MaxControl

Apresentação Institucional

GROUPE SNEF

Key Figures

Nossa Presença

Global e no Brasil

+15

Milhões de Reais em contratos de serviços

+16

Equipe técnica (Engenheiros e Técnicos)

+40

Anos de experiencia da nossa equipe

+10

Clientes que confiam na nossa experiência

Oficces:
Rio de Janeiro (MaxControl), São Paulo (SNEF), Belo Horizonte (SNEF-HQ), Rio Claro-SP (SNEF) Porto Alegre (Sequor)

Contracts executed internationally:

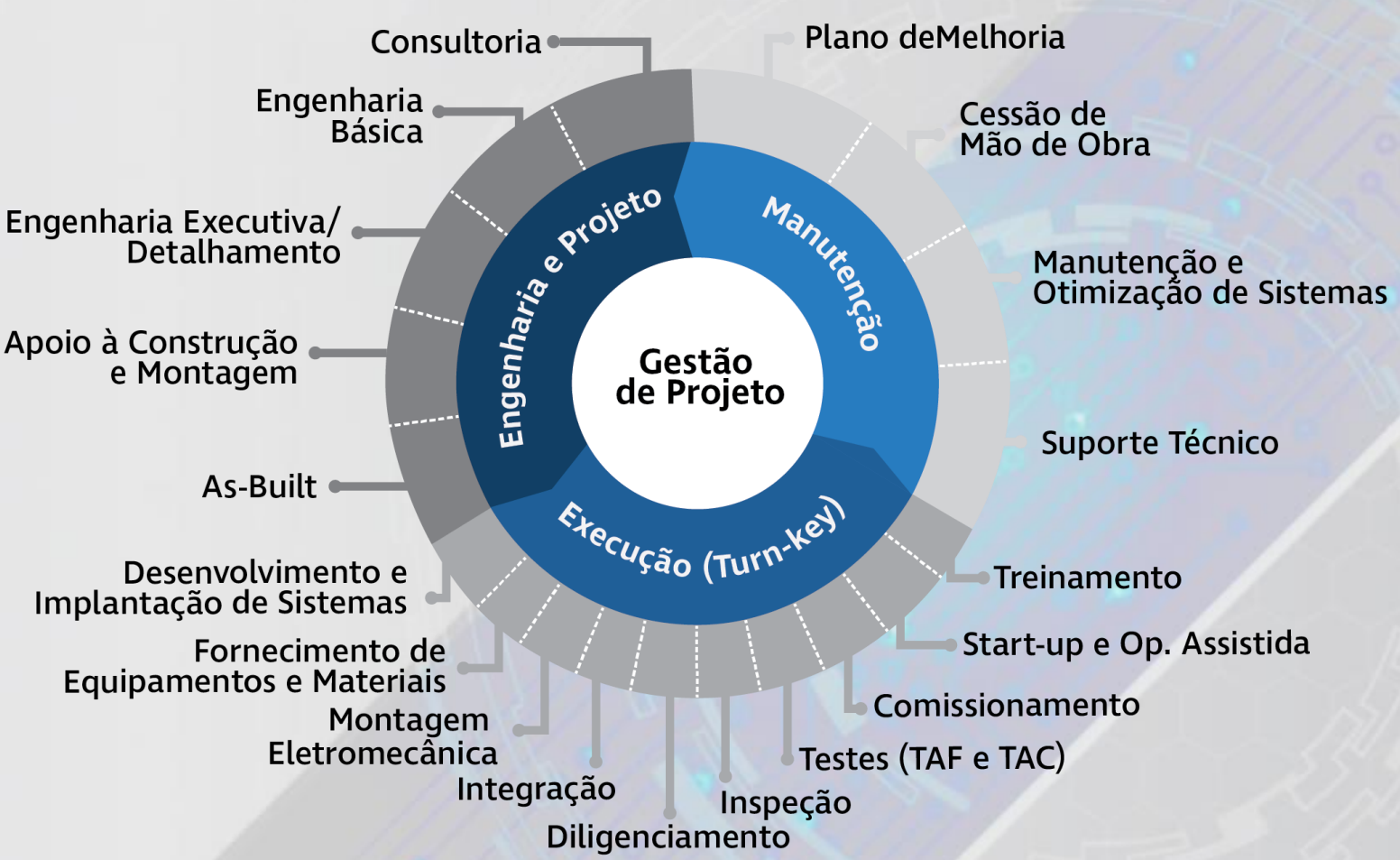
China: Dalian

Singapore

Malaysia: Kuala Lumpur

Colombia

Serviços


Consultoria
Engenharia Básica
Engenharia Executiva/ Detalhamento
Apoio à Construção e Montagem
As-Built
Desenvolvimento e Implantação de Sistemas
Fornecimento de Equipamentos e Materiais
Montagem Eletromecânica
Integração
Diligenciamento
Inspeção
Testes (TAF e TAC)
Comissionamento
Start-up e Op. Assistida
Treinamento
Suporte Técnico
Manutenção e Otimização de Sistemas
Cessão de Mão de Obra
Plano deMelhoria
Engenharia e Projeto
Manutenção
Execução (Turn-key)
Gestão de Projeto

Disciplinas

- Processo/Segurança/Utilidades
- PLC/SDCD/SCADA
- Redes Industriais
- Centro de Comando e Controle

- Baixa e Média Tensão
- Eletrocentros e Subestações
- Painéis (CDC/CCM)
- Relés Inteligentes/Dijuntores
- Conversores de Frequência/Soft-starter

- Redes
- Telemetria
- CFTV
- PA/GA
- Radio
- GPS

Controle e Automação | **Instrumentação** | **Elétrica** | **TI Industrial** | **Telecom**

- Sensores/Detectores/Transmissores
- Válvulas/Atuadores/Posicionadores
- Analisadores
- Medidores

- Desenvolvimento de Sistemas
- Redes
- PIMS/LIMS/MES
- ERP
- RFID
- IIoT
- ITS (Intelligent Transportation System)

Diferenciais

Tecnologias e Certificações

MaxControl

GE Intelligent Platforms

SIEMENS

altus

EMERSON Industrial Automation

Schneider Electric

HIMA SAFETY NONSTOP

Honeywell

Rockwell Automation

TÜVRheinland

HIRSCHMANN

ISA

IACS CYBER SECURITY

- **Industrial Automation Control System**
- A Cyber Security para sistemas de controle e automação industrial é baseada na ISA/IEC62443
- A preocupação da IACS Cyber Security é com a disponibilidade e integridade , ela deve garantir a continuidade do negócio.
- Insidentes de Cyber Security em redes corporativas normalmente tem como consequência a perda financeira , em IACS as consequências podem ser a perda de vidas humanas , desastres ambientais , e prejuízos na média R$5 milhões por falha de segurança.(fonte : NCSC)

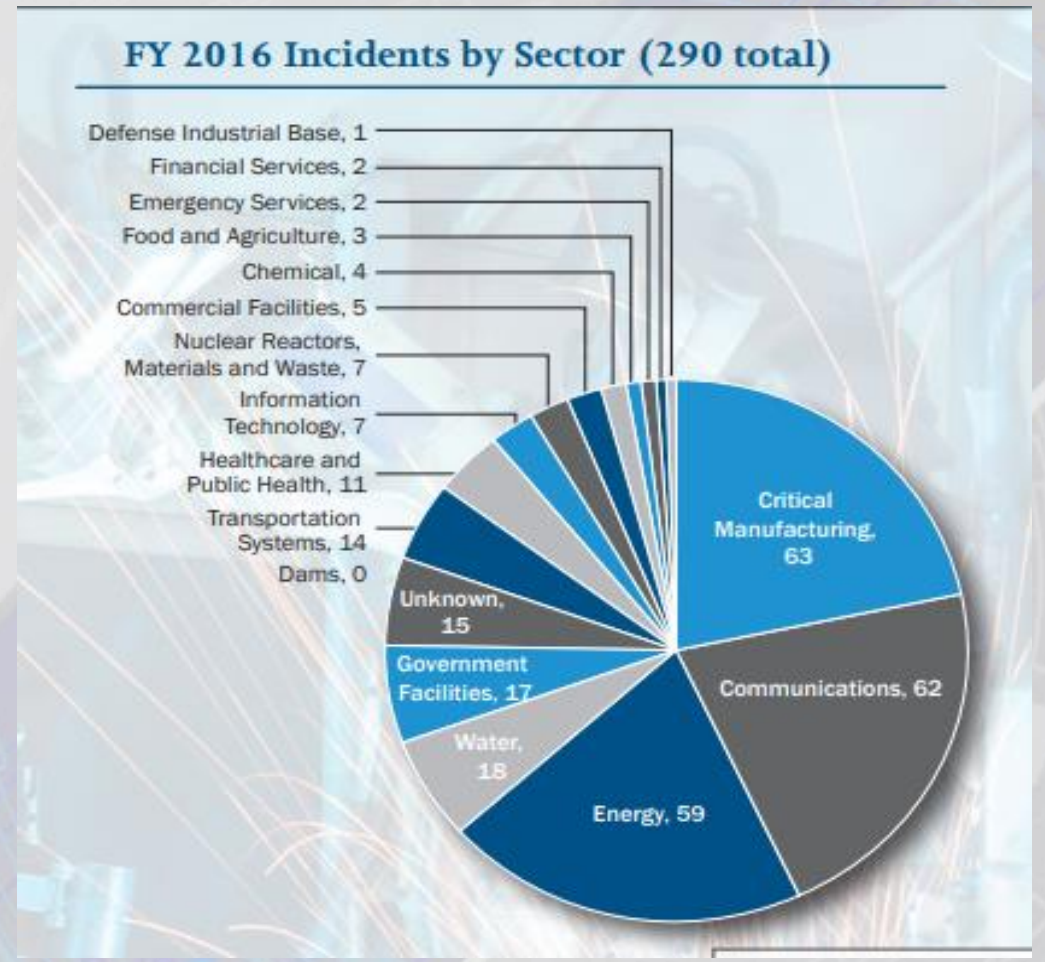
IACS MITOS

- IACS não está conectado a internet – e as atualizações são feitas por onde ?
- Estou atrás do Firewall – os ataques mais perigosos são os internos e as ameaças estão cada vez mais sofisticadas.
- Hackers não entendes de IACS – a conferência hacker black hat , tem uma área dedicada a IACS.
- Minha planta não é um alvo – Nos EUA só o CERT-US respondeu a 290 incidentes de IACS em 2016
- Meus sistemas de segurança vão me proteger - 86% das grandes empresas já reportaram algum incidente

Estamos sendo atacados !

NCCIC

- ICS-CERT Industrial Control Systems Cyber Emergency Response Team respondeu 290 incidentes em 2016



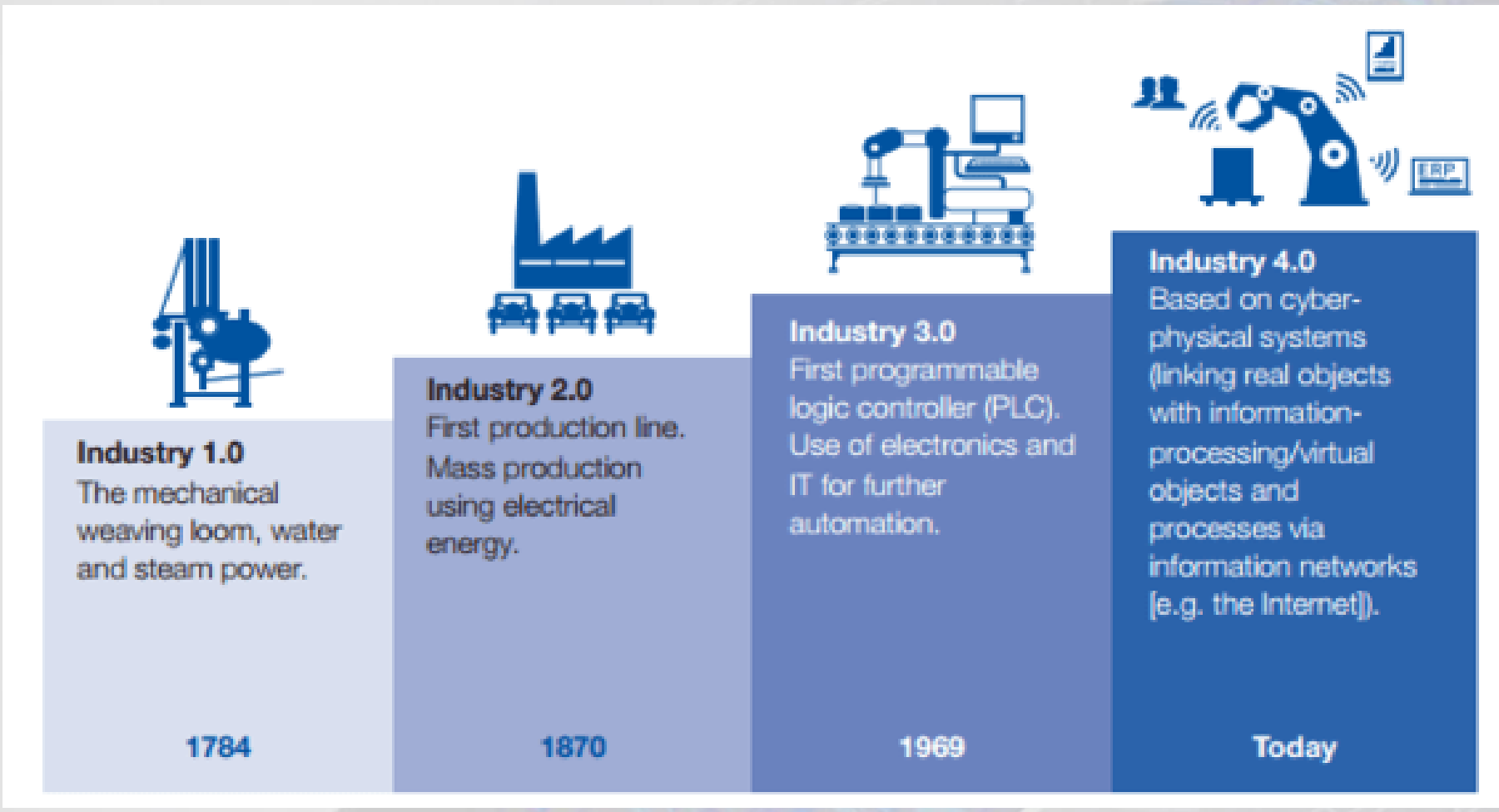
LEGISLAÇÃO

- A PNSIC (Política Nacional de segurança de infraestruturas críticas Dec N° 9.573) e PNSI (Política nacional de segurança da informação Dec 9.637), LGPD (Lei Geral de Proteção de dados)
- Apesar da estratégia nacional ainda não estar concluída as empresas já precisam tomar ações para proteger os ativos , o meio ambiente e a população.

IOT , INDÚSTRIA 4.0 ,TA,TO, TIC

TECNOLOGIA DA INFORMAÇÃO + IACS

ONDE ESTAMOS

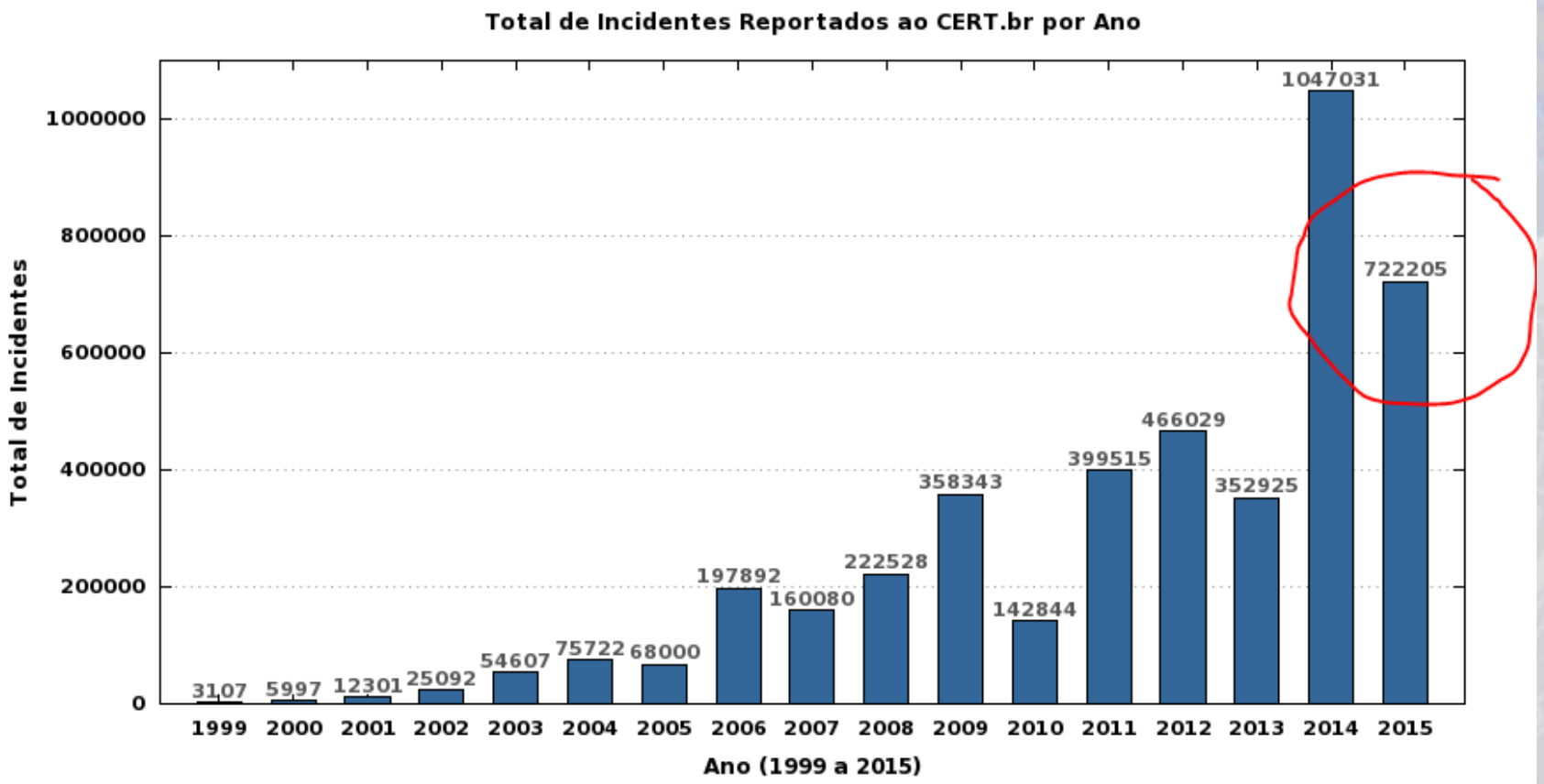


Cert.br , isto é sério ?

Estatísticas dos Incidentes Reportados ao CERT.br

| 2015 | 2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002 | 2001 | 2000 | 1999 |

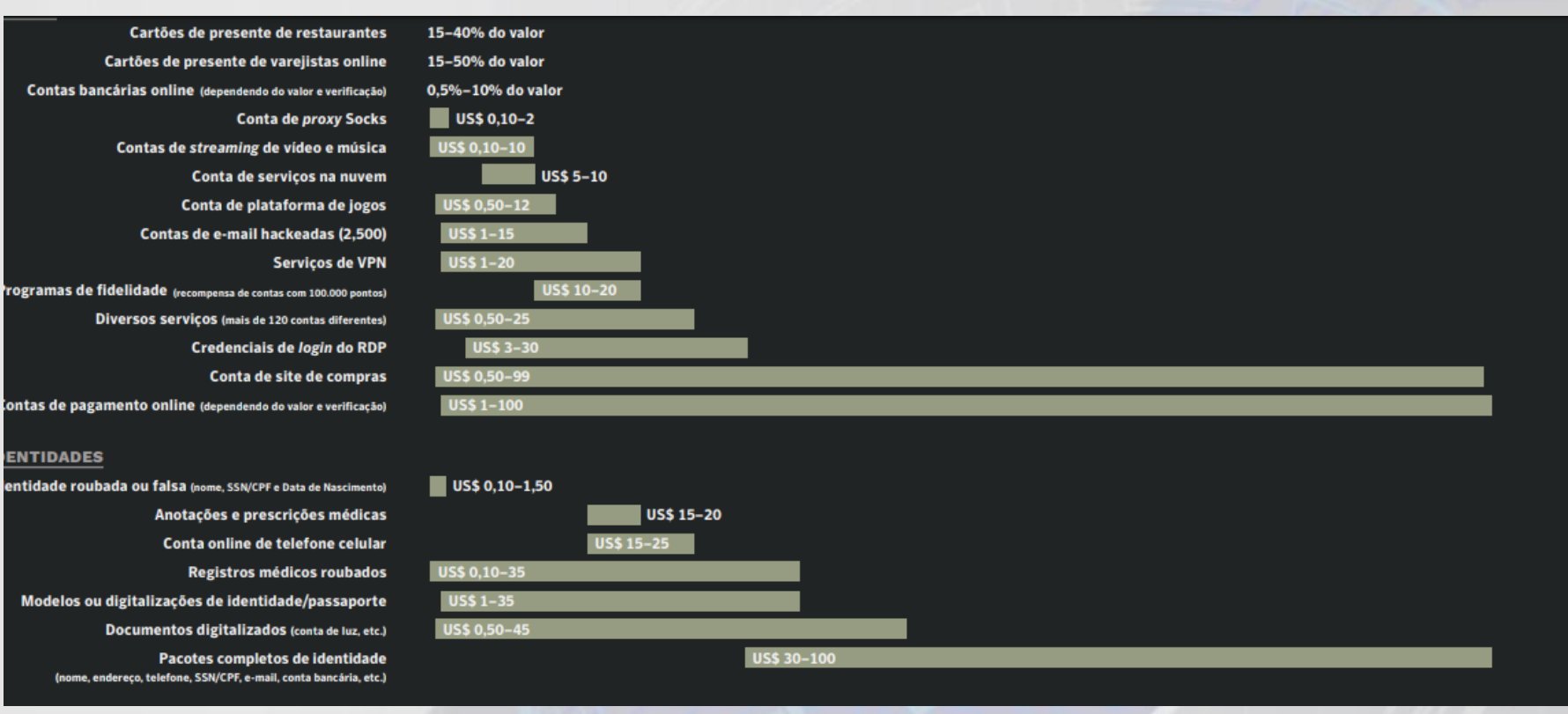
Valores acumulados: 1999 a 2015 novo



GROUPE SNEF

Deep Web

MAXCONTROL



O cyber crime faz parte do crime organizado.

MAXCONTROL

- Transformação do cibercrime em um setor plenamente desenvolvido, com fornecedores, mercados, provedores de serviços **(“cyber crime as a service”)**, financiamento, sistemas de comércio e uma proliferação de modelos de negócios.
- Um fornecedor de segurança **informou** um retorno de investimento de 1,425% em uma campanha de malware hipotética, porém realista. Além disso, em um **estudo encomendado pela Intel Security**, o custo anual do cibercrime para a economia global foi estimado em aproximadamente US$ 400 bilhões.

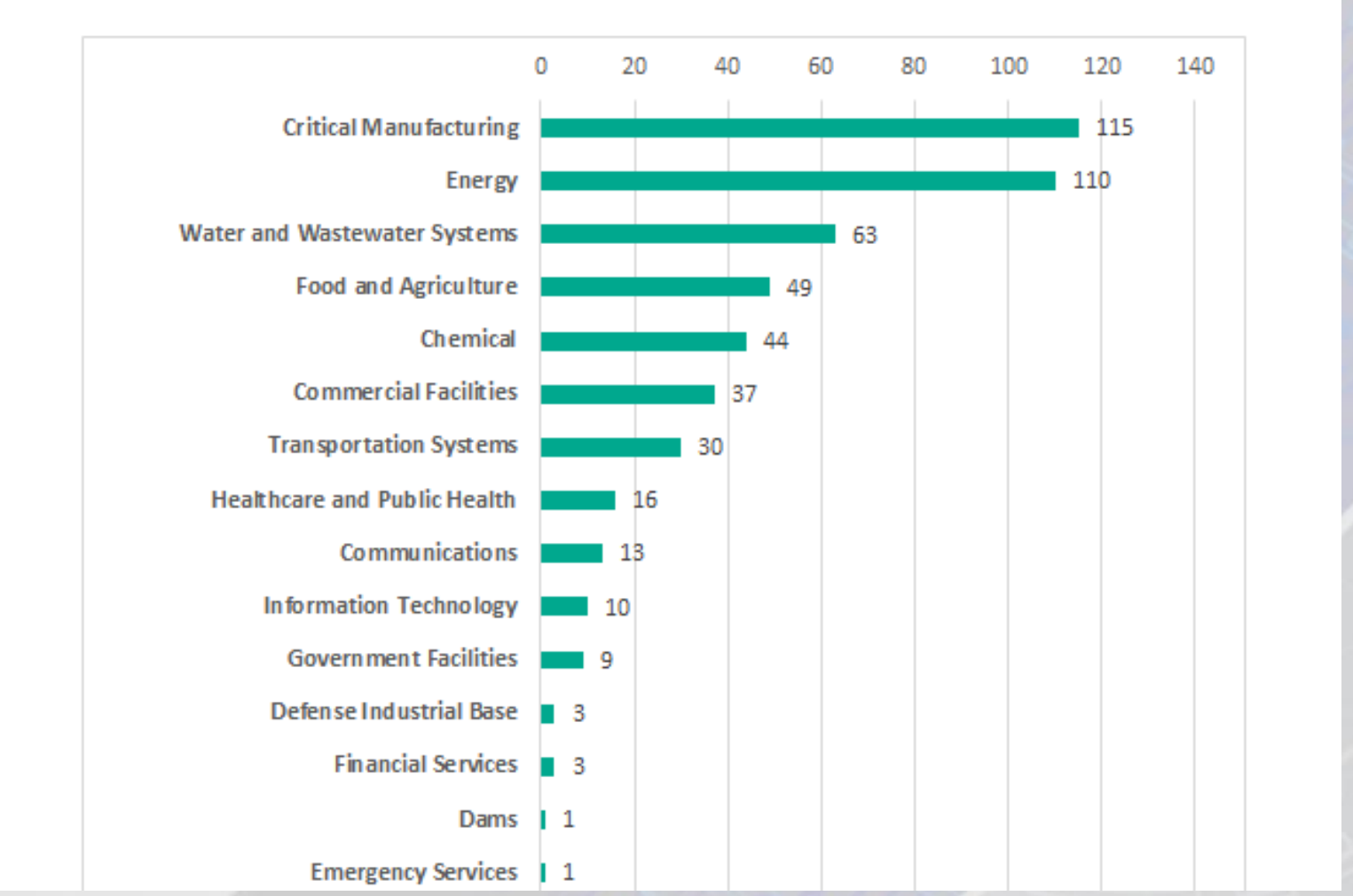
A ameaça é real e representativa

- **Um total de 295 incidents envolvendo infraestruturas críticas nos EUA,**
- O setor de energia corresponte a 32% dos incidents .
- O BlackEnergy malware existe desde 2007 e tem sido usado em inúmeros alvos incluindo o grande ataque à Ucrânica.

Sequestro da rede Elétrica de Israel

- *Nem um mês após a rede elétrica da Ucrânia ter sido vítima do primeiro apagão da história causado por malware, outra fornecedora de energia foi atingida por um ataque cibernético. Os noticiários foram rápidos em relatar o "grave ciberataque" anunciado pelo Ministro de Infraestrutura Nacional, Energia e Água de Israel, Yuval Steinitz.*

Kapersky vulnerabilidades



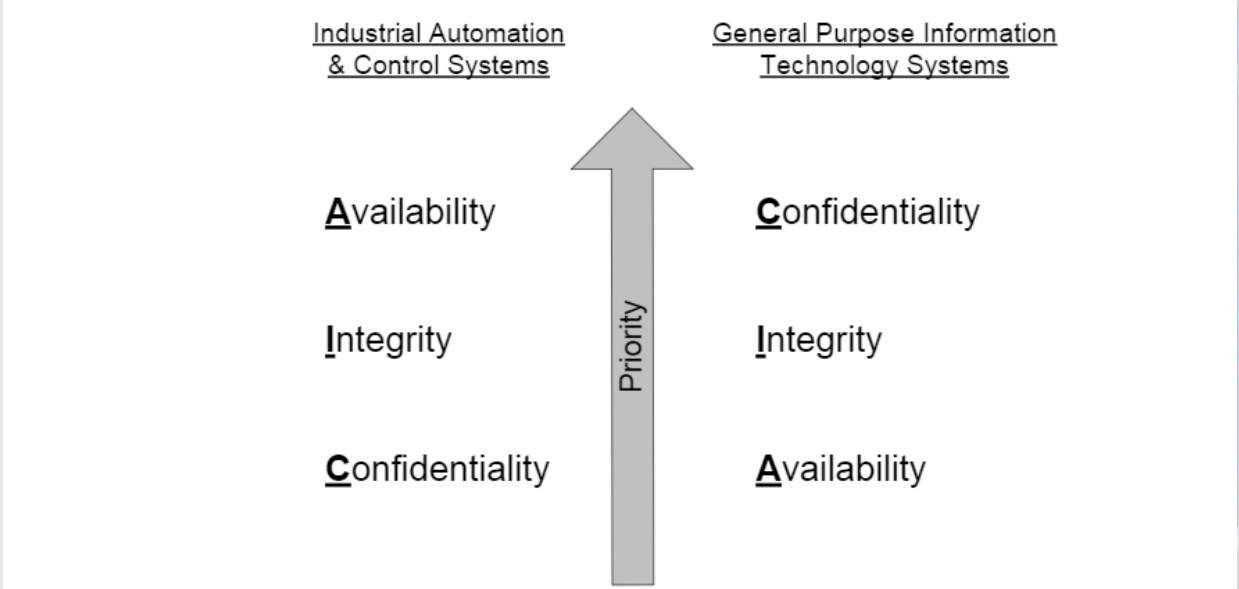
Estrutura da norma ISA99/ANSI 62443

MAXCONTROL

- ANSI/ISA 62443 – 1 – 1 : Terminologia , conceitos e modelos
- ANSI/ISA 62443 – 2 – 1 : Estabelecendo um programa de segurança para os Sistemas de controle e automação industrial
- ANSI/ISA 62443 – 2 – 3 : Trilha para Gerenciamento de Sistemas de controle e automação industrial
- ANSI/ISA 62443 – 3 – 3 : Requisitos de segurança de sistemas e níveis de segurança (maturidade)

Estratégias diferentes

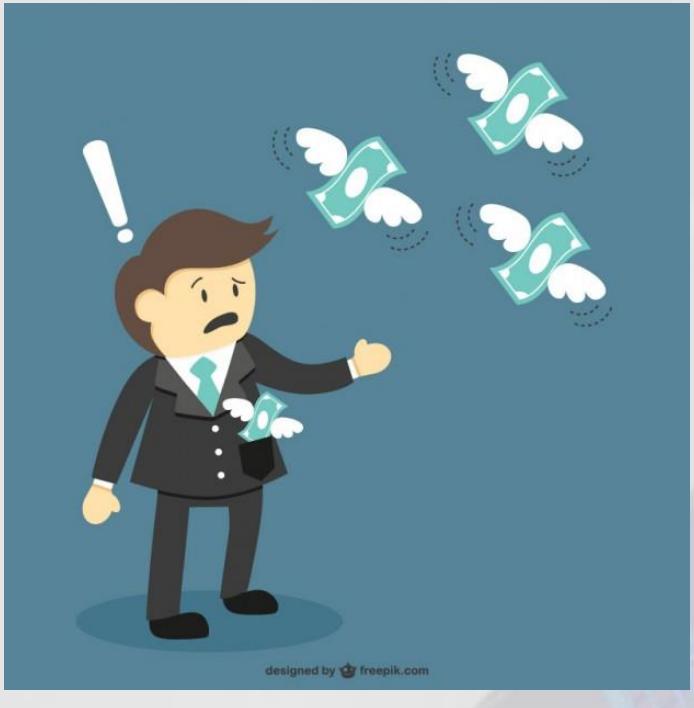
In some situations the priorities are completely inverted, as shown in Figure 1.



ISA 99 / IEC62443

- Preocupada com a disponibilidade e integridade
- Manutenção das infraestruturas críticas
- Preservação da vida das pessoas , consideradas como um ativo de segurança da informação
- Manutenção do nosso estilo de vida.

A diferença é o impacto



Consequências de um sinistro

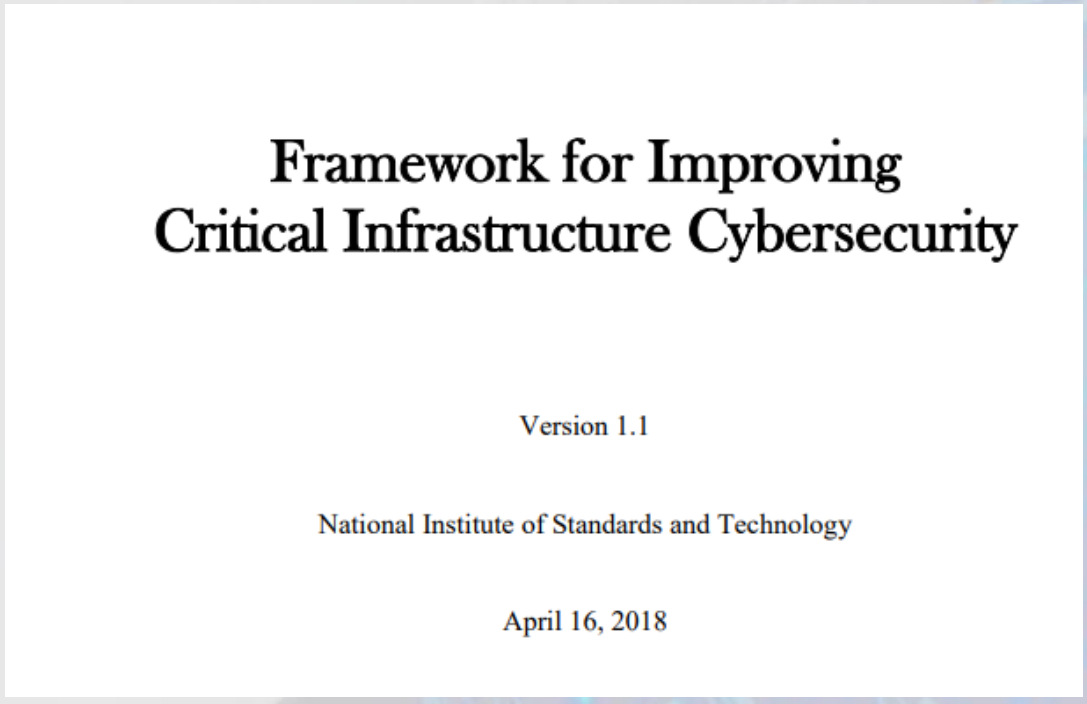
Table A.2 – Typical consequence scale

Consequence									
	Risk area								
	Business continuity planning		Information security			Industrial operation safety		Environmental safety	National impact
Category	Manufacturing outage at one site	Manufacturing outage at multiple sites	Cost (million USD)	Legal	Public confidence	People – on-site	People – off-site	Environment	Infrastructure and services
A (high)	> 7 days	> 1 day	> 500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional or national agency or long-term significant damage over large area	Impacts multiple business sectors or disrupts community services in a major way
B (medium)	> 2 days	> 1 hour	> 5	Misdemeanor criminal offense	Loss of customer confidence	Loss of workday or major injury	Complaints or local community impact	Citation by local agency	Potential to impact a business sector at a level beyond that of a single company. Potential to impact services of a community
C (low)	< 1 day	< 1 hour	< 5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits	Little to no impact to business sectors beyond the individual company. Little to no impact on community services

IEC 62443 / ISA 99 como padrão para o NIST

- O gerenciamento de risco está na vanguarda dessa nova versão. Já está acontecendo um aumento no uso de abordagens baseadas em risco para a segurança cibernética que se norteiam pelos conceitos de HAZOP e matriz de risco em segurança de processo.
- Essa novidade do NIST não protege sozinha, há outros recursos que devem usados, incluindo o padrão de segurança cibernética da International Electrotechnical Commission (IEC), #IEC62443.

NIST



Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

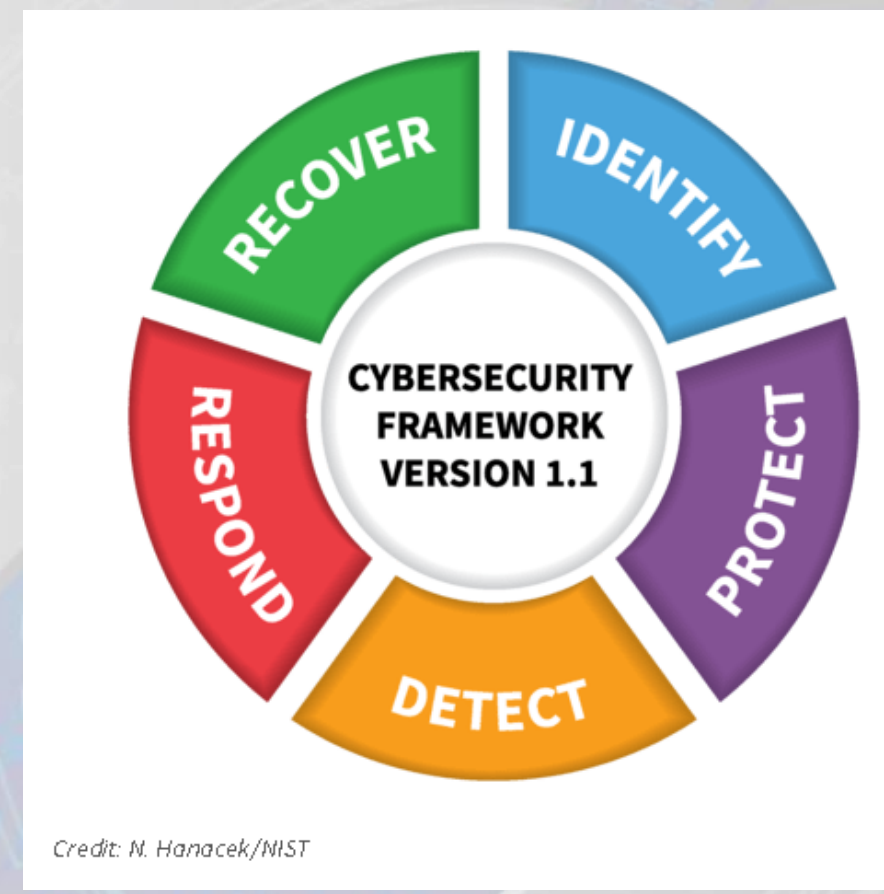
National Institute of Standards and Technology

April 16, 2018

MAXCONTROL

Framework para infraestruturas críticas

- O National Institute of Standards and Technology (NIST) divulgou a versão 1.1 de sua Framework for Improving Critical Infrastructure Cybersecurity, mais conhecida como a Estrutura de Segurança Cibernética



Six Cyber Threats to Really Worry About in 2018

MAXCONTROL

- https://www.technologyreview.com/s/609641/six-cyber-threats-to-really-worry-about-in-2018/
- **More huge data breaches**
- **Ransomware in the cloud**
- **The weaponization of AI**
- **Cyber-physical attacks**
- **Mining cryptocurrencies**
- **Hacking elections (again!)**

Cyber-physical attacks

MAXCONTROL

- Mais hackers direcionados a redes elétricas, sistemas de transporte e outras partes da infra-estrutura crítica dos países ocorrerão em 2018. Alguns serão projetados para causar perturbações imediatas , como o ataque que mergulhou a Ucrânia na escuridão ainda pode causar muito mais danos
- Outros envolverão ransomware que seqüestram sistemas vitais e ameaçam causar estragos, a menos que os proprietários paguem rapidamente para recuperar o controle sobre eles. Durante o ano, os pesquisadores - e hackers - provavelmente descobrirão mais brechas nas defesas de aviões, trens, navios e outros meios de transporte mais antigos que poderiam deixá-los vulneráveis.

Modelo de arquitetura segura

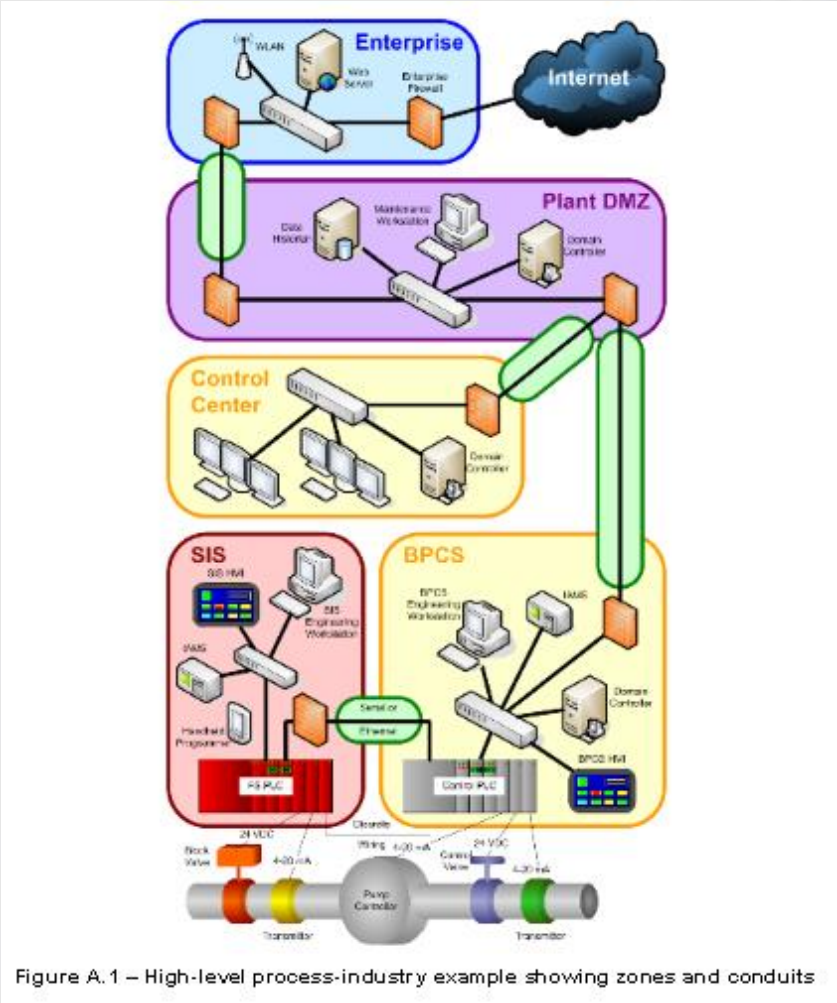


Figure A.1 – High-level process-industry example showing zones and conduits

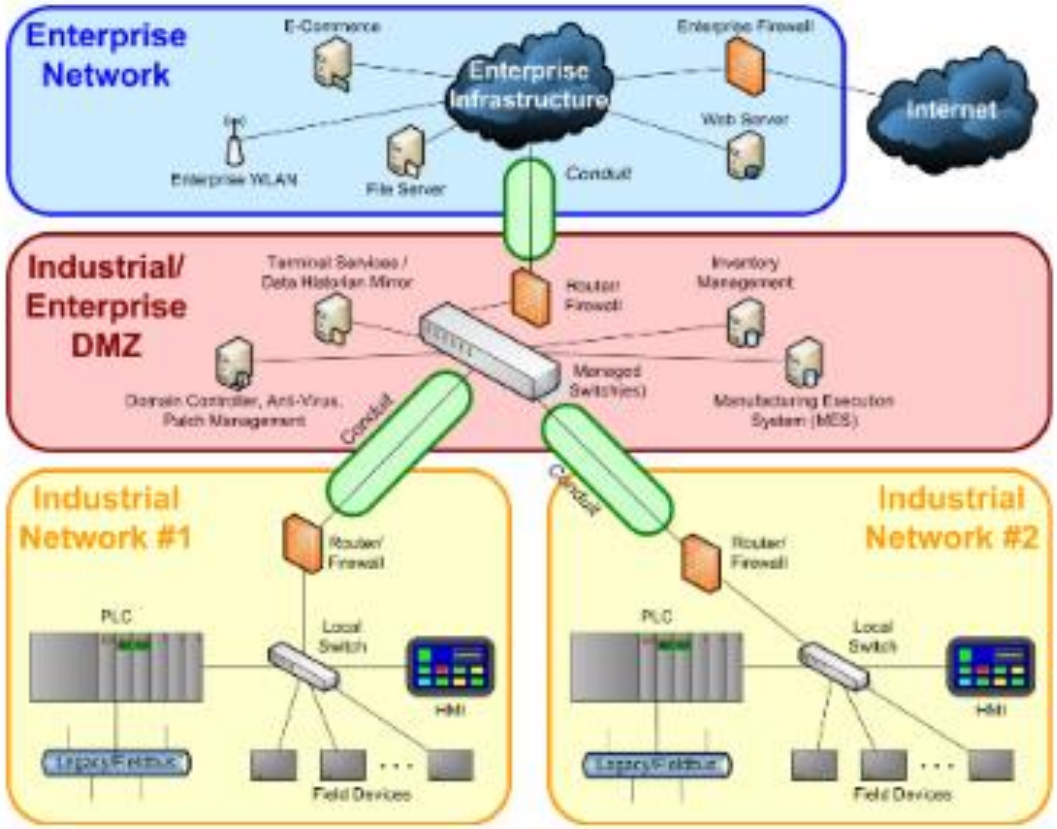
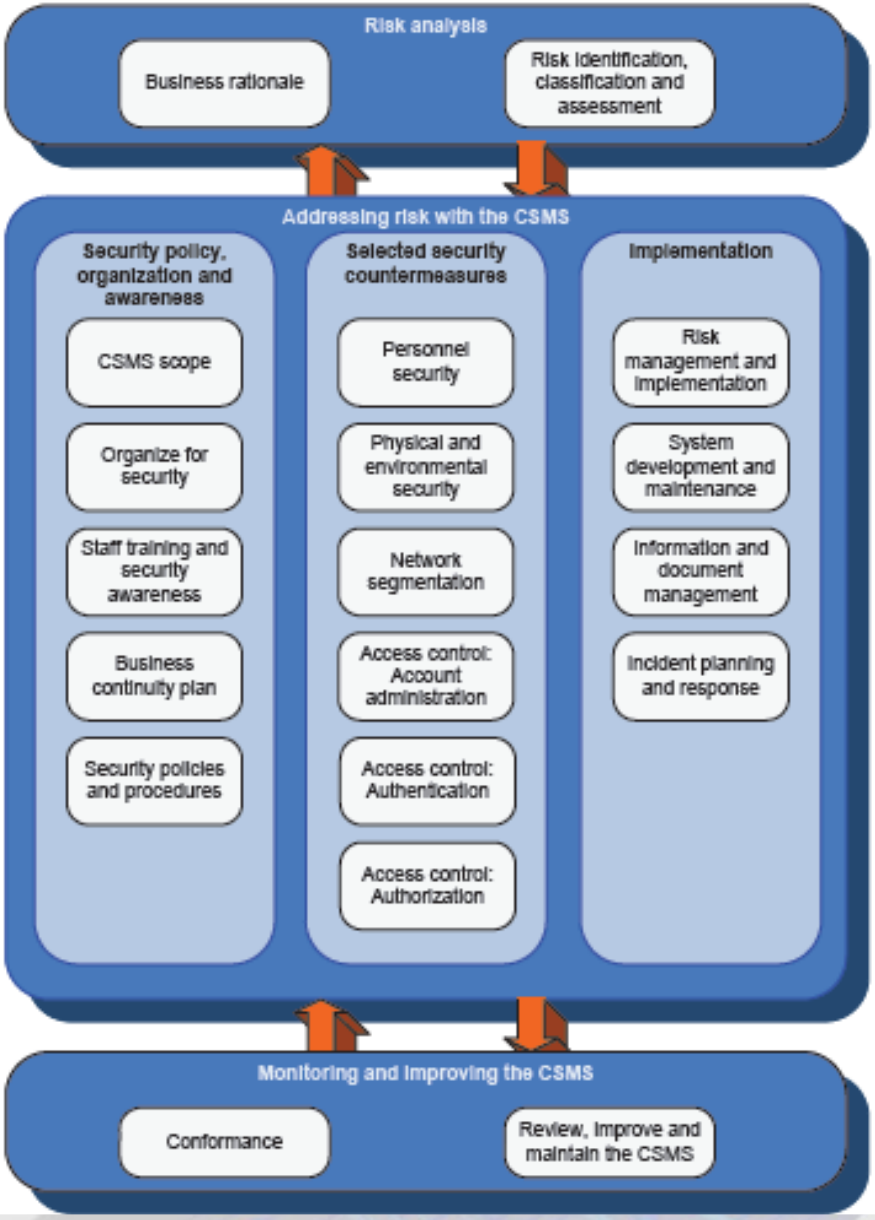
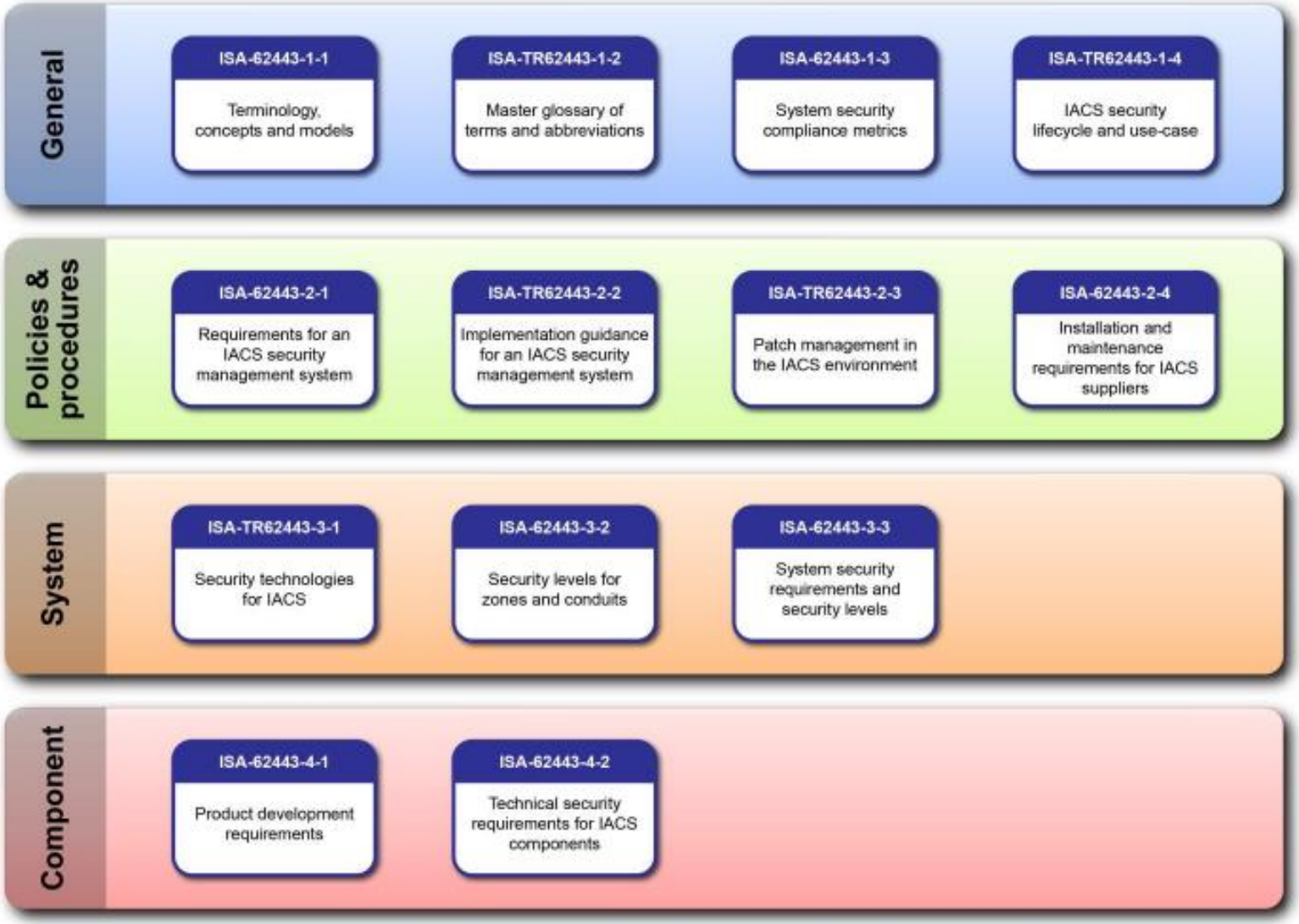


Figure A.2 – High-level manufacturing example showing zones and conduits

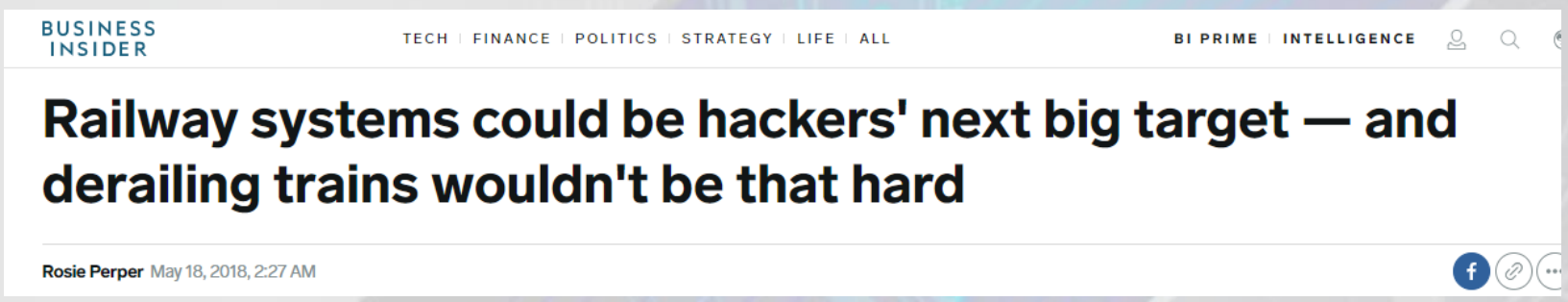

Risk analysis
Business rationale
Risk identification, classification and assessment
Addressing risk with the CSMS
Security policy, organization and awareness
CSMS scope
Organize for security
Staff training and security awareness
Business continuity plan
Security policies and procedures
Selected security countermeasures
Personnel security
Physical and environmental security
Network segmentation
Access control: Account administration
Access control: Authentication
Access control: Authorization
Implementation
Risk management and implementation
System development and maintenance
Information and document management
Incident planning and response
Monitoring and Improving the CSMS
Conformance
Review, improve and maintain the CSMS

MAXCONTROL


General
ISA-62443-1-1
Terminology, concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security compliance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-case
Policies & procedures
ISA-62443-2-1
Requirements for an IACS security management system
ISA-TR62443-2-2
Implementation guidance for an IACS security management system
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Installation and maintenance requirements for IACS suppliers
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security levels for zones and conduits
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product development requirements
ISA-62443-4-2
Technical security requirements for IACS components

MAXCONTROL

- **The British rail network came under attack from hackers 4 times in 2015. Although the attacks are said to have been purely exploratory in nature, the consequences could have been dramatic both for the company and for the passengers.**



BUSINESS INSIDER

TECH | FINANCE | POLITICS | STRATEGY | LIFE | ALL

BI PRIME | INTELLIGENCE

Railway systems could be hackers' next big target — and derailing trains wouldn't be that hard

Rosie Perper May 18, 2018, 2:27 AM

São Francisco

Gridlock

Cyberattack on San Francisco transit agency prompts Senate questions for Metro

- Sen. Mark R. Warner (D-Va.) wants to know how susceptible the Metro is to a cyberattack, following a “ransomware” hack that took down computers for San Francisco’s light-rail system late last year.

Conclusão

- Com a Indústria 4.0 não podemos simplesmente segregar redes corporativas das redes industriais e da núvem.
- Estratégias diferentes em localizações diferentes dentro desta rede integrada precisam ser implementadas.
- Uma análise de riscos minuciosa , deve ser feita constantemente com o auxílio de profissionais qualificados e especialistas na operação.
- Testes de invasão são fundamentais para rastrear vulnerabilidades.
- Uso de tecnologias biométricas como o reconhecimento facial para controle de perímetro.
- O Risco residual deve ser coberto com seguro ciber.

MAXCONTROL


danke
謝謝
teşekkür ederim
спасибо
thank you
gracias
dank je
tapadh leat
bedankt
hvala
mauruuru
dziękuję
mochchakkeram
go raibh maith agat
obrigado
sukriya
kop khun krap
taiku
arigatō
takk
dakujem
sagolun
grazie
merci
terima kasih
감사합니다
мерси

Perguntas

Obrigado

- Guilherme Neves
- Guilherme@doutornet.com.br
- Facebook.com.br/doutornet tecnologia.
- Twitter @doutornetgui
- Blogspot.doutornet.com
- www.doutornet.com.br
- Linkedin : Guilherme Neves Doutornet

Serviços

Avaliação – CSET (cyber security evaluation tool)

Análise de riscos – HAZOP Detalhado

Análise do Nível de Maturidade e Plano estratégico

Teste de Invasão

CSMS (Cyber Security Management System)

Projeto de Cyber Security integrado com a Automação

Plano de continuidade de negócios

Política de segurança

Equipe de resposta a incidentes (treinamento e operação)