Setting the Standard for Automation™

Tutorial ISA 99 /IEC 62443

Prof. MSc Guilherme Neves

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

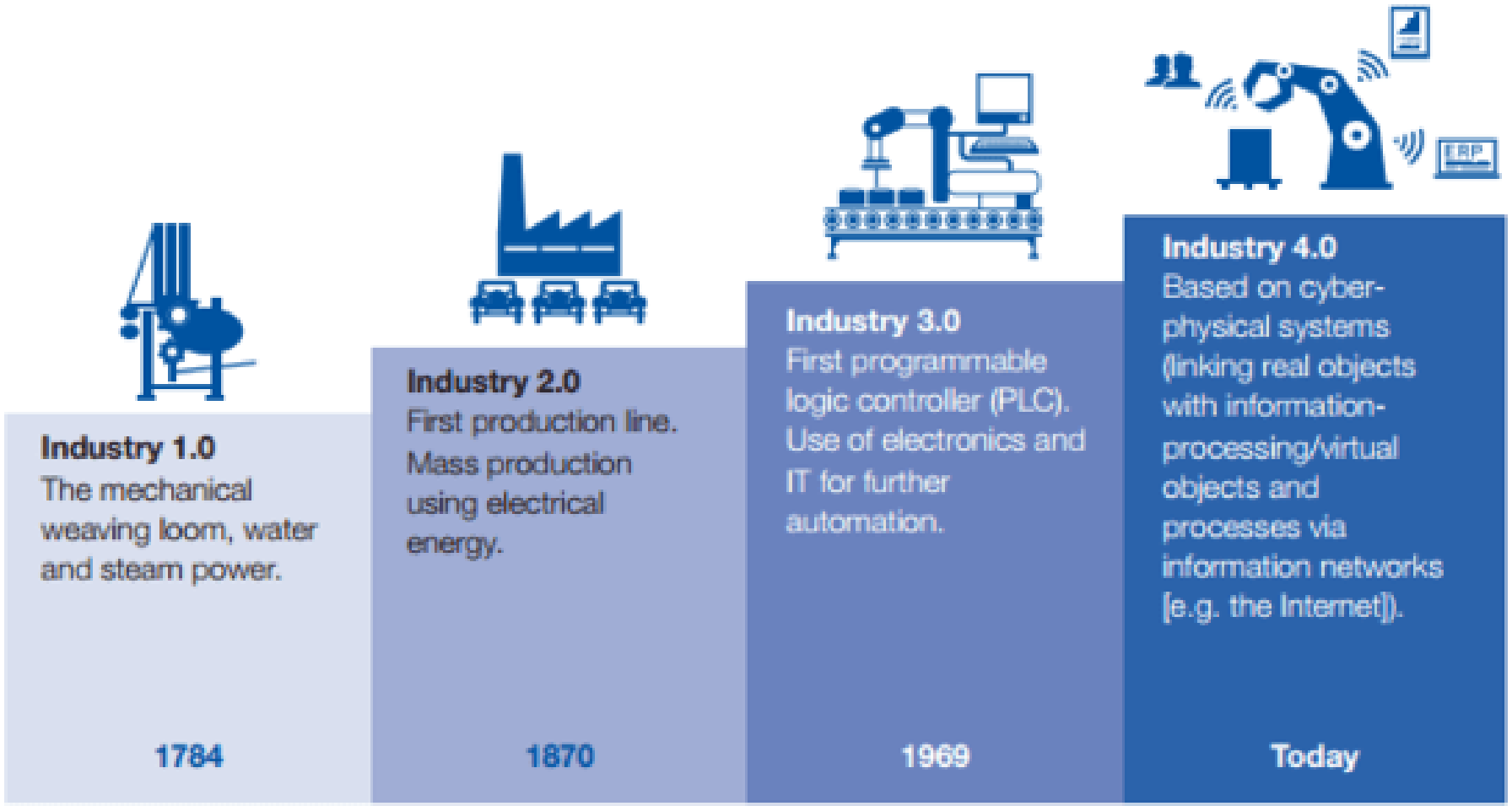
Quem sou eu

- Graduado em Redes de Computadores pelo Centro Universitário da Cidade (2011) , .Pos Graduado (Master Security Information-2012) , Mestre em Sistemas de Informação (M.Sc) UNIRIO, Doutorando em Projetos de TIC (PhD) Universidad Internacional do Mexico . Professor Graduação em Redes de Computadores da Faculdade SENAC , do MBA de Segurança da Informação na Universidade Petrobras, das Pós Graduações da UNICARIOCA, da UNIABEU e da ESTÁCIO,, . Palestrante de segurança da Informação na Marinha do Brasil e da Sociedade Internacional de Engenharia Farmaceutica (ISPE) e International Society of Automation (ISA). Autor do Livro segurança em redes . Membro do comitê Risk Mapp do ISPE , Membro do comitê da norma ISA99 / IEC 62443, Diretor de Ciber Segurança da ISA RJ, membro do IEEE (Institute of Eletrical and Eletronic Engenniers). Especialista em Investigação Digital Forense , Teste de invasão de redes . Formação em Data Science na T/UE (Eindehoven - Holanda) ,extensão em Information security in 10 domains (Kennesaw State University, Georgia , EUA), Coordenador do grupo de estudo da ISA 99 do D4 . Perito Judicial.

IOT , INDÚSTRIA 4.0 ,TA,TO, TIC

TECNOLOGIA DA INFORMAÇÃO + TECNOLOGIA DA AUTOMAÇÃO

ONDE ESTAMOS

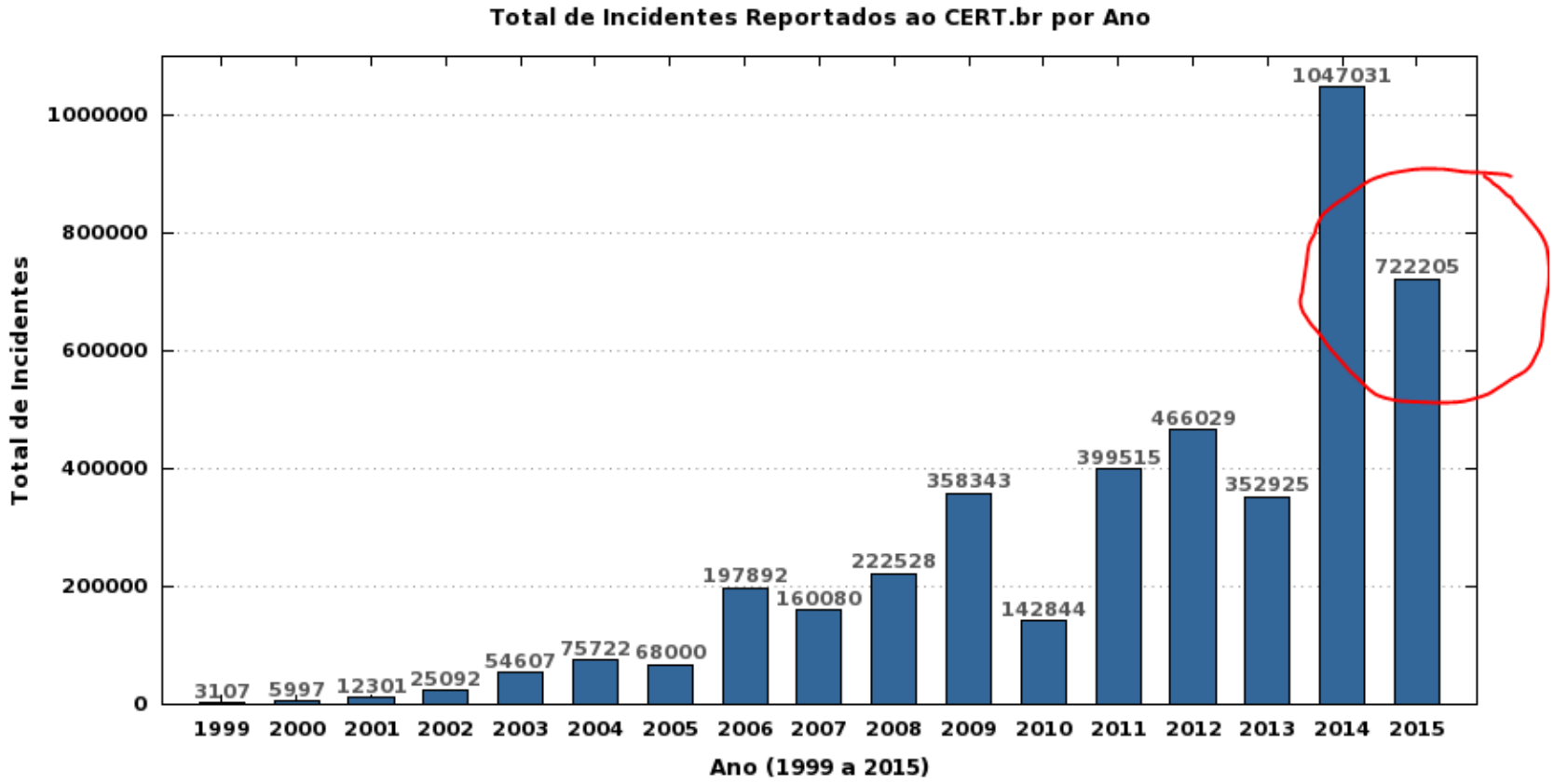


Cert.br , isto é sério ?

Estatísticas dos Incidentes Reportados ao CERT.br

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

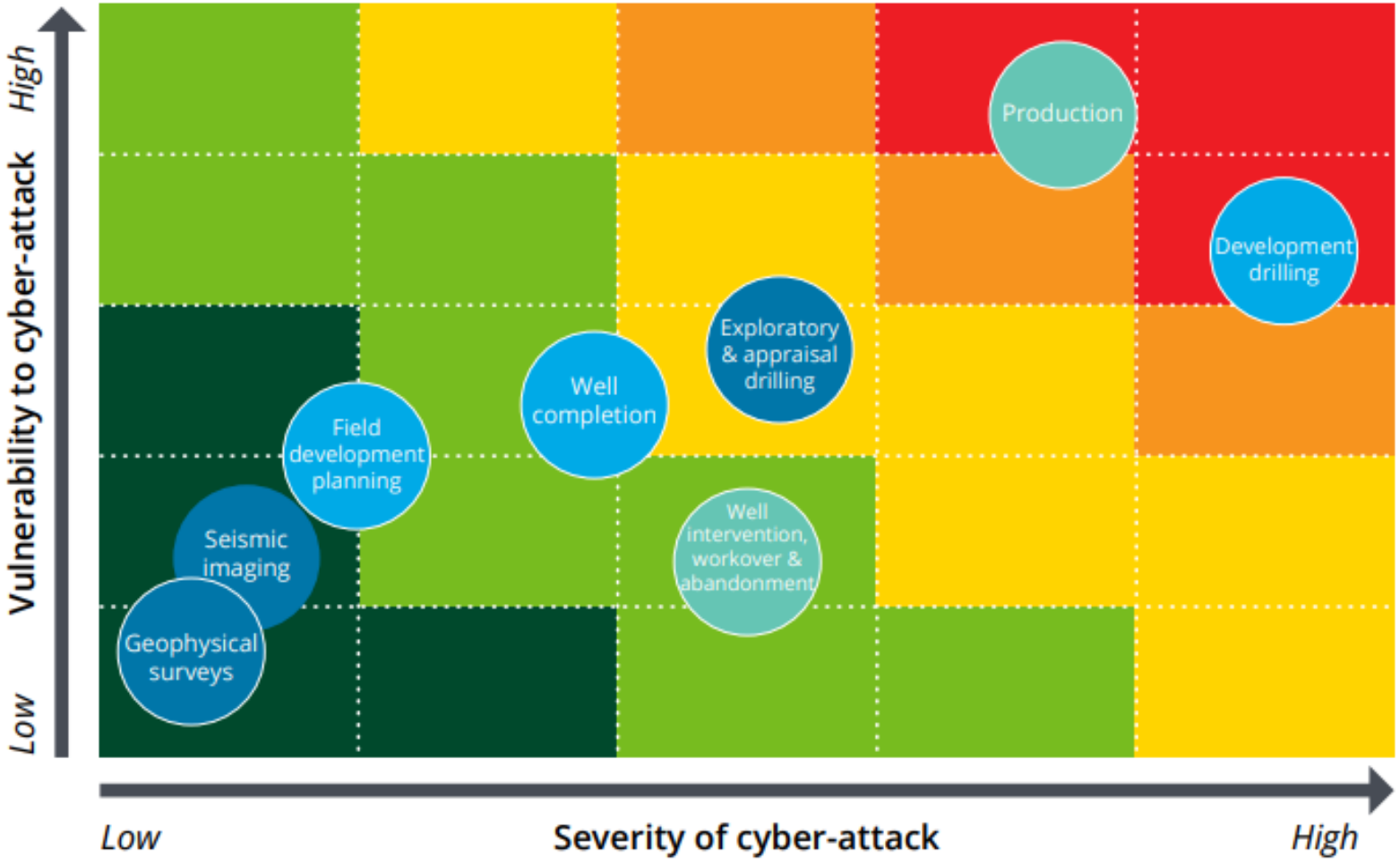
Valores acumulados: 1999 a 2015 novo



A ameaça é real e representativa

- **Um total de 295 incidents envolvendo infraestruturas críticas nos EUA, foram reportadas em sistemas de automação , Segundo o (ICS-CERT) no ano de 2015, comparado com 245 em 2014.**
- 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. (http://www.securityweek.com/critical-infrastructure-incidents-increased-2015-ics-cert)

Figure 3. Cyber vulnerability/severity matrix by upstream operations



https://www2.deloitte.com/insights/us/en/industry/oil-and-gas/cybersecurity-in-oil-and-gas-upstream-sector.html

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.*

- *"O vírus já foi identificado e o software certo já foi preparado para neutralizá-lo", disse Steinitz para milhares de profissionais de segurança na Cybertech 2016, em Tel Aviv. "Tivemos que paralisar muitos dos computadores da Central Elétrica de Israel. Estamos cuidando da situação e espero que em breve esse grave evento estará terminado… mas até agora, os sistemas de computadores ainda não estão funcionando como deveriam", disse ainda, como foi noticiado pelo The Times of Israel.*

O cyber crime faz parte do crime organizado.

- O que não esperávamos foi a 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. Naturalmente, o crime segue o caminho de menor resistência até o dinheiro e precisa ser bastante compensador, caso contrário, as pessoas deixarão de praticá-lo. Infelizmente, o cibercrime tem sido altamente compensador.
- 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.

Estrutura da norma ISA99/ANSI 62443

- 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)

Visão da ISO27002

Os controles considerados essenciais para uma organização, sob o ponto de vista legal, incluem, dependendo da legislação aplicável:

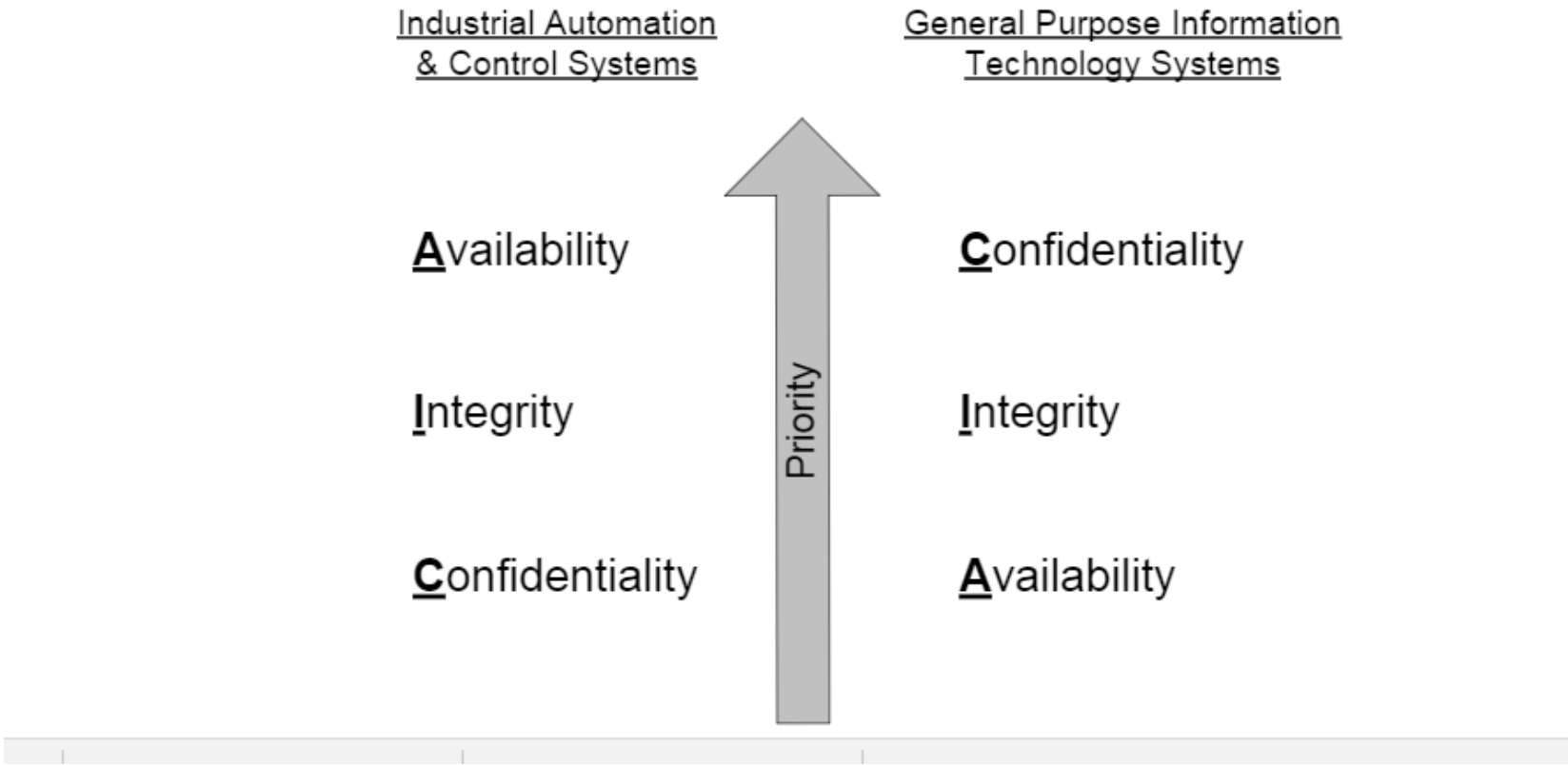
a) proteção de dados e privacidade de informações pessoais (ver 15.1.4);

b) proteção de registros organizacionais (ver 15.1.3);

c) direitos de propriedade intelectual (ver 15.1.2).

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

ISA

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

Fluxo da tomada de decisões

- Toma como base os níveis de maturidade da IEC 62443 / IDA 99

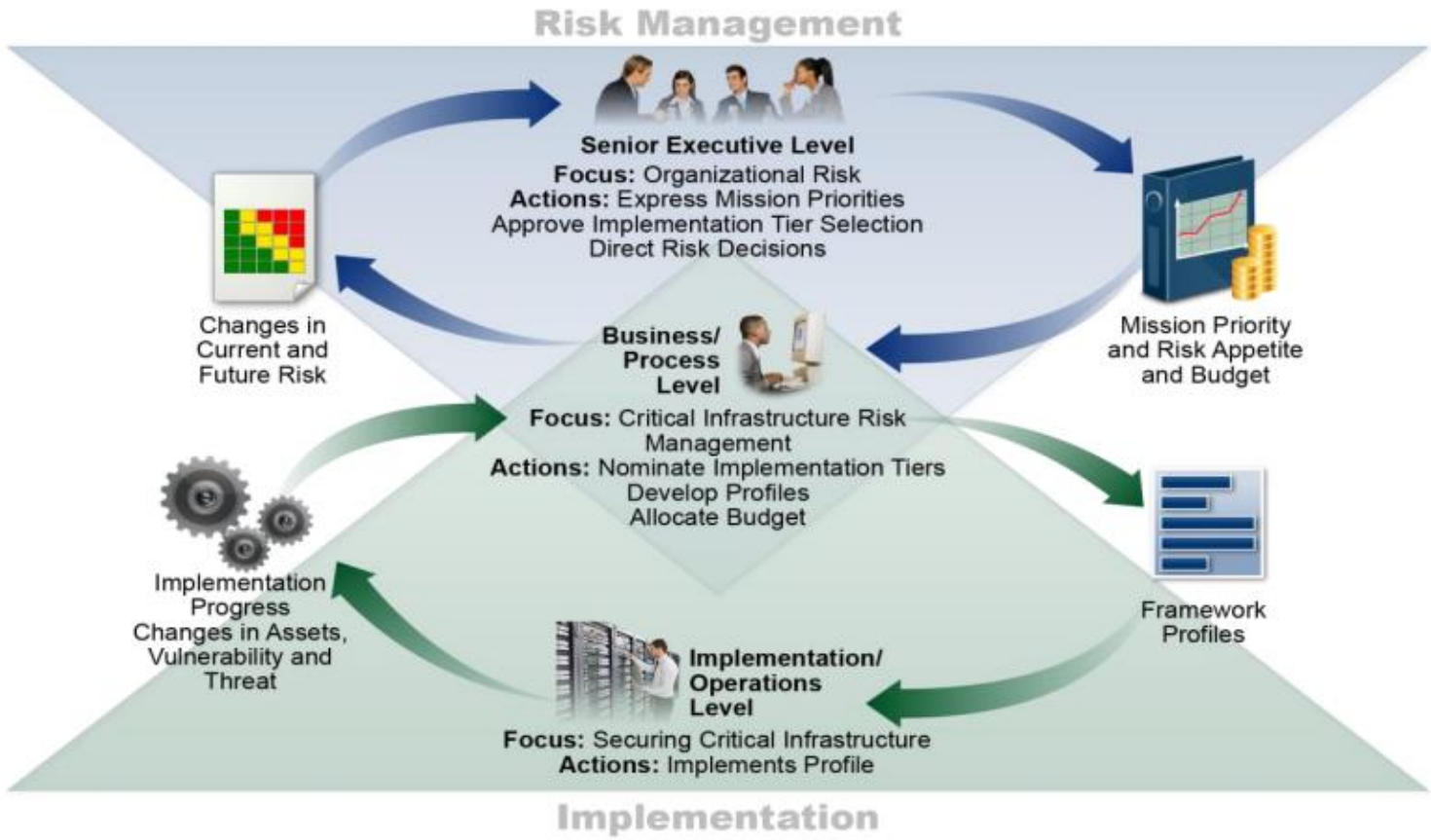


Figure 2: Notional Information and Decision Flows within an Organization

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

Credit: N. Hanacek/NIST

Em todo o CORE do Famework NIST a ISA é citada

Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

Six Cyber Threats to Really Worry About in 2018

- 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

- 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.

Consumidor x Prosumidor

- Impacto de um usuário com baixa infraestrutura entrado na GRID
- Vetores novos de ataque
- Quem vai garantir a segurança da cogeração doméstica ?
- Pequenas smart grids multi fontes , como integrar os SCADAS ?

Certificação ISA99 / 62443

- Produtos e fornecedores homologados
- Pessoal treinado e aculturado
- Processos de negócios alinhados com os objetivos da segurança da informação.
- Segurança da informação alinhada com os objetivos do negócio.
- Análise de riscos dos processos de negócio.
- Infraestrutura certificada e monitorada.
- Equipe de resposta a incidentes de segurança da informação.
- Plando de continuidade de negócios

Topologia de segurança rede ind.

- Segmentação para conter os impactos
- Multiplos níveis de acesso
- Quando mais próximo da operação mais barreiras para transport

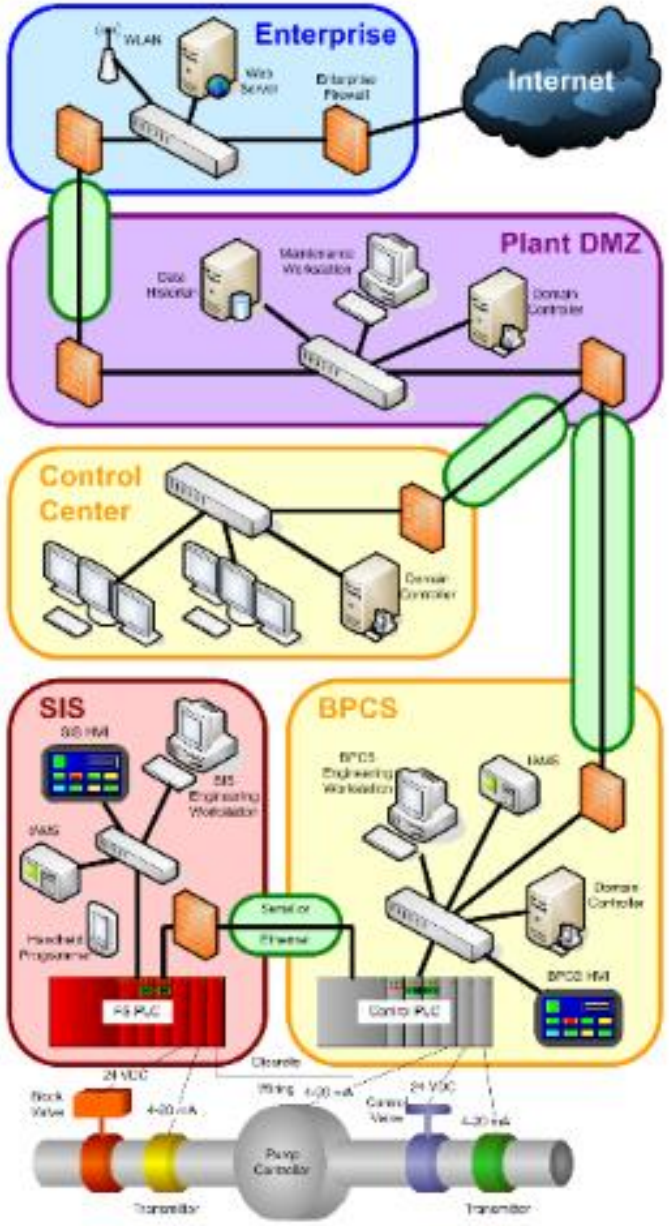


Figure A.1 – High-level process-industry example showing zones and conduits

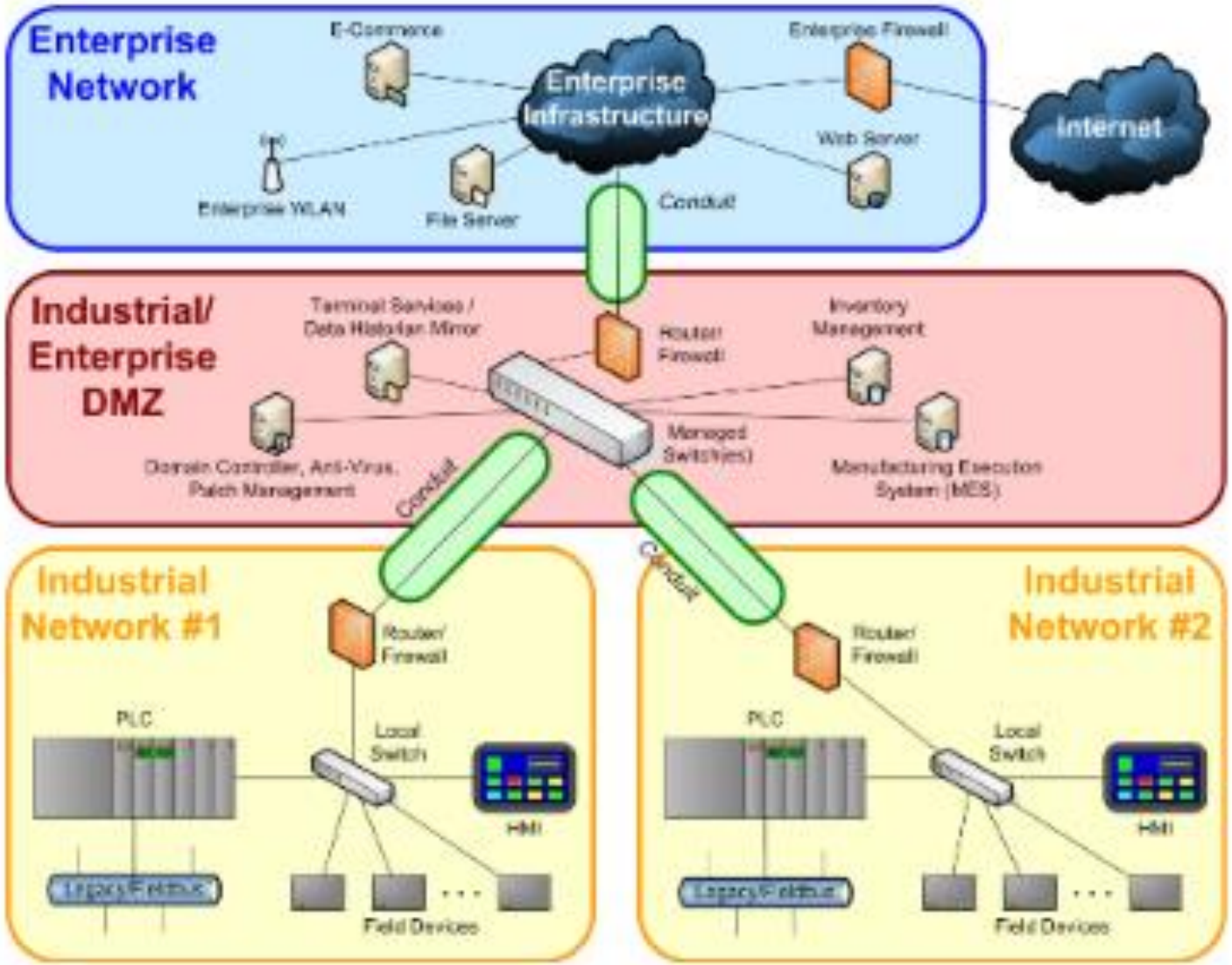


Figure A.2 – High-level manufacturing example showing zones and conduits

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.


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