  - ⇨ Acesso remoto e comunicação segura entre plantas de automação;

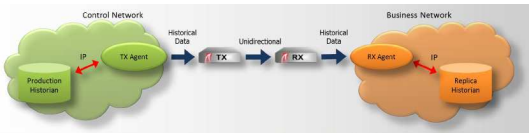
WATERFALL
One Way to Connect

ISA São Paulo Section

TI Safe Segurança da Informação

Caso de Uso: Replicação de Historian

- Agente TX é cliente convencional do historian – Ele requer uma cópia dos novos dados assim que chegam no historian.
- Agente RX é um coletor convencional do historian – Ele coloca novos dados na réplica que chegam do TX.
- Agente TX envia dados históricos e metadados para o RX, usando protocolo ponto-a-ponto não roteável.
- Réplica completa, acompanha todas as mudanças, novas tags, alertas em réplica.

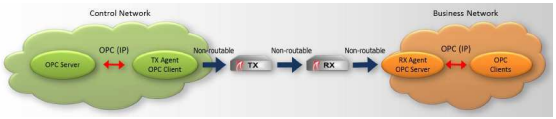


ISA São Paulo Section

TI Safe Segurança da Informação

Caso de Uso: Replicação do OPC

- Protocolo OPC-DA é complexo: com base no modelo de objeto DCOM - intensamente bi-direcional.
- O agente TX é um cliente OPC: ele reúne dados de servidores de produção OPC.
- O agente RX é um servidor OPC: ele dispõe dados para clientes OPC na rede de negócios.
- O agente TX envia apenas os dados e metadados OPC para o RX.
- O protocolo OPC é usado apenas na rede de produção e rede de negócios, mas não através de ligação unidirecional.

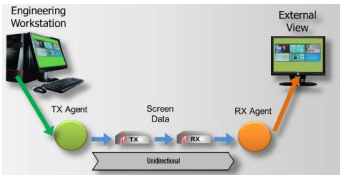


ISA São Paulo Section

TI Safe Segurança da Informação

Caso de Uso: Tela de visualização remota

- Os fornecedores podem ver telas do sistema de controle no navegador web.
- Quaisquer alterações de software ou dispositivos são realizadas por pessoal no local, supervisionado por fornecedores que podem ver as telas do local em tempo real.
- Fornecedores acham que estão supervisionando o local pessoalmente.
- Pessoas no local acham que estão sendo supervisionandas pelos fornecedores.
- Ambas as perspectivas são legítimas, ambos os conjuntos de necessidades são cumpridos.



São Paulo Section

TI Safe Segurança da Informação

Treinamento e Conscientização

TI Safe Segurança da Informação

São Paulo Section

TI Safe Segurança da Informação

Escopo da Formação

Academia TI Safe

- **Formação em Segurança de Automação Industrial**
- Baseada na norma ANSI/ISA-99
- Escopo:
  - ⇨ Introdução às redes industriais e SCADA
  - ⇨ Infraestruturas Críticas e Ciberterrorismo
  - ⇨ Governança para redes industriais
  - ⇨ Introdução à Análise de Riscos
  - ⇨ Análise de riscos em SCADA
  - ⇨ Malware e Ciberarmas
  - ⇨ Segurança de perímetro em redes de automação
  - ⇨ Criptografia em redes industriais
  - ⇨ Controle de Acesso em sistemas SCADA
  - ⇨ Defesa em profundidade e Monitoramento contínuo

São Paulo Section

TI Safe Segurança da Informação

Formação Presencial

Academia TI Safe

Próximas turmas em 2014:
- Rio de Janeiro: de 25 a 27/11
- São Paulo: de 2 a 4/12
- Salvador: de 9 a 11/11

- Aulas ministradas nas instalações da TI Safe ou na empresa (mínimo de 10 alunos)
- Alunos recebem livro texto e material didático complementar em formato digital
- Formação com 20h de duração
- Objetiva formar profissionais de T.I. e T.A.:
  - ⇨ Apresenta, de forma teórica e prática, aplicações reais da segurança de acordo com o CSMS (*Cyber Security Management System*) preconizado pela norma ANSI/ISA-99
  - ⇨ Totalmente em português, adequada ao perfil do profissional de segurança requerido pelas empresas brasileiras

ISA São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

Instrutores com Renome Internacional

RSA Conference, San Francisco - EUA

DEFCON, Bangalore - India

ACS Conference, Washington - EUA

CEBIT, Hannover - Alemanha

ISA São Paulo Section

TI Safe Segurança da Informação

www.tisafe.com

Formação via Ensino a Distância (EAD)

Academia TI Safe

Matricule-se em www.tisafe.com/ead_fsai

ISA São Paulo Section

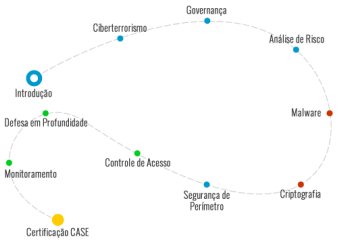
TI Safe Segurança da Informação

www.tisafe.com

Trilha de Aprendizado Online

Academia TI Safe

- Aulas ministradas online via internet
- Alunos recebem livro texto e material didático complementar em formato digital
- Conteúdo em 20 módulos com 10 horas de vídeos gravados
- Ao final de cada módulo o aluno é avaliado com uma rápida prova de revisão de conhecimentos

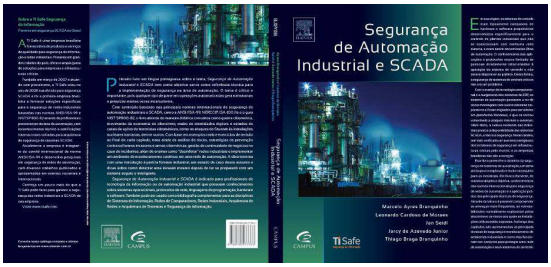


São Paulo Section

TI Safe Segurança da Informação

Livro Texto, 2014

Academia TI Safe



Único livro sobre segurança SCADA escrito em português no mundo

São Paulo Section

TI Safe Segurança da Informação

Certificação CASE

Academia TI Safe

- Prova **presencial** com 60 perguntas de múltipla escolha em português.
- Tempo de prova: 90 minutos.
- As questões com pesos diferentes. Aluno será aprovado se acertar 70% do valor total dos pontos.
- Se aprovado o aluno receberá o certificado por e-mail e seu nome será incluído em listagem no site da TI Safe.
- Os certificados tem 2 anos (24 meses) de validade a partir da emissão.
- Guia de estudos, simulado e calendário disponíveis no website.

Matricule-se em www.tisafe.com/ead_case

São Paulo Section

TI Safe Segurança da Informação

CLASS 2014 – Novembro no RJ

ISA São Paulo Section

TI Safe Segurança da Informação

CLASS 2014 em números

- 230 participantes
- 28 palestrantes, sendo 14 internacionais
- 28 palestras, 5 cursos (4hs)
- 3 dias de evento
- Demonstração de soluções em stands
- Projeto ICSSF – ICS Security Framework

Visite www.class2014.com.br

ISA São Paulo Section

TI Safe Segurança da Informação

Siga a TI Safe nas redes sociais

- Twitter: @tisafe
- Youtube: www.youtube.com/tisafevideos
- SlideShare: www.slideshare.net/tisafe
- Facebook: www.facebook.com/tisafe
- Flickr: http://www.flickr.com/photos/tisafe

ISA São Paulo Section

TI Safe Segurança da Informação


Contatos
Contato
| Contato
Rio de Janeiro
Centro Empresarial Città America – Barra da Tijuca
Av. das Américas, 700, bloco 01, sala 331
CEP – 22640-100 – Rio de Janeiro, RJ – Brasil
Telefone: +55 (21) 2173-1159
Fax: (21) 2173-1165
São Paulo
Rua Dr. Guilherme Bannitz, nº 126 – 2º andar
Cj 21, CV 9035 – Itaim Bibi
CEP – 04532-060 – São Paulo, SP – Brasil
Telefone: +55 (11) 3040-8656
Fax: (11) 3040-8656
Salvador
Av. Tancredo Neves nº 450 – 16º andar – Edifício Suarez Trade
CEP – 41820-901 – Salvador, BA – Brasil
Telefone: +55 (71) 3340-0633
Fax: (71) 3040-0699
Na web
Twitter: @tisafe
Skype: ti-safe
ISA São Paulo Section
TI Safe
Segurança da Informação
www.tisafe.com