Segurança Cibernética, Desafios e Processos Aplicados à Redes de Automação de Subestações

Alisson Oliveira – Solution Architect Manager – Schneider Electric Brasil

III Encontro Técnico ISA São Paulo na Eletropaulo:
Gestão de Ativos de Automação

31 de agosto de 2018 - Barueri / SP

Segurança Cibernética, Desafios e Processos Aplicados à Redes de Automação de Subestações

Alisson Oliveira
alisson.oliveira@schneider-elecric.com

III Encontro Técnico
ISA São Paulo
na Eletropaulo

ISA Sao Paulo Section

Eletropaulo

Introdução

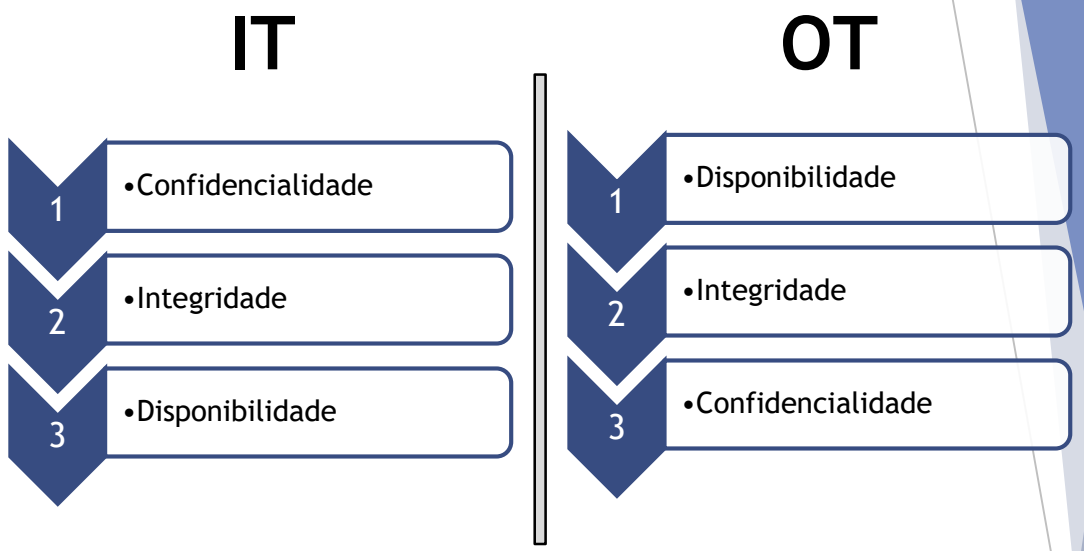
A evolução da tecnologia expôs os sistemas de controle a vulnerabilidades que antes afetavam apenas os computadores residenciais, de escritórios e de empresas. Embora o malware encontrado no mundo tenha sido desenvolvido para ataques em computadores domésticos, comerciais ou corporativos, os computadores das subestações, que empregam a mesma tecnologia, ficaram expostos a práticas de segurança internas negligentes, a prestadores de serviços externos com acesso aos sistemas e interfaces inadvertidamente acessíveis em rede.

Segurança cibernética – O que é?

- Aprimora a disponibilidade da rede nos seguintes quesitos:
  - Na proteção do sistema contra harkers
  - Na proteção do sistema contra erros
    - Intencionais
    - Não intencionais
  - Nos processos de operação e manutenção
- Segurança cibernética é um processo contínuo
  - A organização dos agentes do setor elétrico estão em constante mudanças
  - Novas vulnerabilidades estão surgindo dia a dia
  - O Sistema elétrico também está em constante mudança
  - Etc.

Segurança cibernética – conceitos

- CIA Tríade
  - Confidencialidade
    - Prevenir o uso não autorizado da informação
  - Integridade
    - O conteúdo da informação não foi modificado
  - Autenticação / Disponibilidade
    - Quem está autorizado para fazer o que?
    - Garante que a informação esteja disponível quando requerida



IT versus OT

Information technology versus Operation technology

IT

- Não se conhece a informação enviada e recebida(e-mail, documentos word, ppt, etc), que foi criada por mãos humanas e pode ser ou não confidencial
- Não há restrição quanto ao tempo de resposta, exemplo, um e-mail pode ser respondido hoje ou amanhã
- A autenticidade não é crítica
- A disponibilidade não é tão relevante, exemplo, se o servidor de e-mail não está disponível no momento, esperar para envia-lo pode não ser um problema.

OT

- Se conhece todas as informações, e tais informações foram criadas por “máquinas”, exemplo, arquivo IEC61850 SCL. Sabe-se quem está enviando e para quem.
- Os sistemas operam em tempo real, portanto, as mensagens não podem ser perdidas
- A autenticidade da informação é crítica, exemplo, deve-se ter certeza de que o comando é um disparo (trip).
- Um comando de disparo(trip) deve chegar ao seu destino

IT = Information technology (PC / servidores / switches / roteadores…)
OT = Operation technology (Reles de proteção / remotas …)

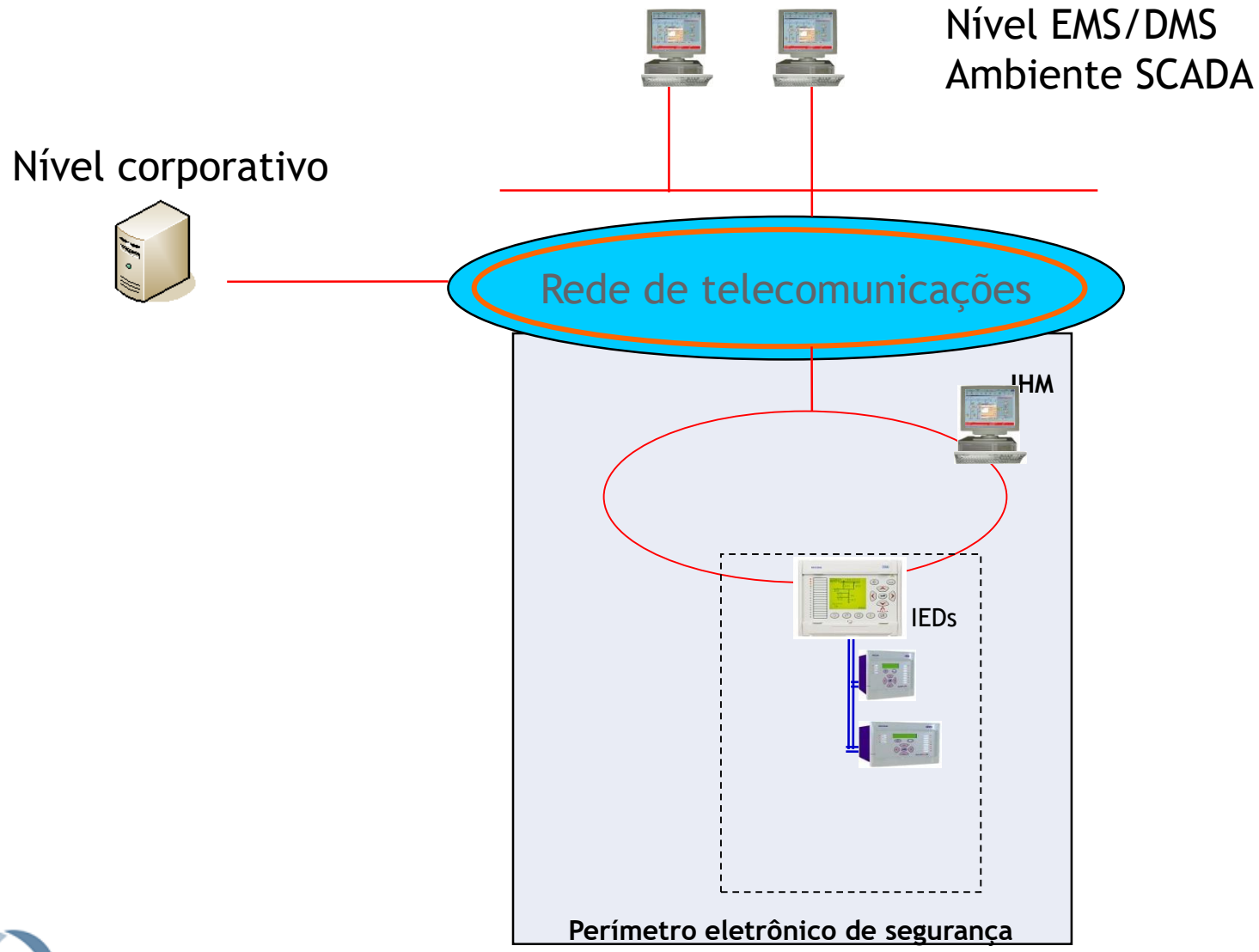
Segurança cibernética, em cinco passos

III Encontro Técnico
ISA São Paulo
na Eletropaulo

ISA Sao Paulo Section

Eletropaulo

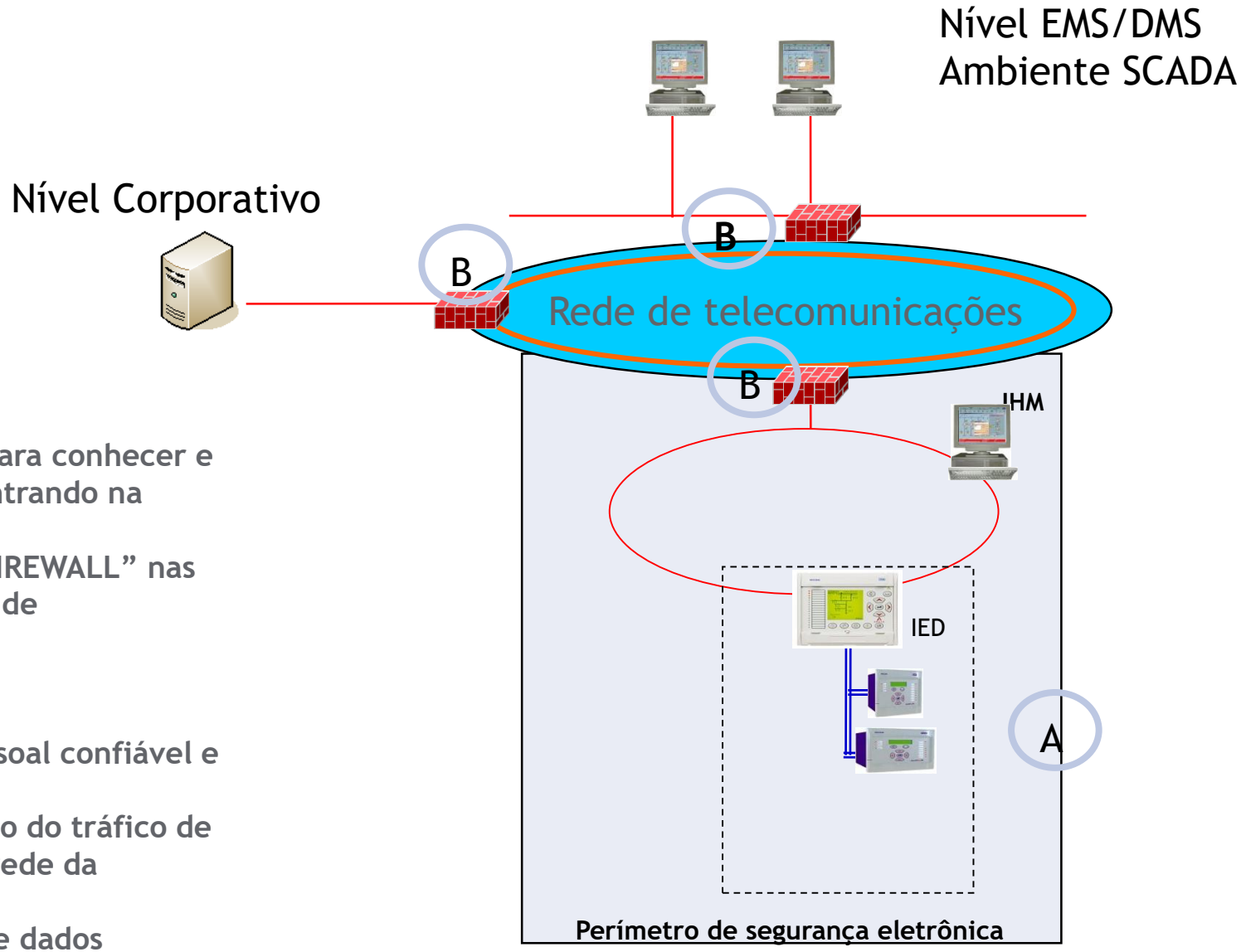
Arquitetura inicial



Passo 1

Proteção de acesso

Passo 1 – Proteção de Acesso



O que fazer?

- Em A, procedimento para conhecer e registrar quem está entrando na subestação.
- Em B, aplicação de “FIREWALL” nas interfaces com a rede de telecomunicações.

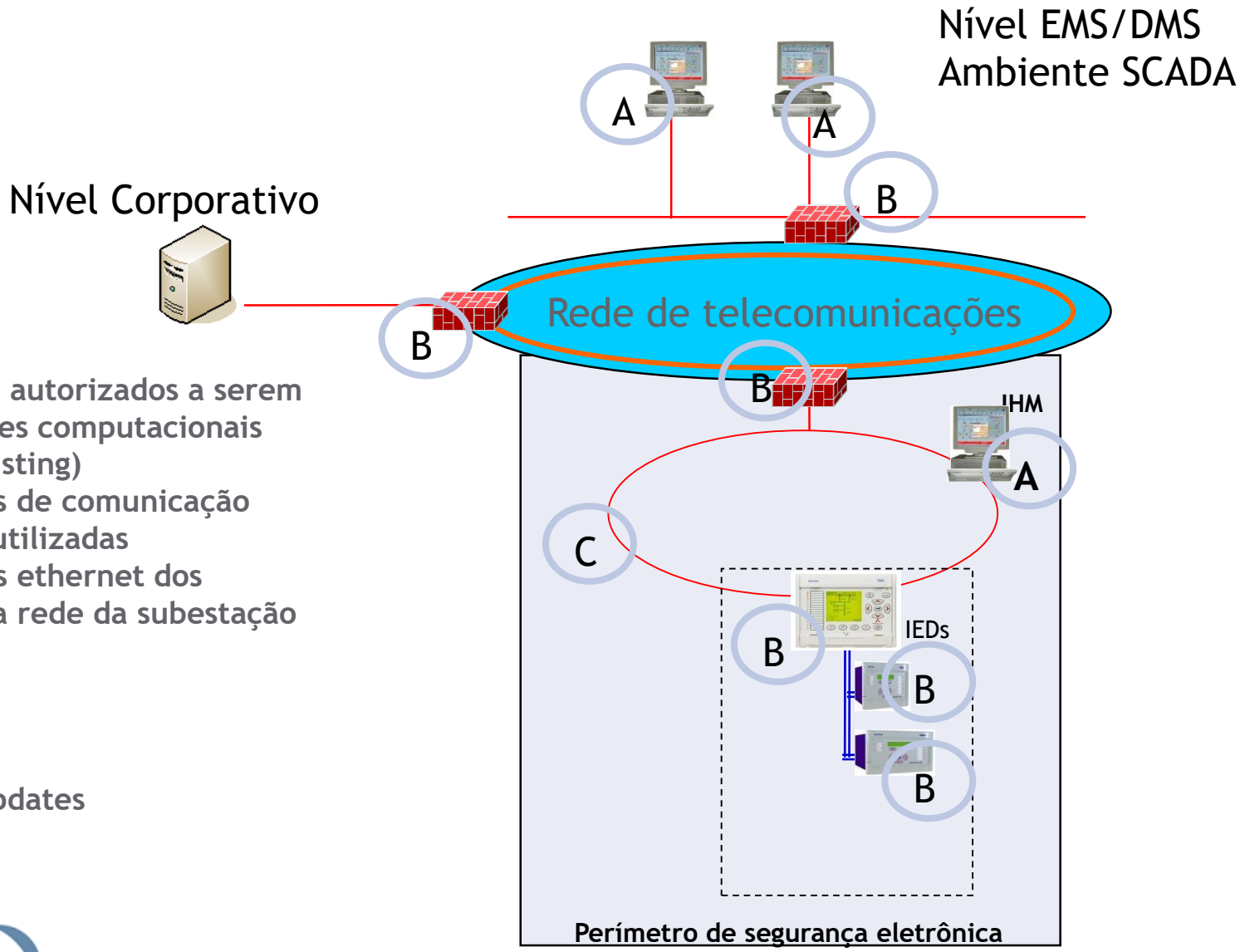
Benefícios:

- Acesso restrito de pessoal confiável e capacitado
- Registro e identificação do tráfico de dados que acessam a rede da subestação
- Bloqueio de tráficos de dados indesejáveis

Passo 2

Hardening

Passo 2 - Hardening



O que fazer?

- Em A, listar os softwares autorizados a serem executados nos servidores computacionais do sistema SPCS (Whitelisting)
- Em B, Bloquear as portas de comunicação que não estejam sendo utilizadas
- Em C, Bloquear as portas ethernet dos switches que compoem a rede da subestação

Benefícios:

- Proteção Stuxnet
- Proteção das portas USB
- Sem a necessidade de updates

Passo 3

Autenticação do usuário em nível de sistema

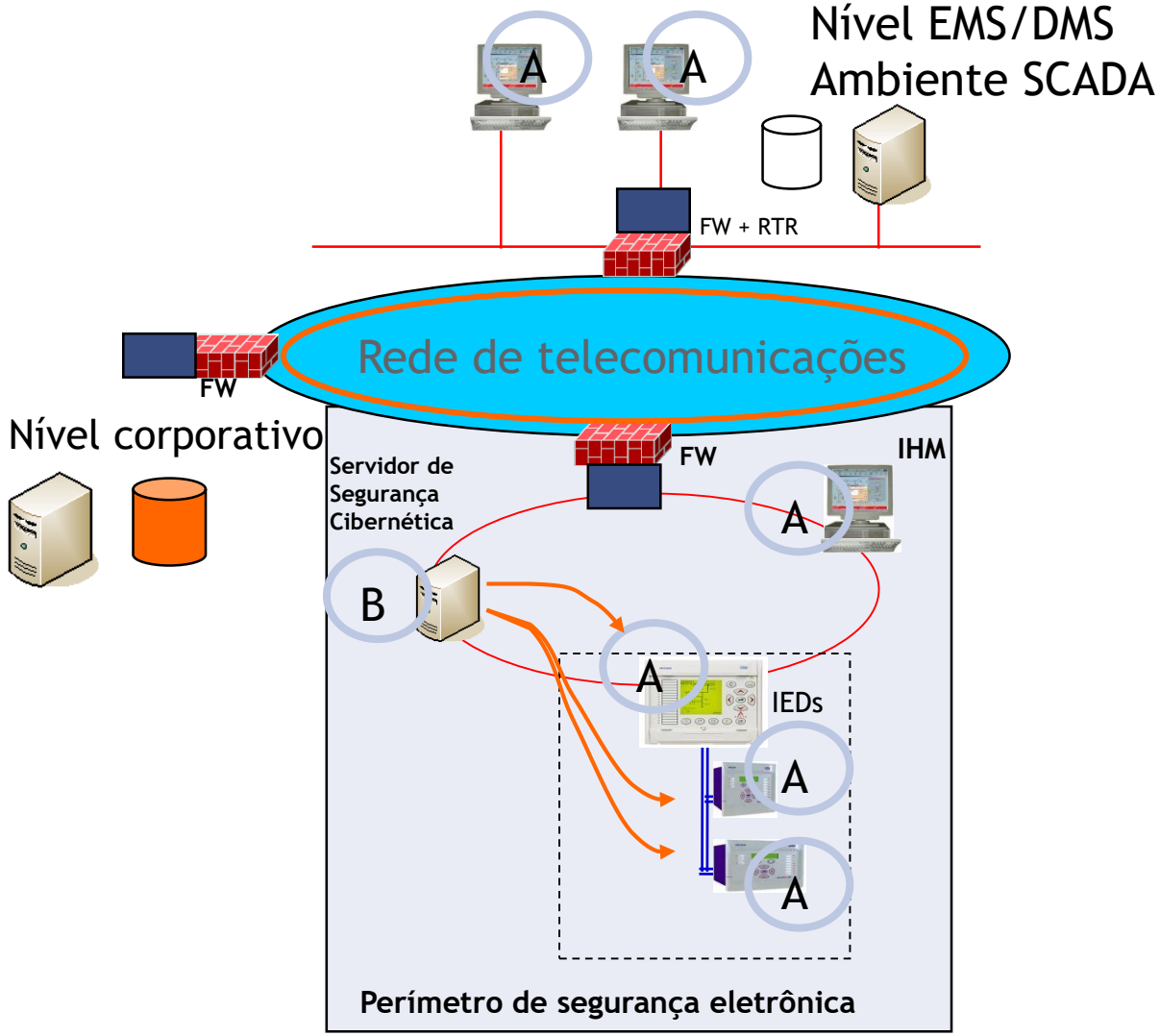
Passo 3 - Autenticação do usuário em nível de sistema

O que fazer?

- Em A, usuários fazem o login, sendo os cargos e privilégios já definidos
- Em B, Atribuir aos usuários os níveis de privilégio, levando em consideração as atividades de cada cargo no servidor da política de segurança.

Benefícios:

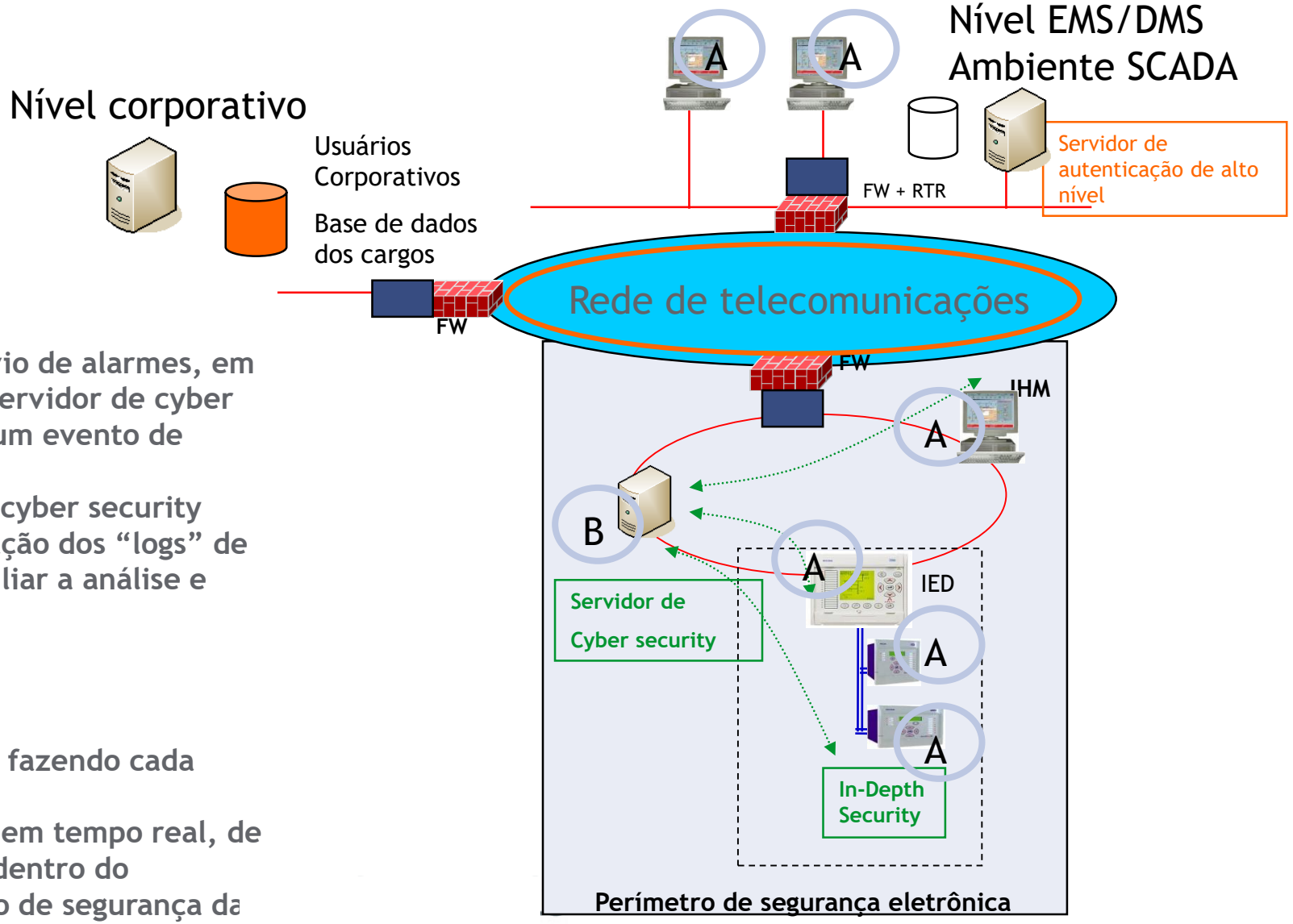
- Alinhamento operacional dos processos para a configuração dos IEDs
- Os usuários tem atribuições claras e que estão alinhadas com a política de segurança para a configuração dos IEDs
- Atualização em tempo real(O funcionário pode ter o acesso bloqueado em segundos)
- Solução normatizada pela norma 62351-8



Passo 4

Monitoramento e registro

Passo 4 - Monitoramento e registro



O que fazer?

- Em A, permite o envio de alarmes, em tempo real, para o servidor de cyber security quando algum evento de segurança ocorrer.
- Em B, o servidor de cyber security permite a centralização dos “logs” de alarmes visando faciliar a análise e auditorias.

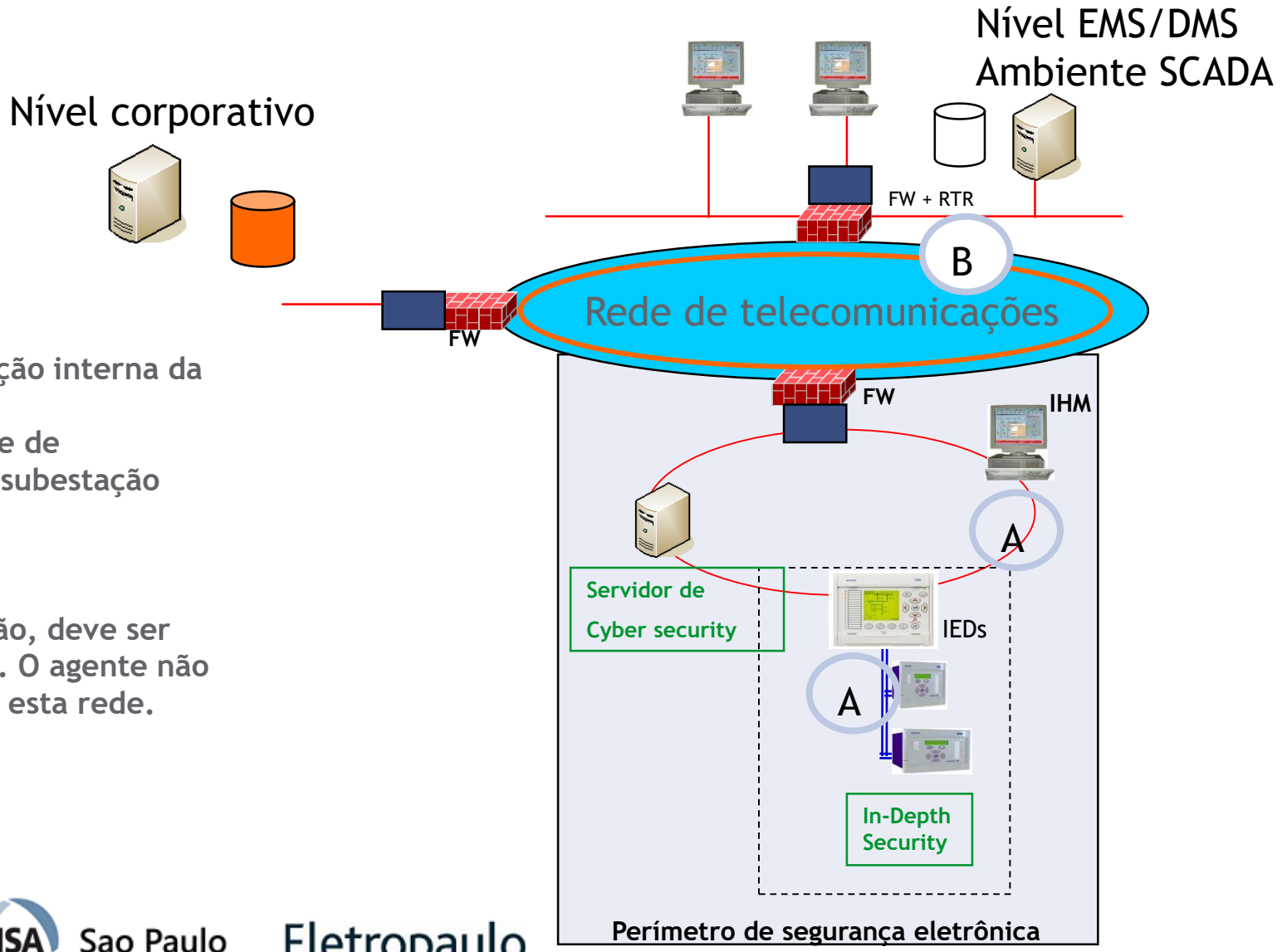
Benefícios:

- Entender quem está fazendo cada ação
- Facilita a obtenção, em tempo real, de todas as alterações dentro do perímetro eletrônico de segurança da subestação visando identificar anormalidades.

Passo 5

Comunicação segura

Passo 5 - Comunicação segura



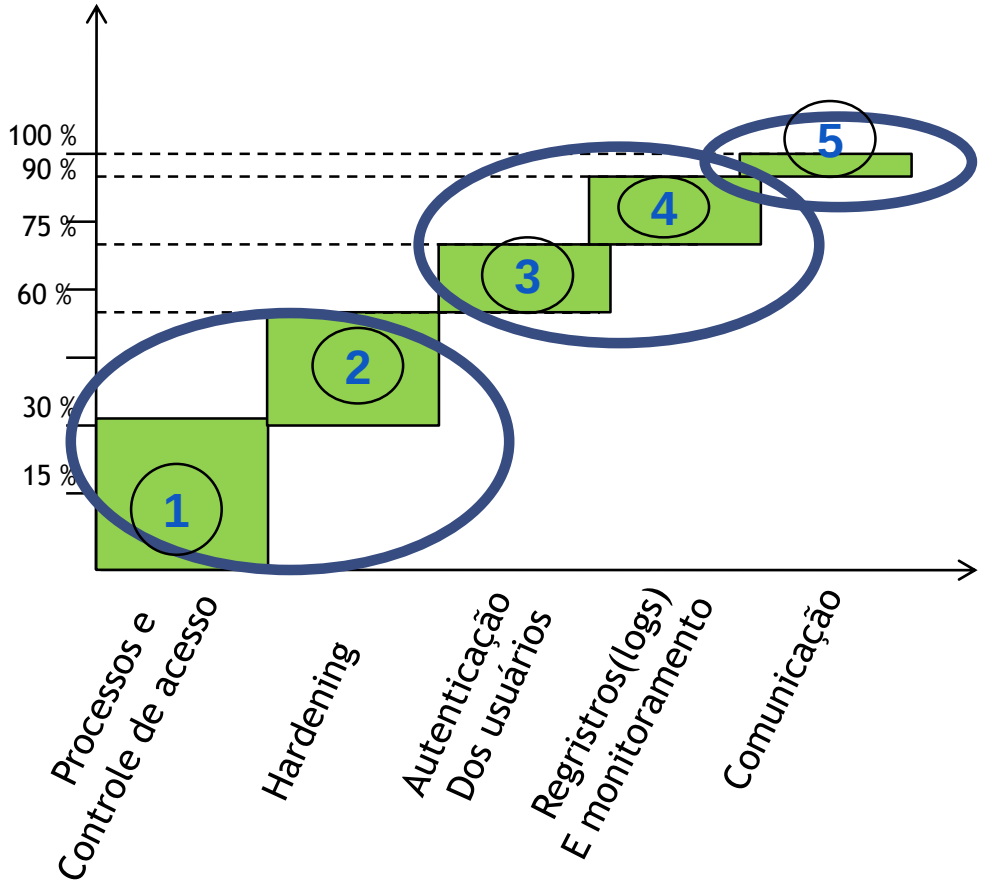
O que fazer?

- Em A: Rede de comunicação interna da subestação segura
- Em B: Garantir que a rede de comunicação externa da subestação seja segura

Benefícios:

- Rede externa a subestação, deve ser mandatoriamente segura. O agente não tem controle ou acesso a esta rede.

Contribuição dos 5 passos para o processo de segurança



III Encontro Técnico ISA São Paulo na Eletropaulo:
Gestão de Ativos de Automação

31 de agosto de 2018 - Barueri / SP

Perguntas

Alisson Oliveira
alisson.oliveira@schneider-electric.com

III Encontro Técnico ISA São Paulo na Eletropaulo

ISA Sao Paulo Section

Eletropaulo