Aspectos de Segurança da Informação - Frameworks

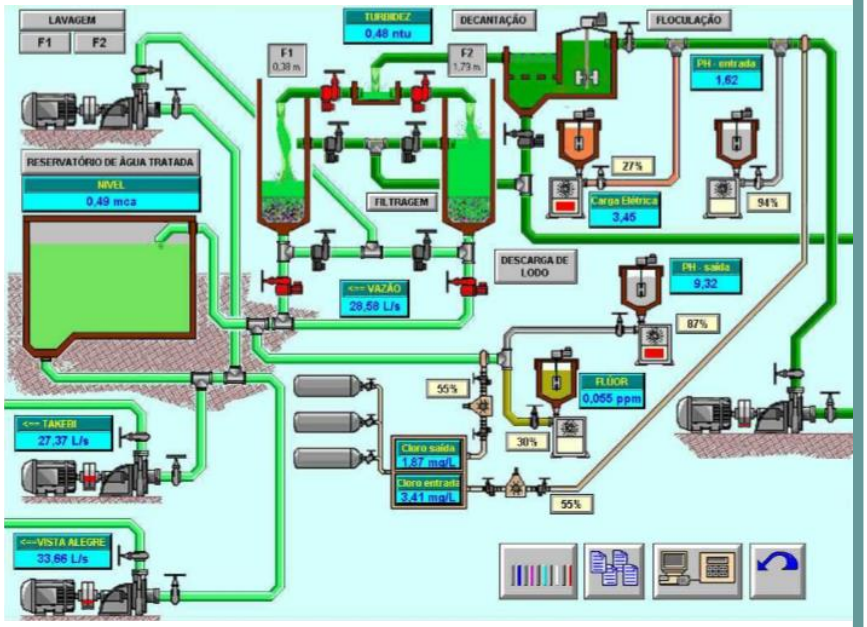
OUTRAS AULAS EM:

www.projetoderedes.com.br

Prof. José Maurício S. Pinheiro – UBM 2016

Redes Industriais

- Redes industriais utilizam os mesmos equipamentos e tecnologias de comunicação das redes tradicionais de dados
- Entretanto, como seu foco de atuação é voltado para informações de controle do processo produtivo , existem certas peculiaridades que as diferem das outras redes, como por exemplo, equipamentos específicos e restrições operacionais.
- Em Indústrias, as soluções baseadas na arquitetura SCADA são as mais usadas

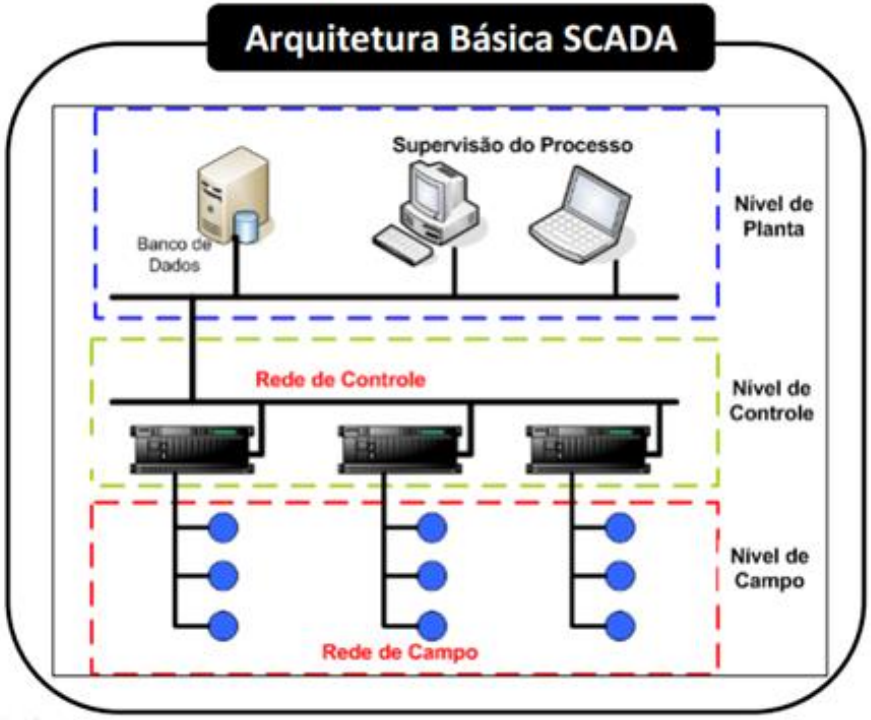


Sistemas Supervisórios

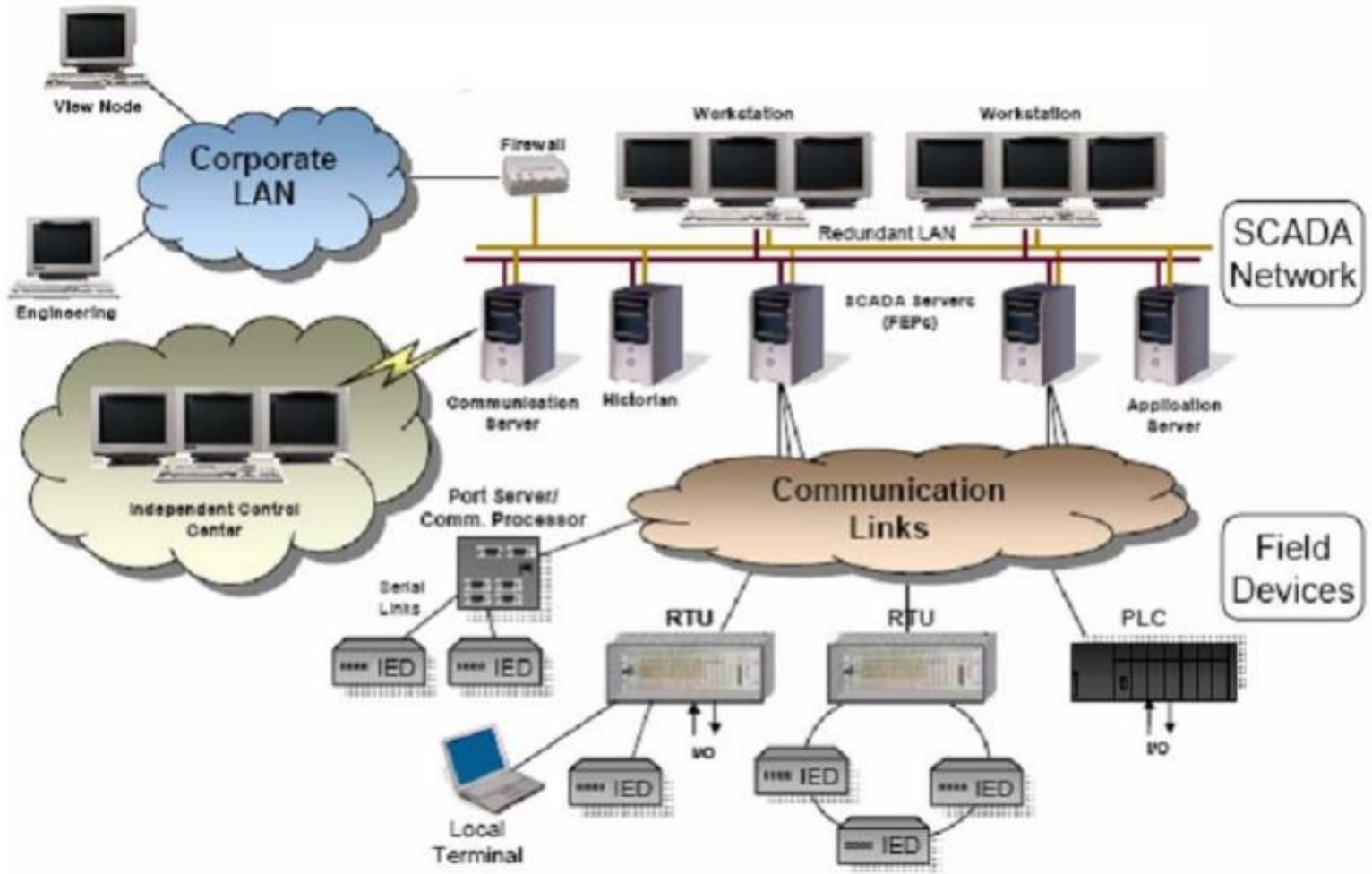
- No início os sistemas supervisórios eram desenvolvidos em plataformas operacionais caríssimas, baseadas em sistemas Unix like e máquinas poderosas como os Digital Vax e Alpha.
- Desenvolver aplicativos para estas plataformas era algo extremamente caro
- Com isto, supervisórios passaram a ser desenvolvidos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

Sistemas Supervisórios

- **Sistemas SCADA – No início**
  - Sistemas proprietários ➔ Dependente de Fabricantes
  - Sistemas isolados
  - Arquiteturas fechadas
  - "Ilhas de automação"



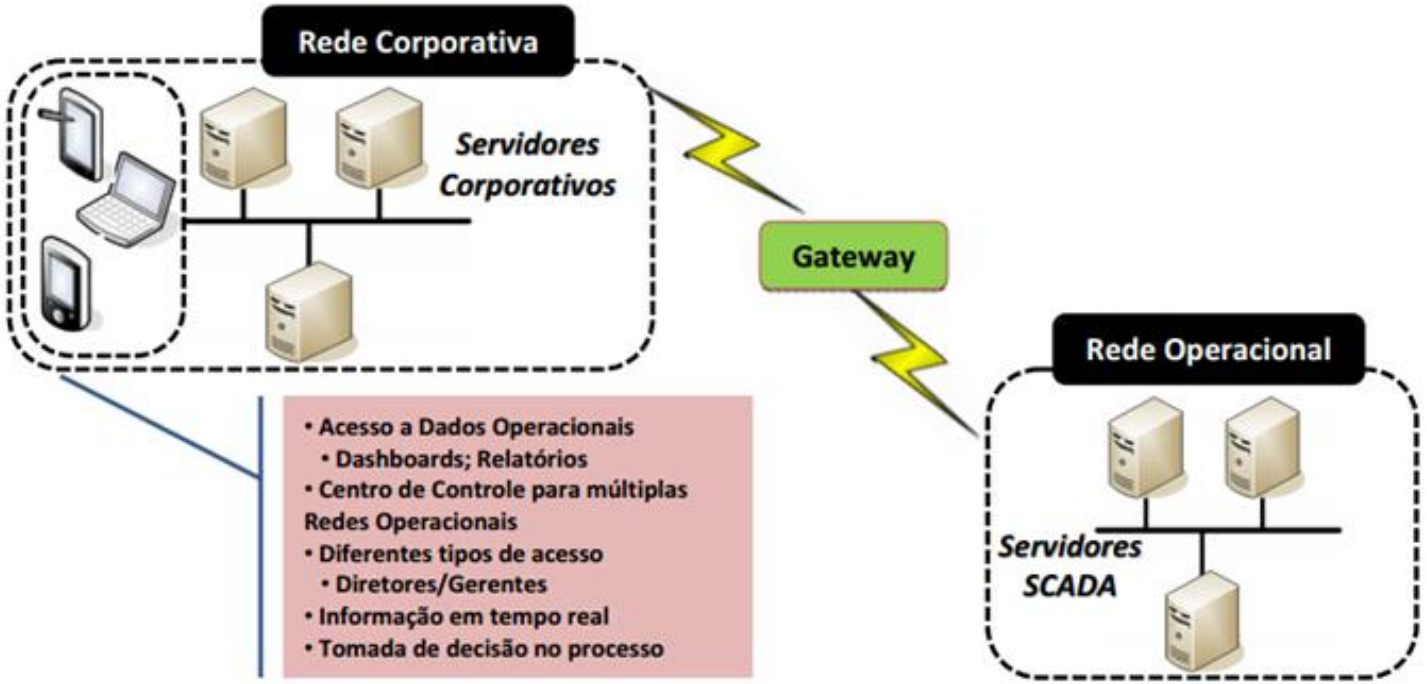
Arquitetura SCADA



Arquitetura SCADA

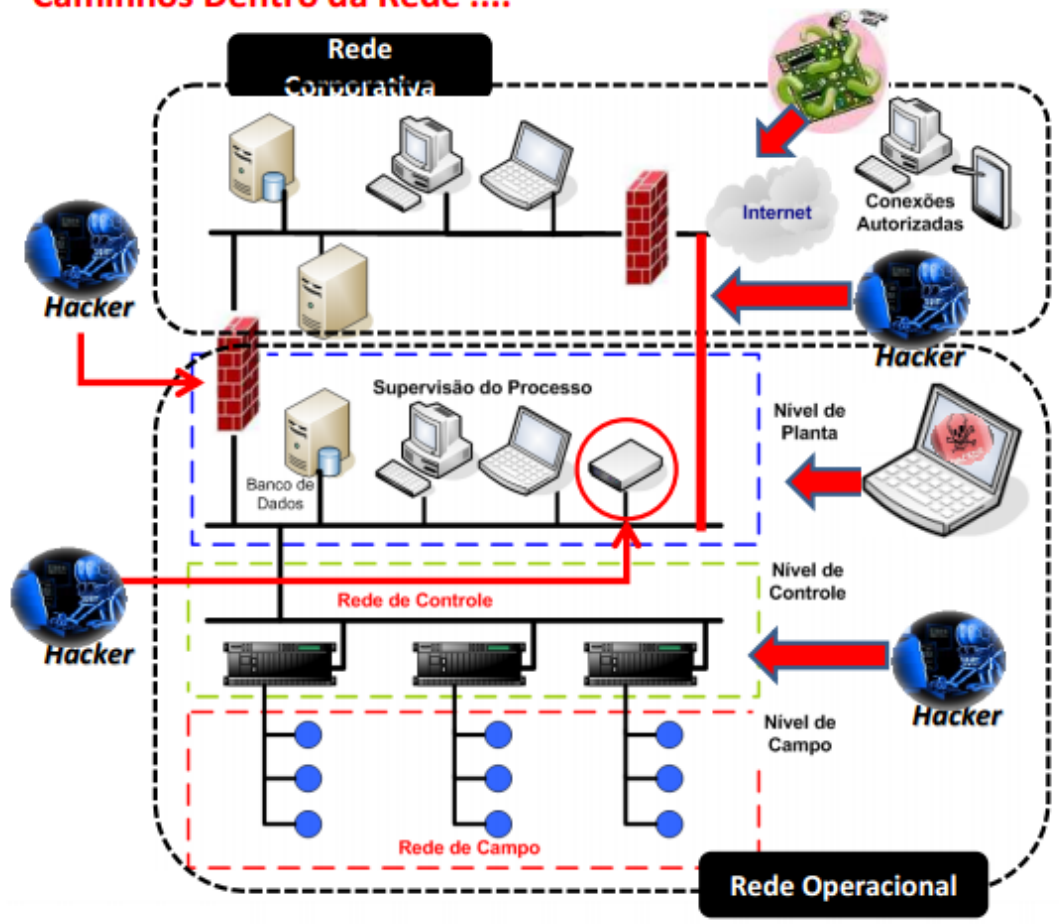
- Sistemas abertos
- Arquitetura centrada em Conectividade

- Integrações cada vez mais freqüentes:
  - Sistemas SCADA e Intranet corporativa
  - Sistemas SCADA e Internet



Vulnerabilidades

- **Caminhos Dentro da Rede ....**



Vulnerabilidades

- Conexões não autorizadas
- Sistemas e Serviços Vulneráveis
- Suporte Remoto Infectado
- Notebooks Infectados
- Firewall mau configurados
- Modems sem proteção
- Rede de PLC´s
- Links RS-232

Vulnerabilidades

Arquitetura de rede insegura

- Configuração de servidores de FTP, web e email 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 permanentemente habilitados, sem mecanismos fortes de controle de acesso
- Firewalls e outros dispositivos de segurança de rede não implementados internamente, deixando pouca ou nenhuma separaração entre as redes corporativa e de automação
- Redes sem fio configuradas sem segurança adequada
- PLCs não requerem autenticação para serem usados
- Softwares de IHM possuem vulnerabilidades publicadas na Internet

Vulnerabilidades

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"

Incidentes de Segurança

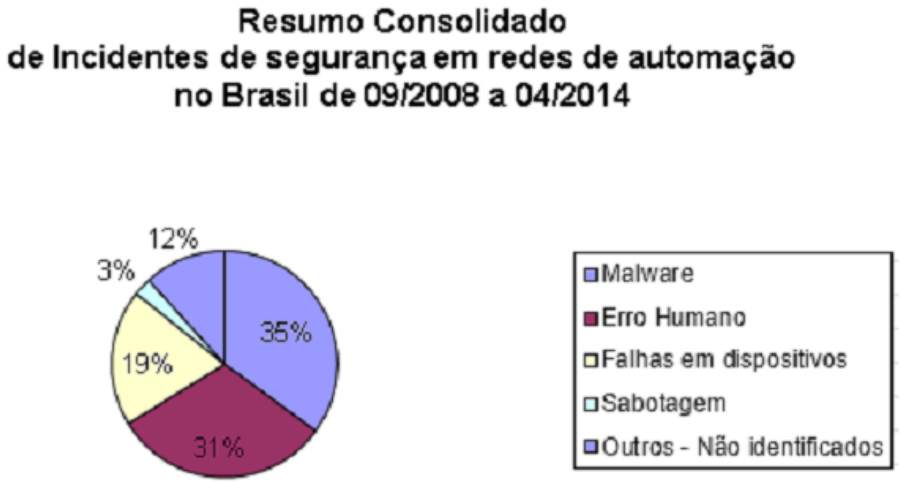
RISI - Repository for Industrial Security Incidents

- 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.

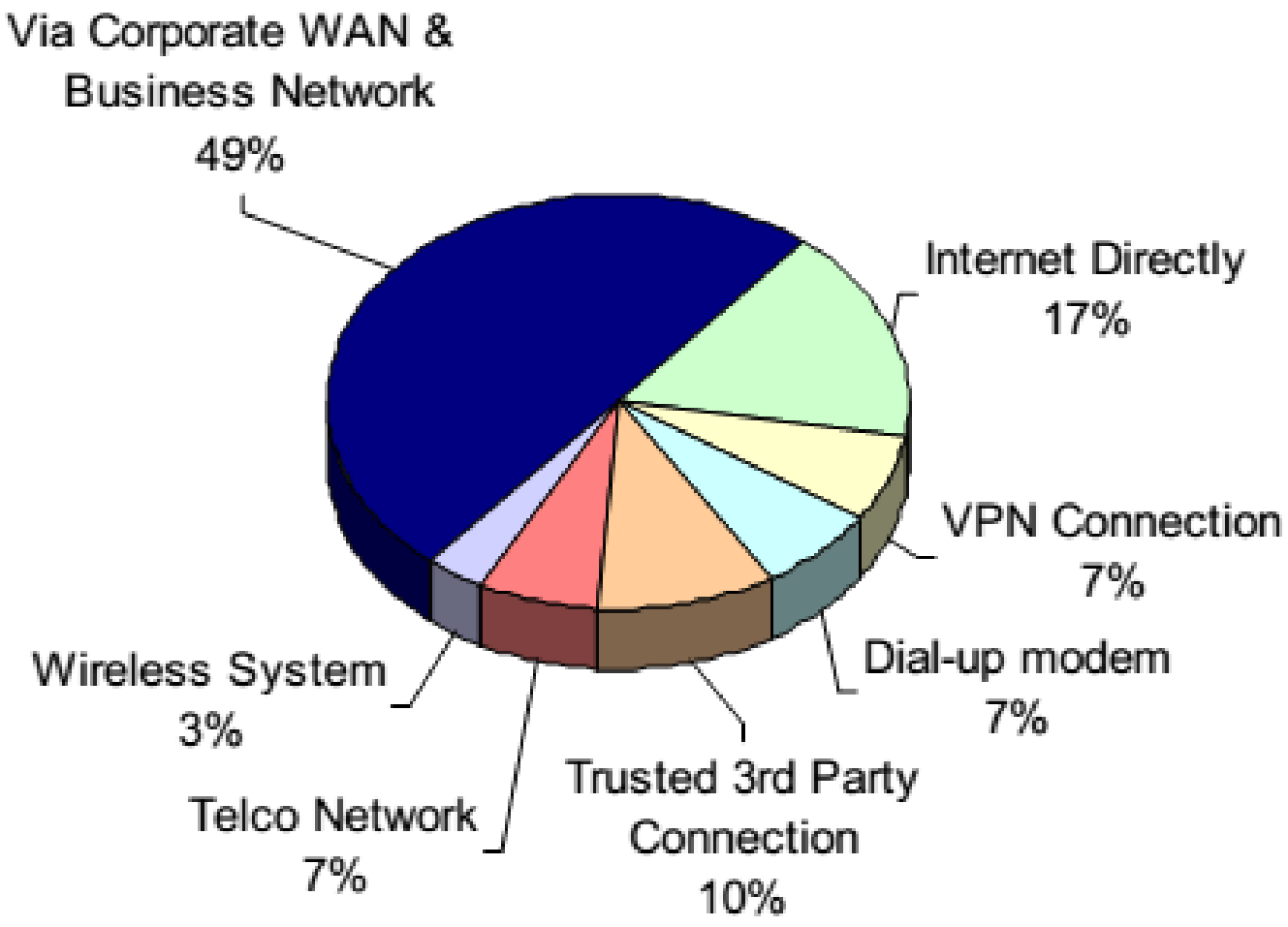
Incidentes de Segurança

O Brasil não possui uma fonte oficial de informações sobre incidentes de segurança em redes industriais e SCADA, o que gera uma lacuna importante no ciclo de proteção destas infraestruturas críticas.

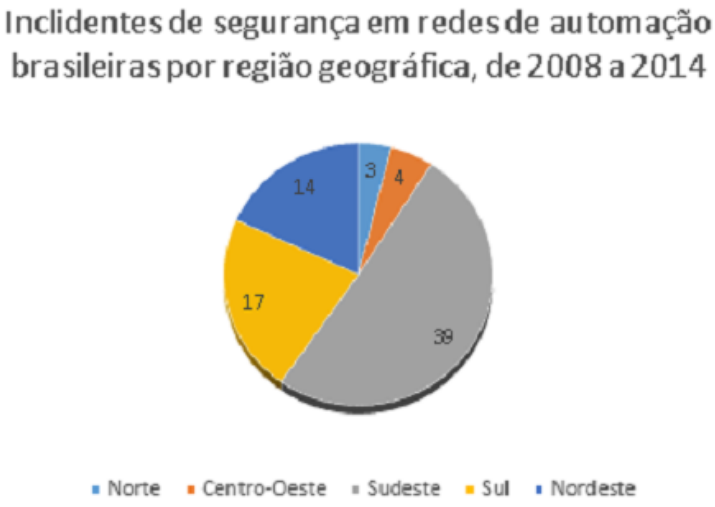
Incidentes	# Casos
Malware	27
Erro Humano	24
Falhas em dispositivos	15
Sabotagem	2
Outros - Não identificados	9



Incidentes de Segurança



Incidentes de Segurança



Origem dos Ataques - Malware

- O DOWNAD, mais conhecido como "Conficker", dominou a contagem de malware em plantas industriais no Brasil.
- Dos 27 casos documentados 14 foram 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, antivírus e medidas para controle de acesso à rede de automação e proteção de portas USB.

Caso: Ataque em Siderúrgica

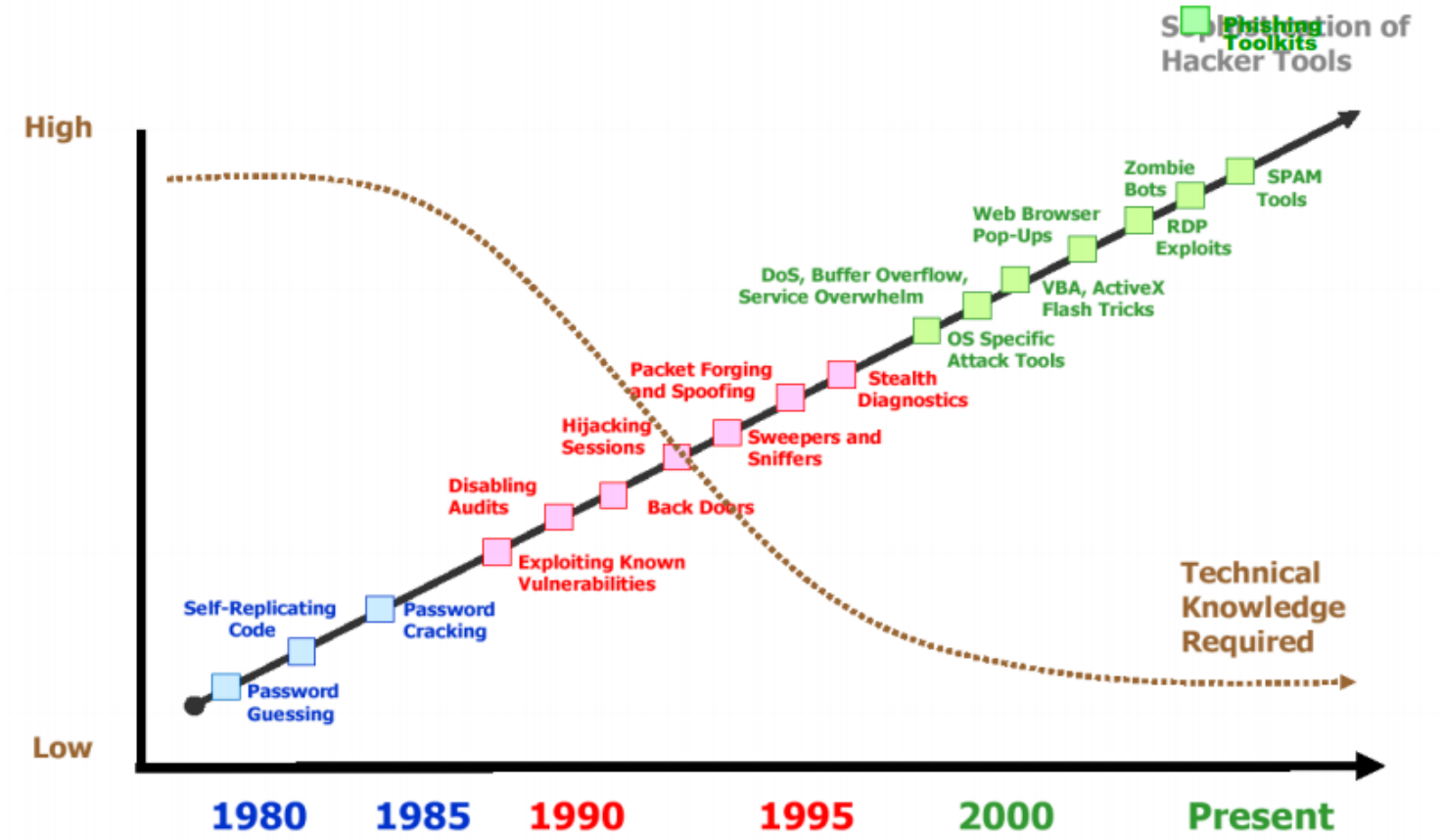
- **Malware e sua variante**: Conficker Win32
- **Número de máquinas infectadas:** toda a rede, mais de 30 computadores entre eles servidores, estações de engenharia, estações de operação e gateway. “Não estou mencionando os problemas do complexo siderúrgico. Apenas relatei a Termelétrica. Houveram outras 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.

Outros Ataques

- **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?**

Outros Ataques

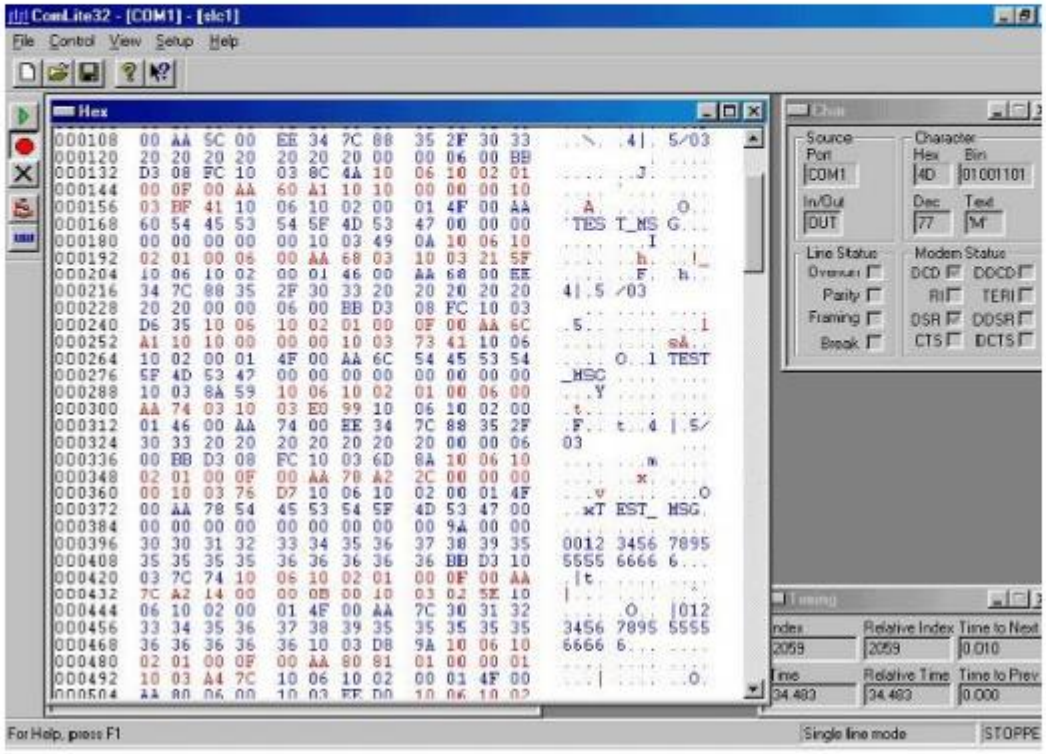
"Script Kiddies", usando toolkits hackers precisam de muito pouco conhecimento técnico para lançar um ataque!



Outros Ataques

Cracking de Senhas em PLC's

- É possível monitorar a comunicação entre o Supervisório e o PLC através da porta COM e obter as senhas (Principal e Master) do PLC
- É igualmente possível injetar/alterar códigos de PLCs para que eles realizem tarefas de maneira incorreta e até mesmo maliciosa



Exemplos de Ataques

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

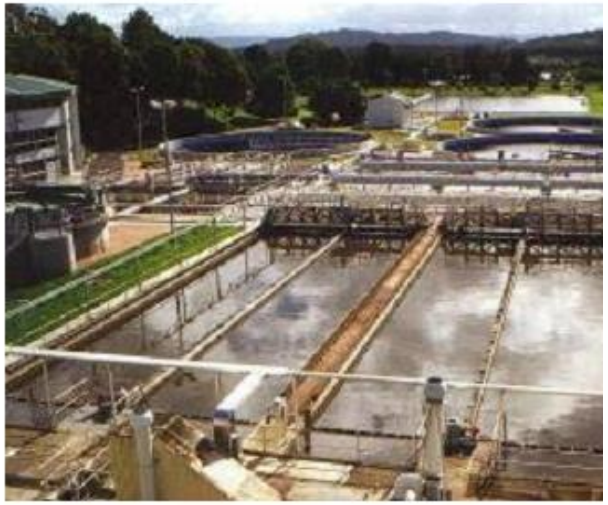
- Um firewall estava no local para isolar a rede de controle da rede da empresa, no entanto, havia uma conexão T1 a partir de uma empresa de consultoria de software, que entrou na rede de controle por trás do firewall, ignorando todas as políticas de controle de acesso impostas pelo firewall corporativo.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

Exemplos de Ataques

Ataque ao sistema de Águas de Maroochy Shire

31/10/2001

- Ataque ao sistema de controle de tratamento de resíduos de Maroochy Shire em Queensland, Austrália.
- Funcionário da Watertec insatisfeito provocou 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.
- Prejuízo da ordem de milhões de dólares.



Exemplos de Ataques

O GLOBO TECNOLOGIA BUSCAR Notícias Na web Busk

Publicada em 30/04/2011 às 22h38m

Epidemia do supervírus Stuxnet se infiltra em indústrias, empresas de energia e teles

Gilberto Scofield Jr.

DÊ SEU VOTO MÉDIA: 5,0 Share 35 Tweet 60

Recomendar 35 pessoas recomendam isso.

SÃO PAULO - Na semana passada, Gholamreza Jalali, diretor da Defesa Civil do Irã, afirmou que o país foi alvo de ataque cibernético por um vírus batizado de "Stars". Segundo ele, foi a segunda vez em menos de um ano que o país sofreu um ataque de um vírus altamente sofisticado, que os especialistas já chamam de "míssil cibernético teleguiado". Em meados de 2010, quando o governo iraniano se preparava para abastecer o reator de sua principal usina nuclear (Bushehr), o sistema de informática da instalação foi paralisado pelo vírus Stuxnet.

A maneira inteligente como o Stuxnet se infiltrou sem ser detectado e, dentro da

Normas de Segurança

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 10 October 2004

NOTICE OF COPYRIGHT
This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.

ISA-The Instrumentation, Systems, and Automation Society

Normas de Segurança

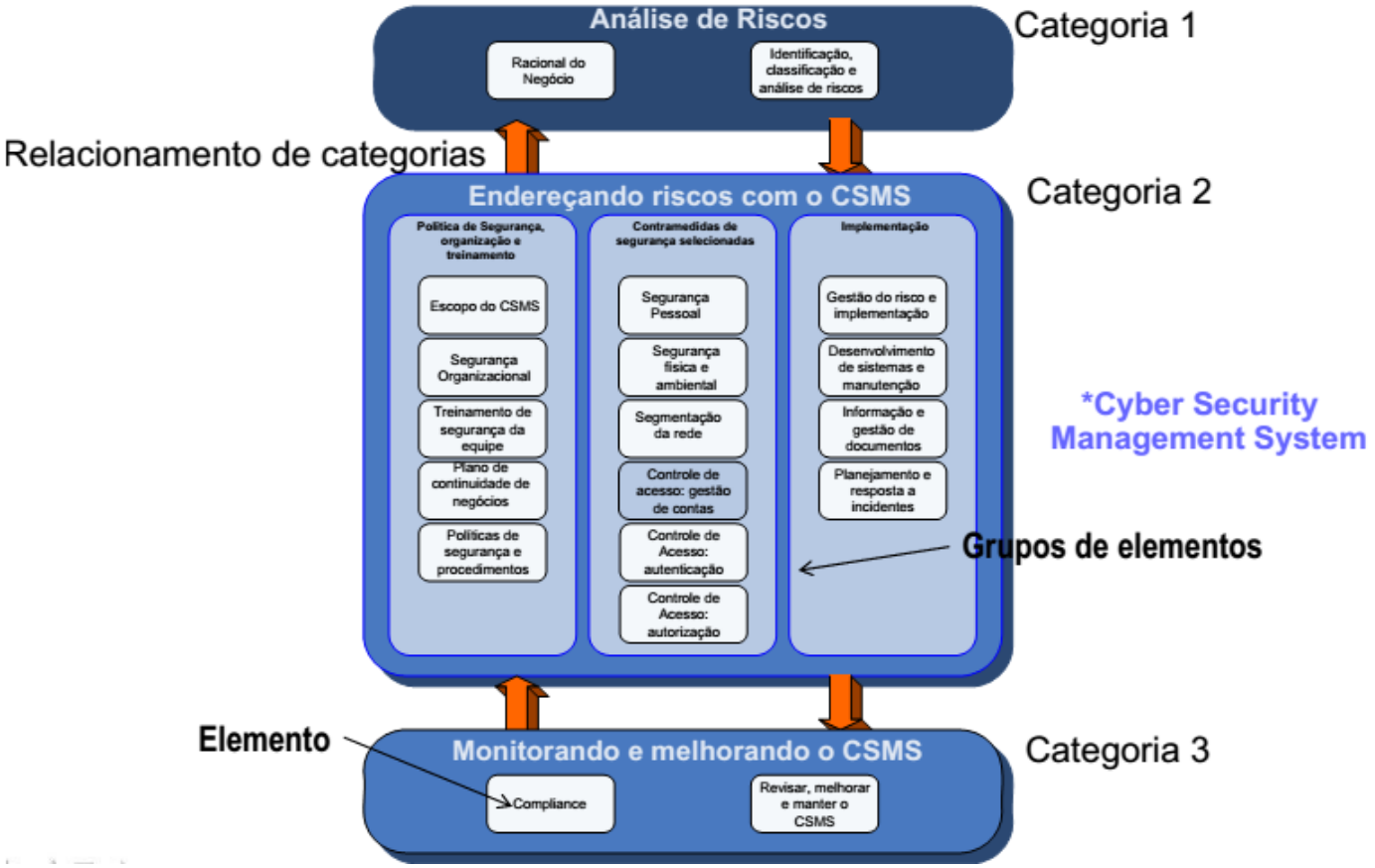
Relatórios Técnicos da ISA 99

- **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

Normas de Segurança

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

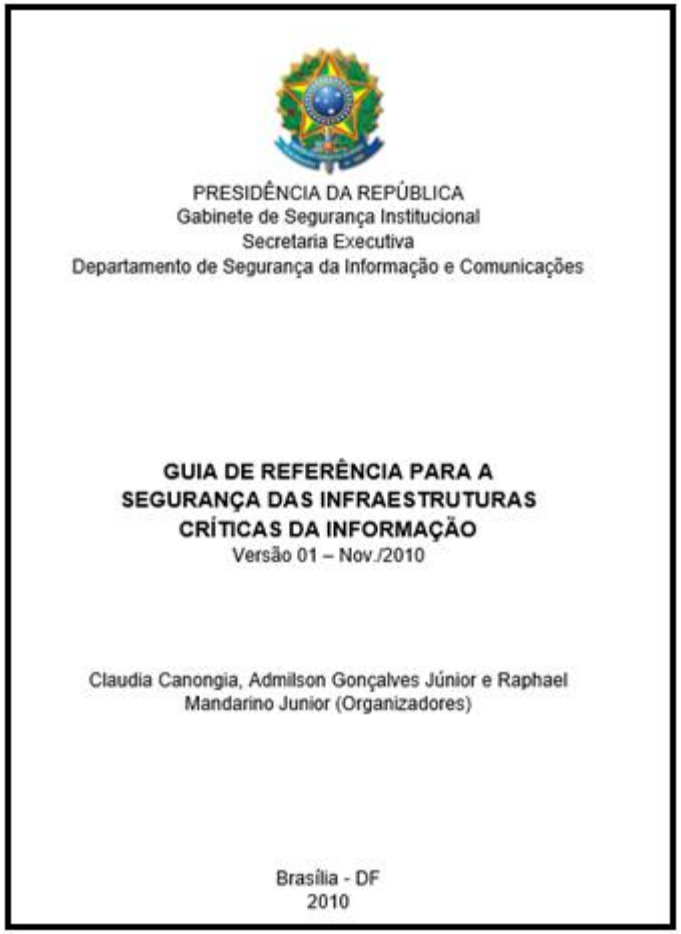


Implementação do CSMS

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

Guia de Referência

- Desenvolvido pelo CGSI (Comitê Gestor da Segurança da Informação), órgão ligado à presidência da república e instituído através da portaria 45 DSIC GSI
- O Guia visa garantir a segurança das infraestruturas críticas da informação no Brasil



PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Secretaria Executiva
Departamento de Segurança da Informação e Comunicações

GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO
Versão 01 – Nov./2010

Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior (Organizadores)

Brasília - DF
2010

Conclusões

- Os sistemas de automação industrial estão migrando para a plataforma windows, o que os torna vulneráveis.
- Incidentes de segurança colocam em risco a estabilidades dos serviços críticos e vidas humanas.
- Surgimento de ataques e Cyberarmas se intensifica.
- Sistemas SCADA são projetados visando disponibilidade e não segurança ➔Indústrias são alvos fáceis.
- Existem normas e frameworks para segurança de automação industrial.
- O Framework CSMS é o caminho para a implementação de segurança em plantas de automação.
- É fundamental investir em treinamento e conscientização.