

A Abordagem da Cemig na Segurança Cibernética



José Lopes @cemig.com.br

7º Fórum Brasileiro de CSIRTs

São Paulo, 14/09/2018

Agenda

1. Contextualização

Cemig e o setor elétrico
Infraestruturas críticas
Motivações de segurança

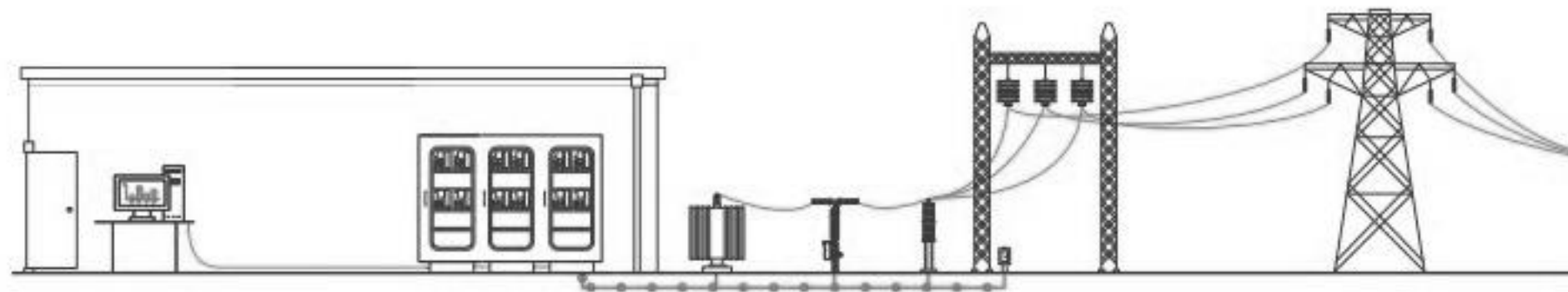
2. Rede Operativa de Dados

Evolução e anatomia
Aplicações e preocupações
Desafios

3. Mecanismos de Segurança

Hierarquia e CSIRT Cemig
Processos, controles, monitoramento e pentests
Protocolo de resposta a incidentes críticos
Novos projetos

4. Considerações Finais



Contextualização 1/5

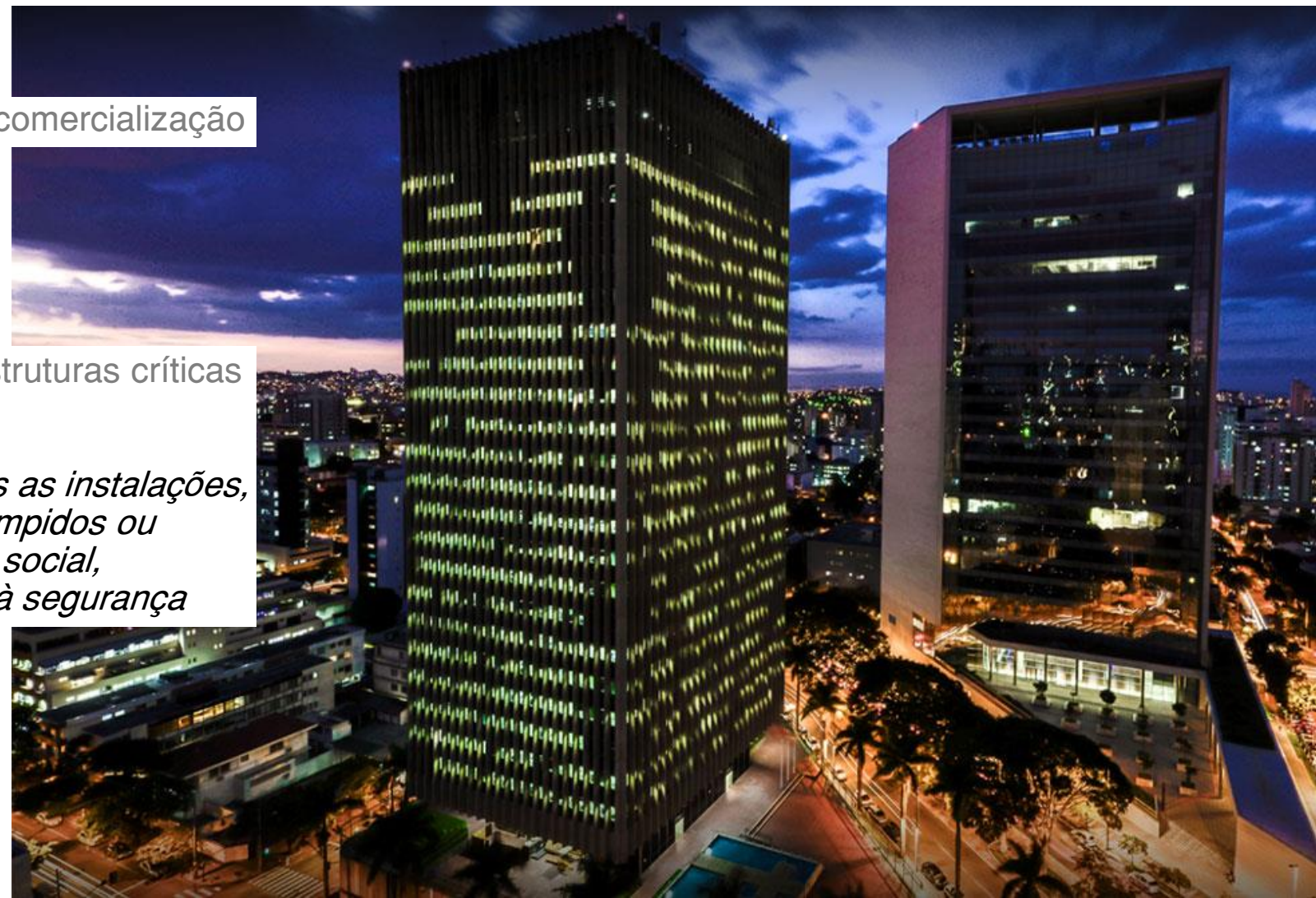
- **Cemig**

Geração, transmissão, distribuição e comercialização de energia

- **Setor elétrico**

Empresas consideradas como infraestruturas críticas pela Defesa Nacional

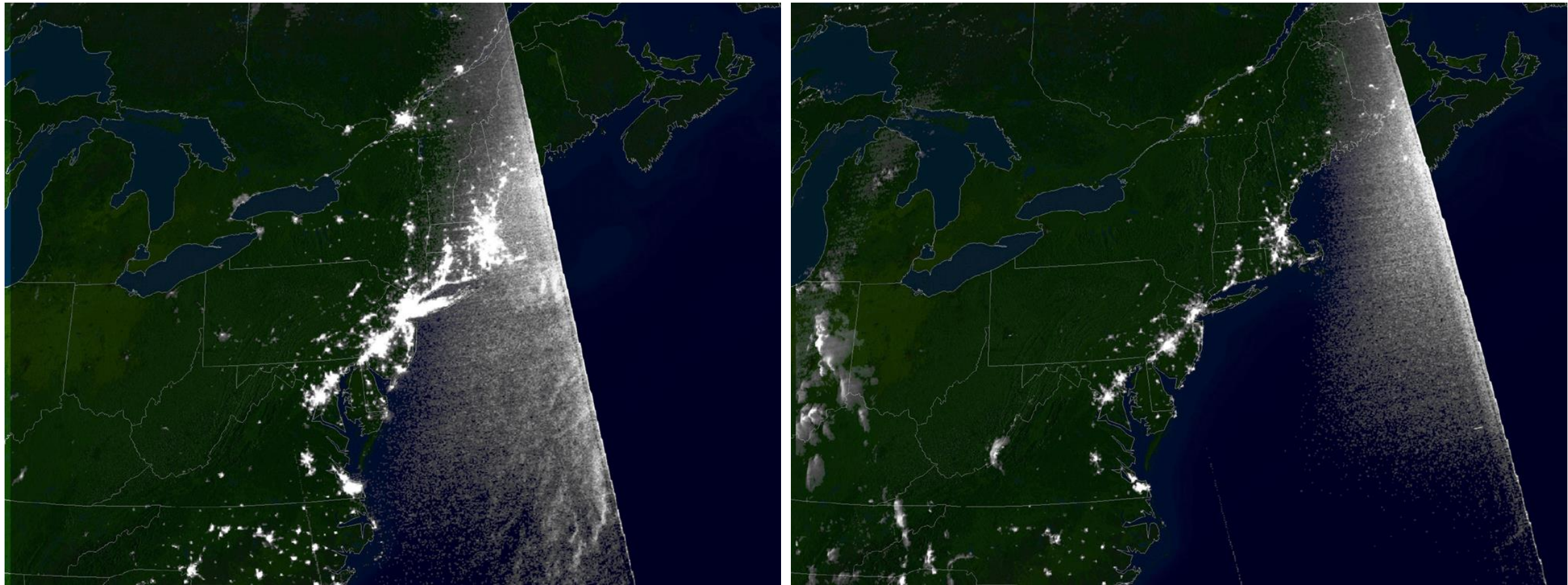
Consideram-se infraestruturas críticas as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. [1]



Contextualização 2/5

- *Blackout* no nordeste dos EUA em 2003 [2]

“Utilities are operating ever closer to the edge of the stability envelope using 1960s-era controls.” [3]



Contextualização 3/5

- *Blackout* no nordeste dos EUA em 2003 [2]

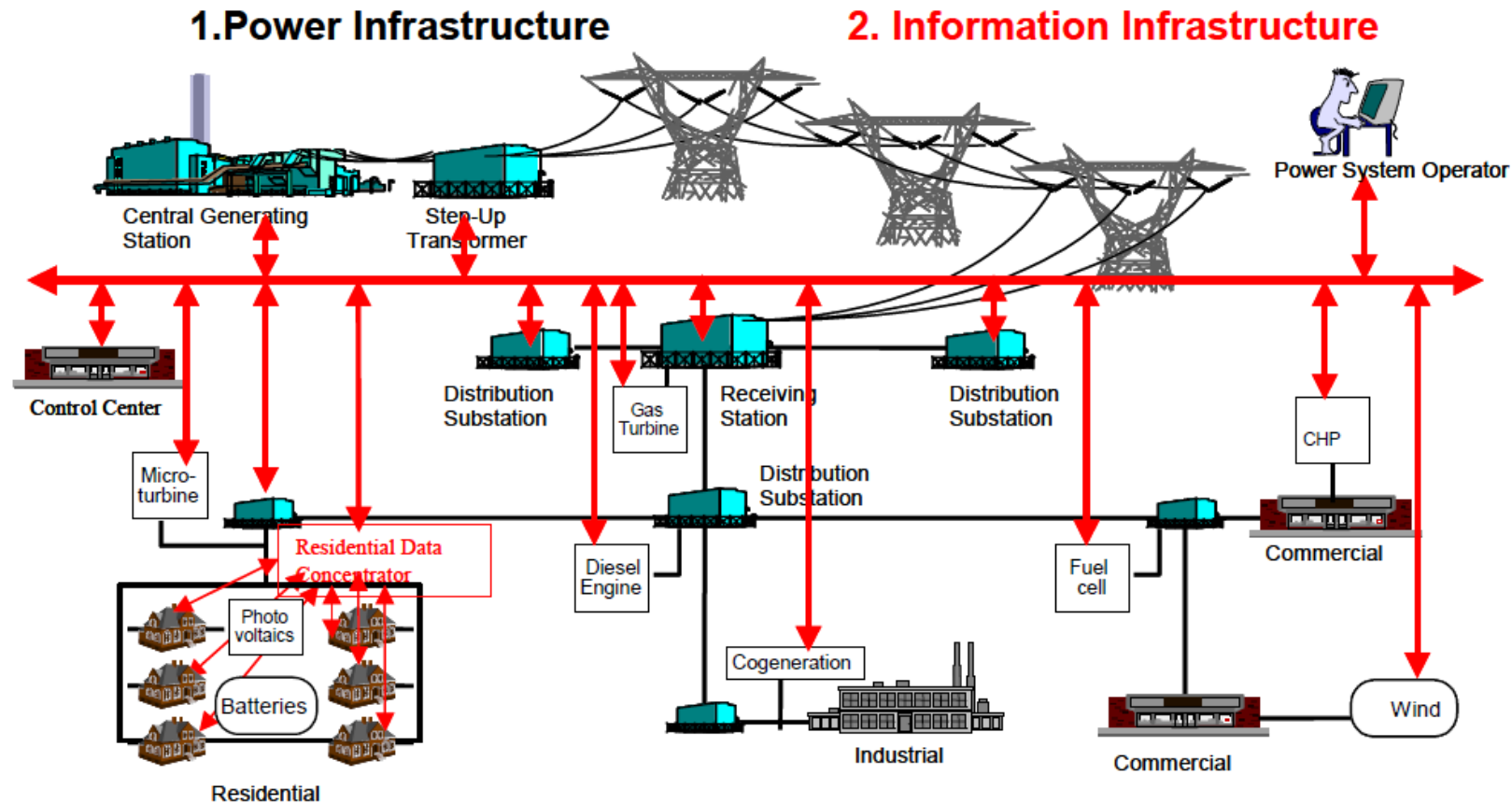


<https://parade.com/64694/iraphael/remembering-the-northeast-blackout-of-2003/>

Contextualização 4/5

- Sistema elétrico de nova geração

Intelligrid [4] (*smart grid*)



Contextualização 5/5

- **Segurança**

Adotar TI implica em trazer as vantagens e desvantagens das tecnologias [5] [6] [7] [8]



Analysis of the Cyber Attack on the Ukrainian Power Grid

Defense Use Case

KIM ZETTER SECURITY 03.03.16 07:00 AM

INSIDE THE CUNNING, UNPRECEDENTED HACK OF UKRAINE'S POWER GRID

Hackers breached US electric utilities: analysts

BY MORGAN CHALFANT - 08/02/18 06:00 AM EDT

SECURITY

DOE to vet grid's ability to reboot after a cyberattack

Blake Sobczak, E&E News reporter

Energywire: Friday, August 3, 2018

Rede Operativa de Dados 1/7

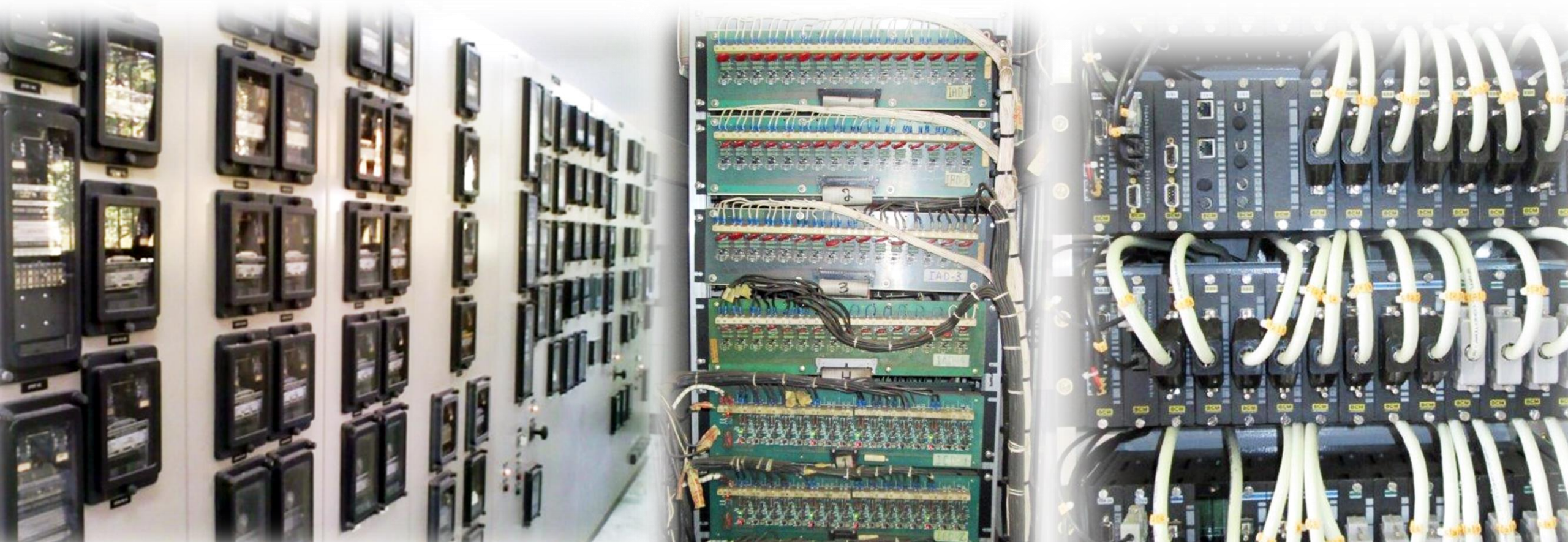
[9]

Category	Information Technology System	Industrial Control System
Risk Management Requirements	<p>Data confidentiality and integrity is paramount</p> <p>Fault tolerance is less important – momentary downtime is not a major risk</p> <p>Major risk impact is delay of business operations</p>	<p>Human safety is paramount, followed by protection of the process</p> <p>Fault tolerance is essential, even momentary downtime may not be acceptable</p> <p>Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production</p>
Component Lifetime	Lifetime on the order of 3-5 years	Lifetime on the order of 15-20 years
Change Management	Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OSs that are no longer supported

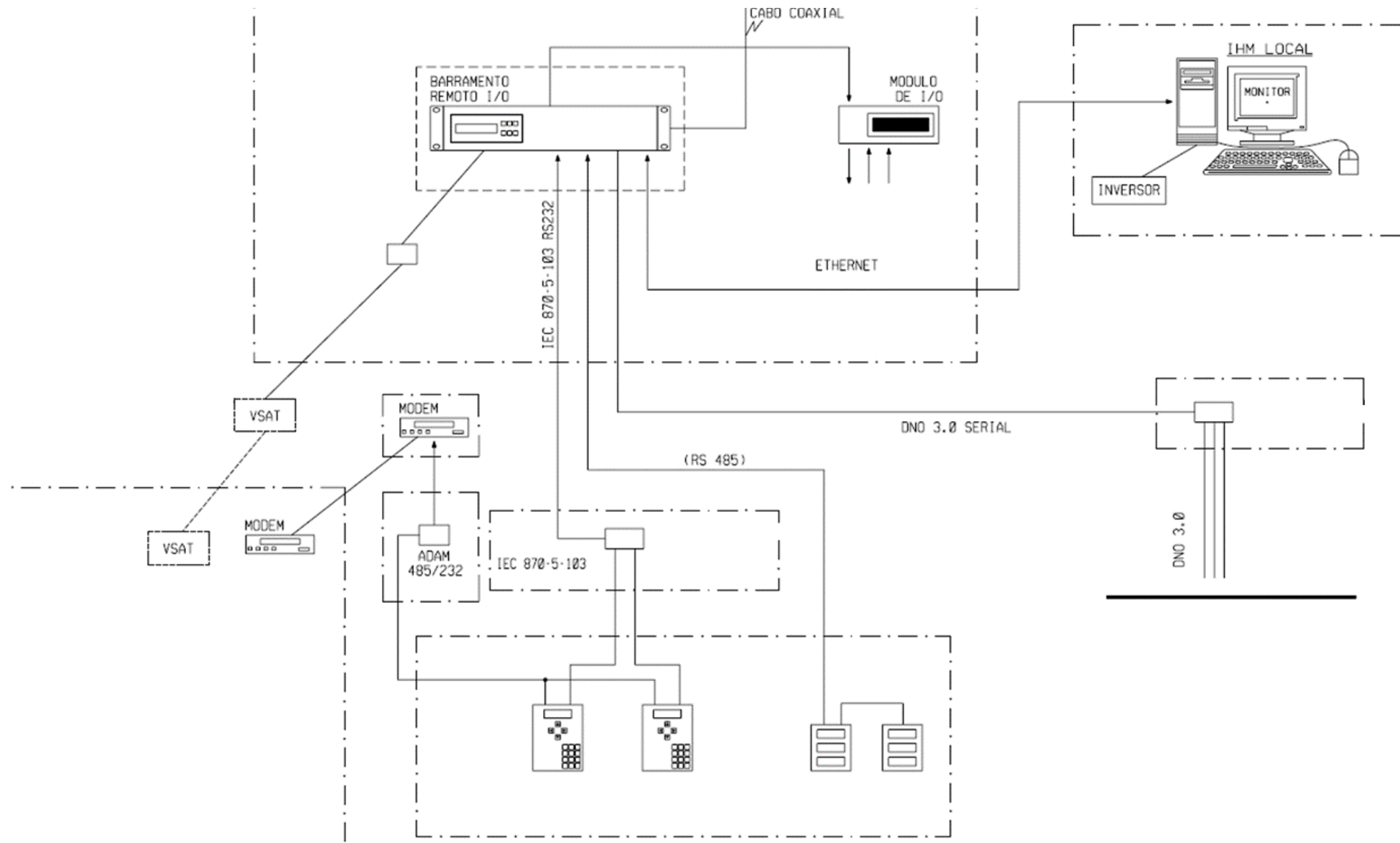
Rede Operativa de Dados 2/7

- Equipamentos analógicos

Comunicação serial, links dedicados, rede segregada, muita fiação



Rede Operativa de Dados 3/7

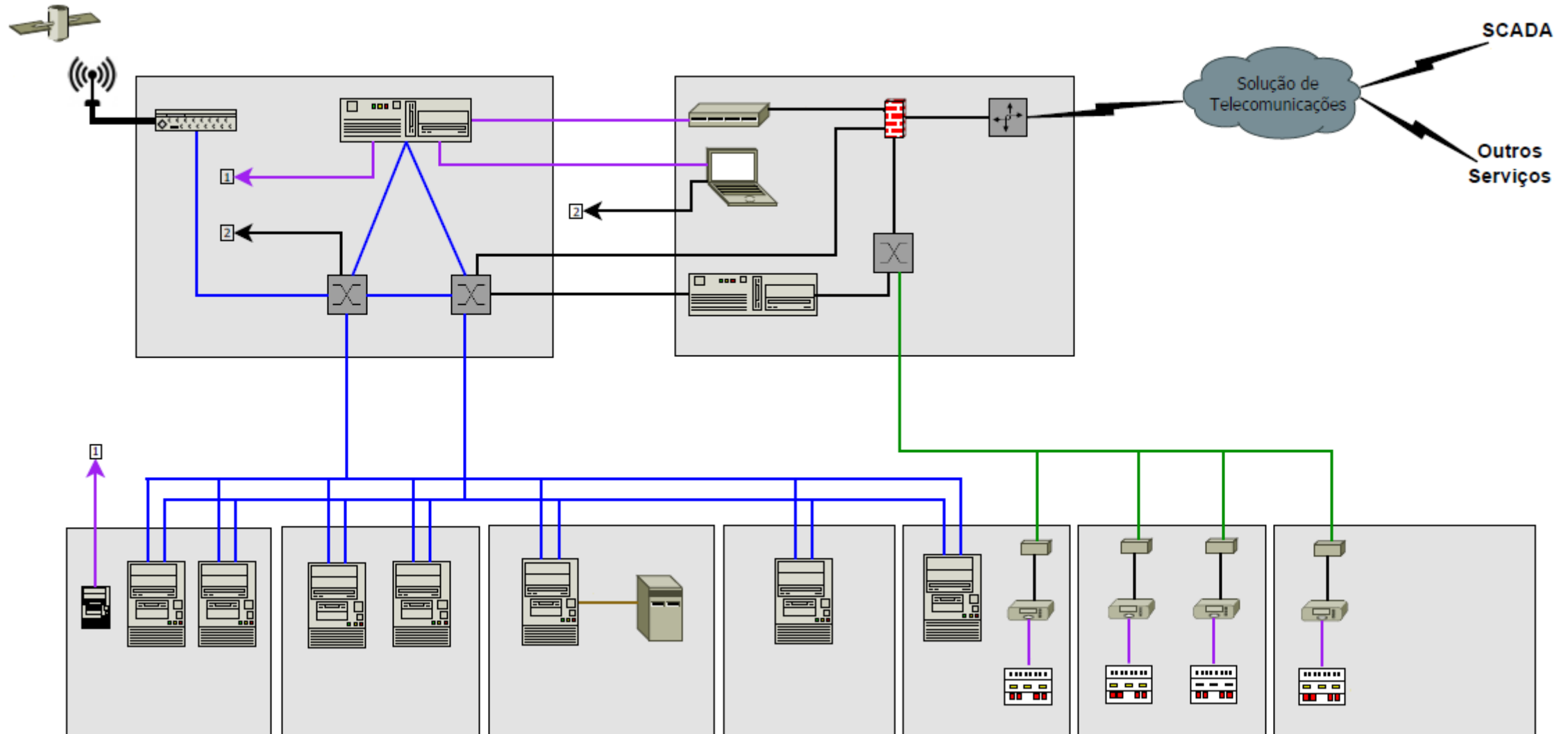


Rede Operativa de Dados 4/7

- Equipamentos digitais
Comunicação via ethernet, links dedicados, redes segregadas?

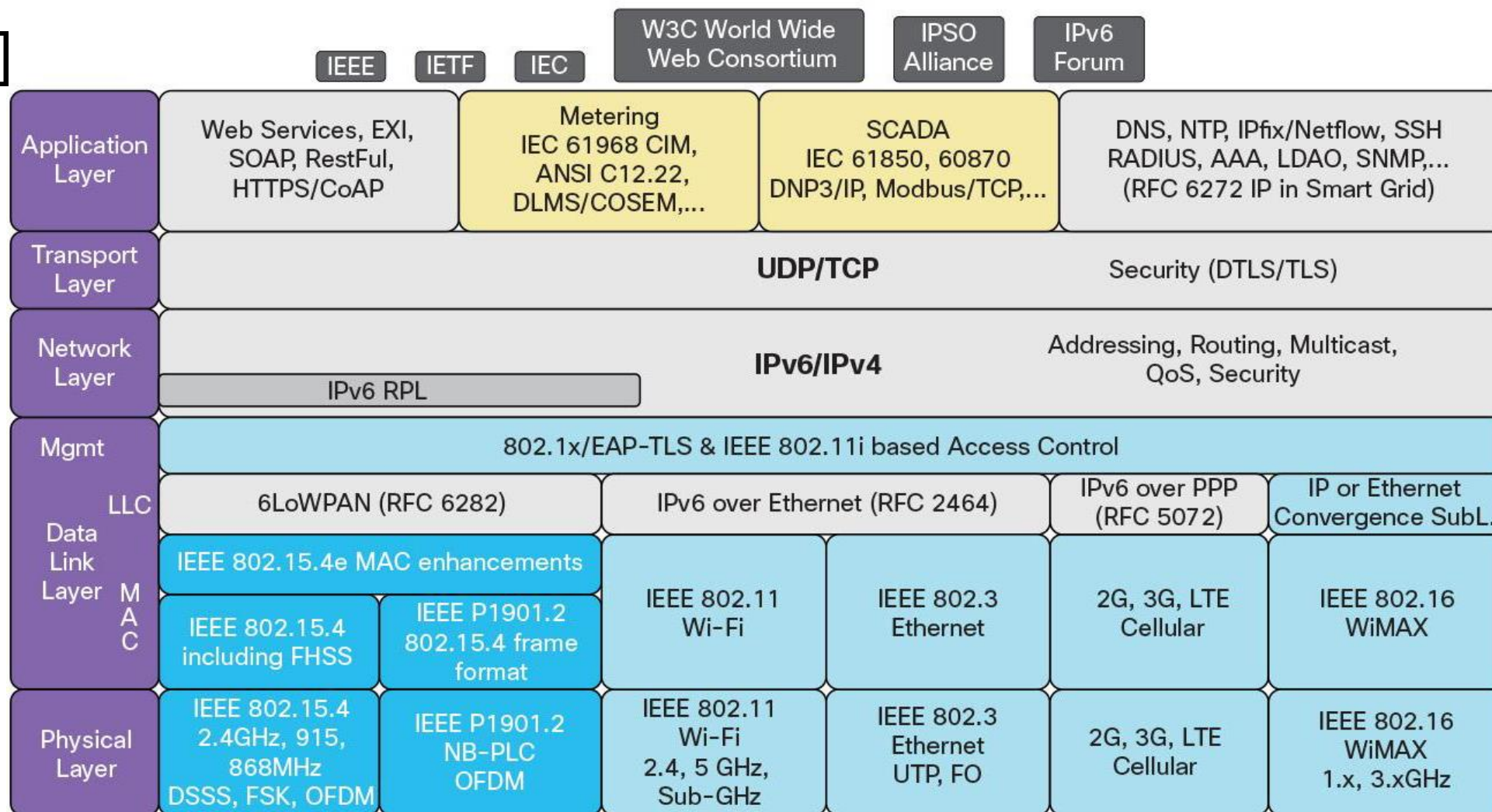


Rede Operativa de Dados 5/7

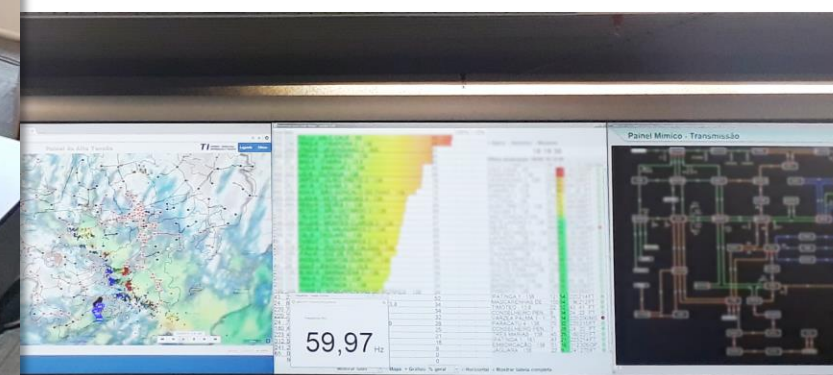


Rede Operativa de Dados 6/7

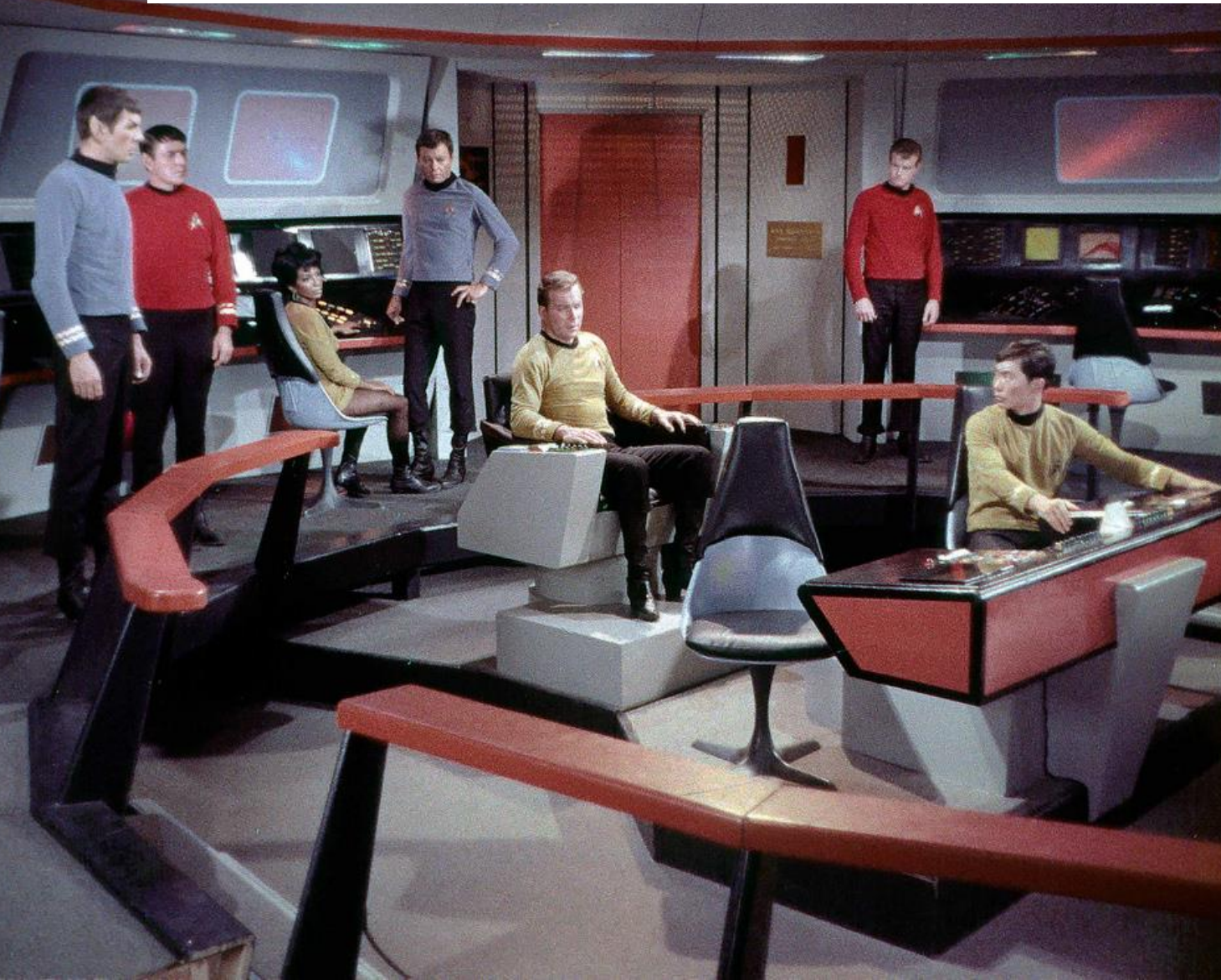
[10]



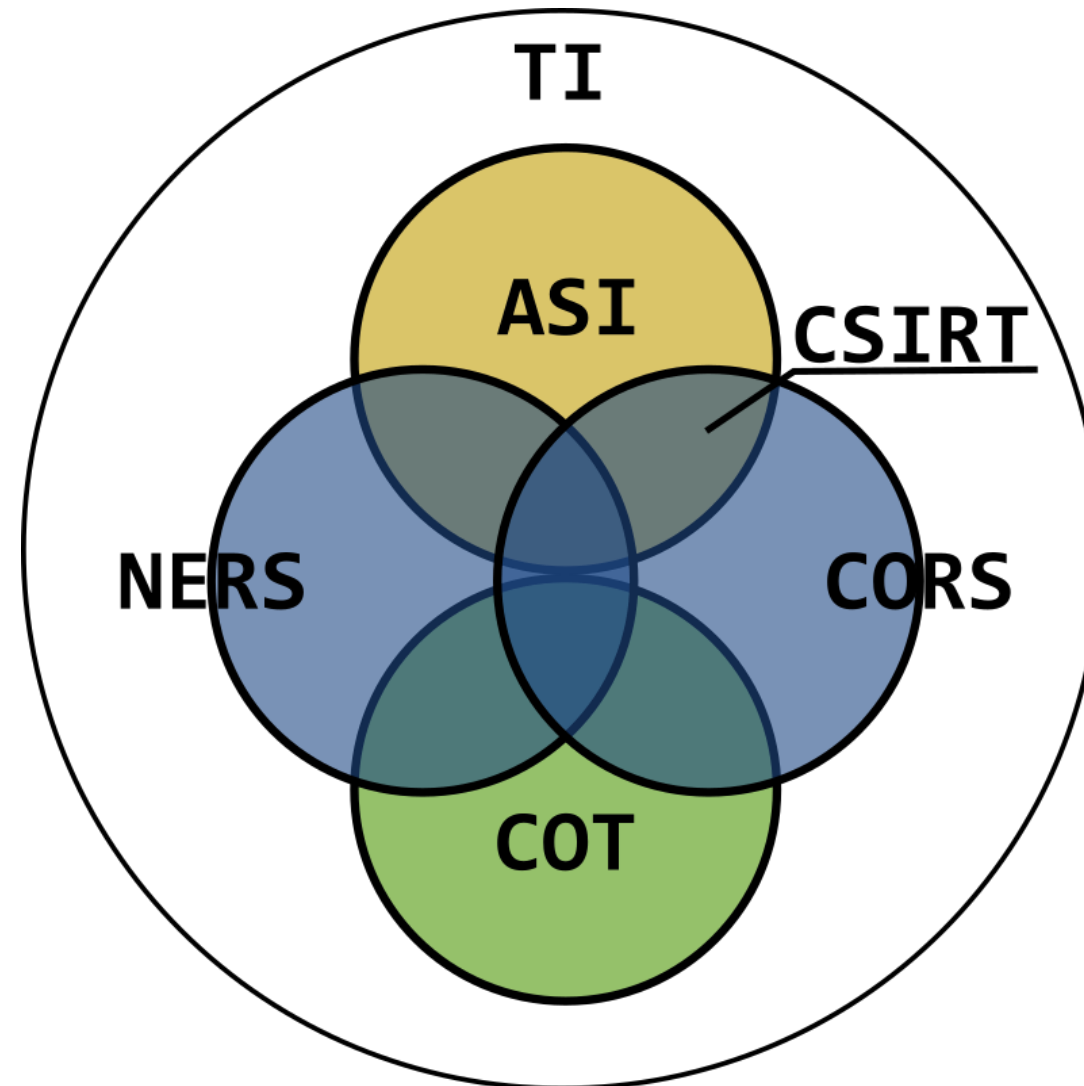
Rede Operativa de Dados 7/7



Rede Operativa de Dados 8/7 (Bônus)



Mecanismos de Segurança 1/9



Mecanismos de Segurança 2/9



Cyber Security Incident Response Team Cemig

Início em abril de 2014

Modelo centralizado (ASI e CORS)

Funcionamento em 24x7

Autonomia compartilhada

<https://www.cert.br/csirts/brasil/#csirt-cemig>

Parque (valores aproximados)

- 3000 ativos (rede + segurança)
 - Firewalls
 - IPS
 - SIEM
 - Proxies
 - Antispam
 - Antivírus
 - Honeypot
- 8000 clientes de antivírus
- 1800 VPNs
- 300 links
- 280 localidades
- 14 controles SOX (diretos e indiretos)
- 800 incidentes / mês

Mecanismos de Segurança 3/9

- **Gestão dos Incidentes de Segurança**

Baseado no modelo PDCERF

Sistematização via software

Taxonomia baseada na ENISA

Em curso: melhorias nos registros e análise



Mecanismos de Segurança 4/9

HP Service Manager

Meus Afazeres Novo - Incidente

Cancelar Salvar Salvar e Sair Aplicar Gabarito Mais Selecionar seção...

Incidente

Titulo: *

Descrição: *

ID do Incidente: IM1485254 Categoria: incidente de segurança

Status: Aberto Subcategoria:

Fase: Registro em Log Área:

Serviço Afetado Primário: * Impacto: * 4 - Usuário

IC Afetado: Urgência: * 4 - Baixa

O IC está operacional (nenhuma interrupção) Origem:

Hora de Início da Interrupção: Pessoa de Contato:

Hora de Término da Interrupção: Destinatário do Serviço:

Grupo Designado: Localização:

Designado:

Solução:

Fluxo de Trabalho

Mecanismos de Segurança 5/9

- Monitoramento de Segurança

The screenshot shows a news feed interface with a search bar at the top left and navigation options at the top right. The feed contains eight article cards, each with a thumbnail image, a title, and a source. The articles are:

- Hanging Up on Mobile in the Name of Security** (Krebs on Security, 4h)
- 'China's MIT' Linked to Espionage Campaign Against Alaska, Economic Partners** (Threatpost, 4h)
- Google Expands Bug Bounty Program to Battle Abuse Methods** (Threatpost, 3h)
- Chrome Bug Allowed Hackers to Find Out Everything Facebook Knows About You** (The Hacker News, 3h)
- Open MQTT Servers Raise Physical Threats in Smart Homes** (Threatpost, 4h)
- Transatlantic Cable podcast, episode 50** (Kaspersky, 4h)
- Australians who won't unlock their phones could face 10 years in jail** (Naked Security, 5h)
- Sacramento admits to tracking welfare recipients' license plates** (Naked Security, 5h)

Mecanismos de Segurança 6/9

IBM QRadar Security Intelligence
Help Messages 15 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Admin
System Time: 3:01 PM

Show Dashboard: Monitoramento - CORS New Dashboard Rename Dashboard Delete Dashboard Add Item... Next Refresh: 00:00:50

Event Rate (EPS) (Count) (Events per Second Raw - Average 1 Min)

Reset Zoom 8/16/18, 2:02 PM - 8/16/18, 3:02 PM

View in Log Activity

CORS.C03 (csip) (time series)

Reset Zoom 8/16/18, 2:02 PM - 8/16/18, 3:02 PM

View in Network Activity

Top IDS/IPS Alert by Country/Region (Count) (Source IP)

Reset Zoom 8/16/18, 2:02 PM - 8/16/18, 3:02 PM

View in Log Activity

Flow Rate (FPS) (Count) (Flows per Second - Peak 1 Min)

Reset Zoom 8/16/18, 2:02 PM - 8/16/18, 3:02 PM

View in Log Activity

Firewall Deny by SRC IP (Event Count)

Reset Zoom 8/16/18, 2:02 PM - 8/16/18, 3:02 PM

View in Log Activity

Offenses by Rule Name (Event Count)

Reset Zoom 8/16/18 2:01 PM - 8/16/18 3:01 PM

View in Log Activity

System Summary

Current Flows Per Second	0
Flows (Past 24 Hours)	64.5K
Current Events Per Second	4.4K
New Events (Past 24 Hours)	250.3M

Firewall Deny by DST IP (Event Count)

Reset Zoom 8/16/18, 2:02 PM - 8/16/18, 3:02 PM

View in Log Activity

Offenses by Source IP (Event Count)

Reset Zoom 8/16/18, 2:02 PM - 8/16/18, 3:02 PM

View in Log Activity

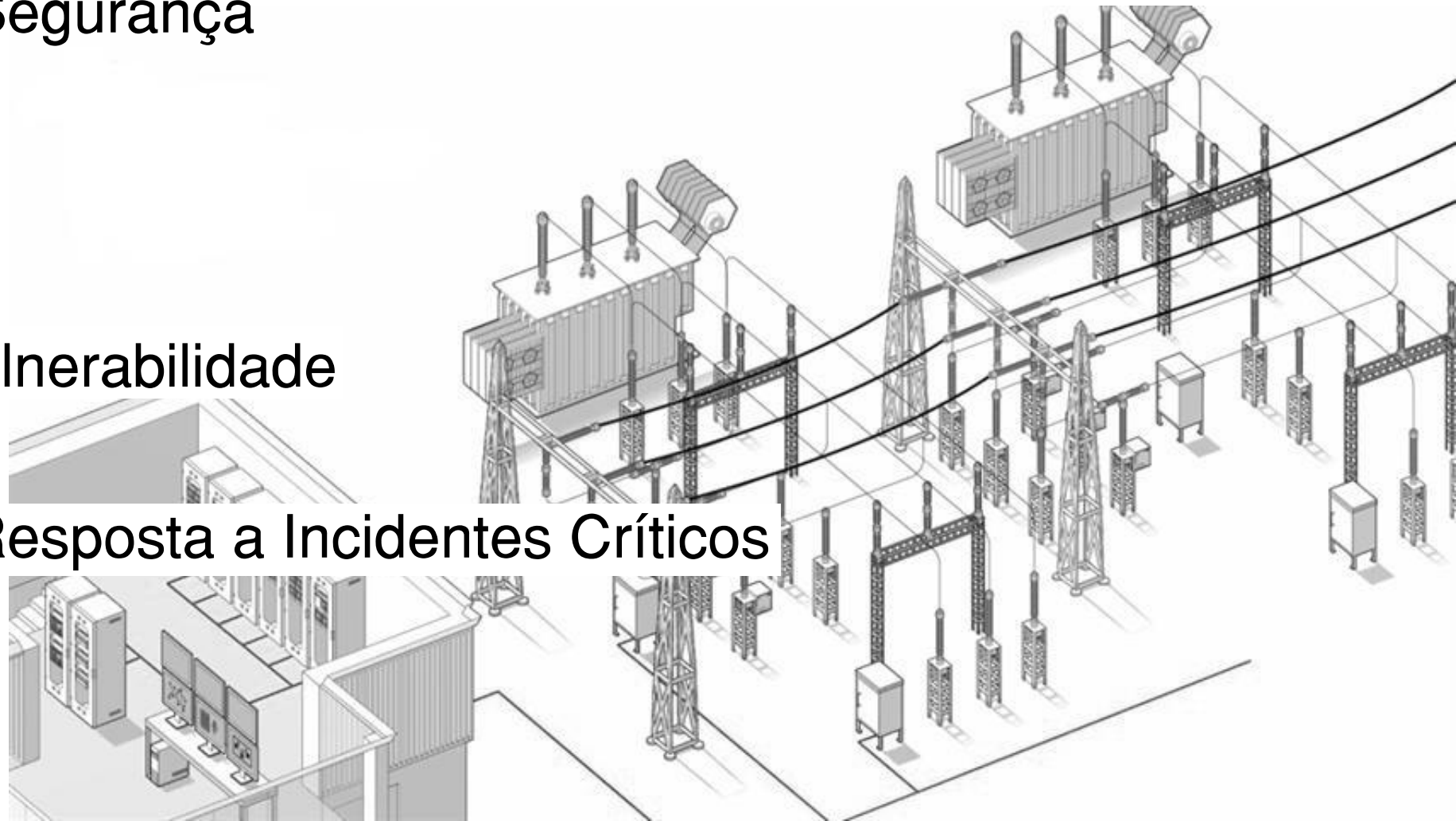
Mecanismos de Segurança 7/9

- Controles de Segurança

- Acessos ao honeypot
 - Análise do proxy
 - Verificação de *backups*
 - Controle de SPAM
 - Auditoria de usuários

- Análises de vulnerabilidade

- Protocolo de Resposta a Incidentes Críticos



Mecanismos de Segurança 8/9

- **Projetos**

- Firewall operativo

- Novo sistema SCADA

- Firewalls para usinas e subestações

- Honeypot SCADA [11]



Mecanismos de Segurança 9/9

- Grupo de Trabalho de Segurança Cibernética

Atendimento ao ONS, procedimento de rede 10, submódulo 10.14

Objetivos:

- criar e homologar controles de segurança cibernética,
- criar planos de contingência cibernética para o COS e
- criar a Política de Segurança Cibernética.



Considerações Finais 1/3

- Tratamento holístico da segurança
- Mais interações com outros CSIRTs



Considerações Finais 2/3

- **Rede Operativa**

Mais alinhamento entre TI e engenharia (TA?, TO?)
Conjunto de sub redes que precisam ser segregadas



Considerações Finais 3/3

- Capacitação
- Melhoria contínua



Obrigado!



Cyber Security Incident Response Team

+55 (31) 3506-7480

abuse@cemig.com.br

266604*100

José Lopes de Oliveira Júnior

joselopes@cemig.com.br

Coordenador do Centro de Operações de Rede e Segurança

Coordenador do CSIRT Cemig

Agradecimentos

- Marisa Lages Murta

“Se vi mais longe, foi por estar sobre ombros de gigantes.”

– Sir Isaac Newton (1643-1727)

Referências

1. Portaria número 2 de 8 de fevereiro de 2008. Gabinete de Segurança Institucional da Presidência da República. 2008.
2. Final report on the August, 14, 2003 Blackout in the United States and Canada: Causes and recommendations. U.S.-Canada Power System Outage Task Force. <https://www3.epa.gov/region1/npdes/merrimackstation/pdfs/ar/AR-1165.pdf>. 2004.
3. Preventing blackouts. Amin, M. and Schewe, P. F. Scientific American. Ed. 296, p.60-67. http://massoud-amin.umn.edu/publications/SciAm_0507_pp60-67.pdf. 2007.
4. The Integrated Energy and Communications Systems Architecture. Volume I: User Guidelines and Recommendations. Hughes, J. Energy Power Research Institute (EPRI). 2004.
5. Analysis of the cyber attack on the Ukrainian power grid. Lee, R. M. et al. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf. 2016.
6. 'Crash Override': The malware that took down a power grid. Greenberg, A. Wired. <https://www.wired.com/story/crash-override-malware/>. 2017.
7. Hackers breached US electric utilities: analysts. Chalfant, M. The Hill. <http://thehill.com/policy/cybersecurity/399999-analysts-say-hackers-breached-us-electric-utilities>. 2018.
8. DOE to vet grid's ability to reboot after a cyberattack. Sobczak, B. E&E News. <https://www.eenews.net/stories/1060092675>. 2018.
9. NIST Special Publication 800-82: Guide to industrial control systems (ICS) security. Stouffer, K., Falco, J., Scarfone, K. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf>. 2011.
10. A standardized and flexible IPv6 architecture for field area networks: smart-grid last-mile infrastructure. Cisco. <https://www.cisco.com/c/en/us/products/collateral/routers/1000-series-connected-grid-routers/white-paper-c11-730860.html>. 2014.
11. Cybercriminals waste no time breaking into experimental honeypot designed to look like ICS environment. Barth, B. SC Magazine. <https://www.scmagazine.com/cybercriminals-waste-no-time-breaking-into-experimental-honeypot-designed-to-look-like-ics-environment/article/787021/>. 2018.