

Projeto SAGA - Implantação de uma solução de segurança cibernética e aos ativos de automação.

Tema: Sistemas de Controle, Automação e Proteção

Autores: Gleidson Mendes Costa

Co-Autores: Rodolfo Queiroz, Tarciso Greco Coelho Silva, Giovane Malcher da Silva, Ivan Sousa Serra Junior, Rodrigo Rodrigues da Silva, José Elisandro Beserra Peixoto, Ítalo José Silva Mendes

Empresa: Equatorial Pará Distribuidora de Energia S.A

Resumo

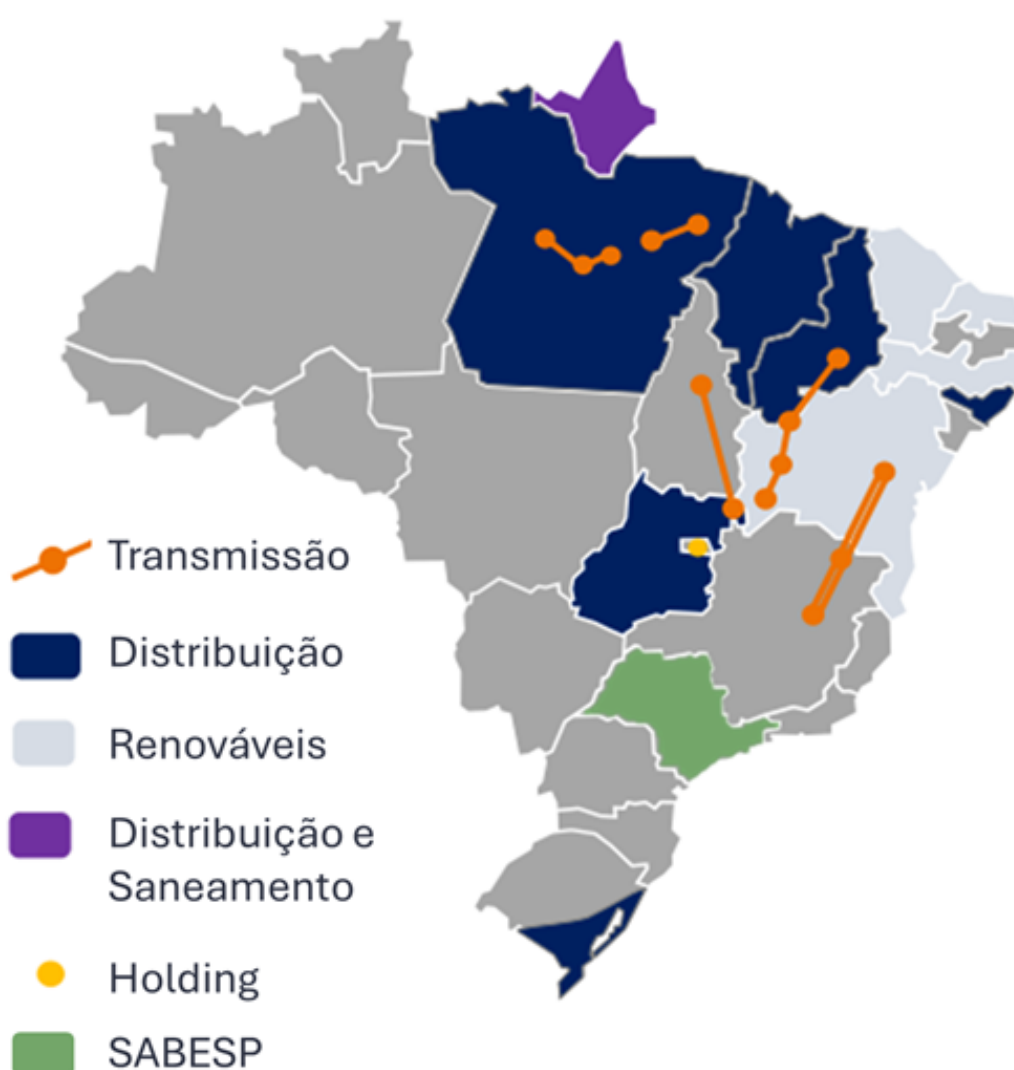
A digitalização das subestações de energia elétrica permite o monitoramento e controle em tempo real do sistema elétrico de uma distribuidora. Essa facilidade possibilita tomadas de decisão rápidas e ações de recomposição de circuitos, atendendo à regulamentação da ANEEL (Agência Nacional de Energia Elétrica). No entanto, essa conveniência pode introduzir vulnerabilidades ao setor devido à exposição das redes de computadores, tanto internas quanto externas. O Grupo Equatorial implantou o SAGA (Sistema de Acesso e Gerenciamento da Automação) para aumentar a segurança no acesso aos ativos de automação, a partir de funcionalidades de troca automática de credenciais e controle de acesso, garantindo o menor privilégio possível para as operações. O trabalho resultou na integração massiva inicial de 4 mil equipamentos, com funcionalidades de troca de senhas, coleta de eventos e oscilografias, persistência em banco de dados. Adicionalmente, a integração de novos equipamentos é uma atividade contínua, com o sistema atualmente contando com 4.700 equipamentos distribuídos pelas 7 distribuidoras do grupo. O sistema possui cerca de 40 mil arquivos de oscilografias e 580 mil eventos salvos, os quais não serão sobrescritos. O volume de equipamentos continua a crescer à medida que novos dispositivos são cadastrados na plataforma.

1. Introdução

A digitalização de subestações traz vantagens no monitoramento em tempo real do sistema elétrico, permitindo um tempo de resposta menor nos incidentes ou atividades envolvendo os equipamentos de proteção de campo. Entretanto, há desafios de mitigação das vulnerabilidades causadas por este tipo de solução. Devido aos equipamentos estarem conectados à uma rede de computadores, eles ficam suscetíveis a incidentes cibernéticos (ROSETO, 2023, p. 1-2).

Esta digitalização permite que os ativos de automação se comuniquem com os sistemas SCADA/EMS (Supervisory Control and Data Acquisition System / Energy Management System) e DCS (Distributed Control Systems), que tem como função o monitoramento e controle. Estes sistemas, inicialmente, possuíam foco na eficiência e confiabilidade dos dados em vez da segurança (HEINISCH, 2012, p. 1). Além disso, ainda é possível acessar os equipamentos remotamente ou local via rede para configuração ou coleta de dados por softwares proprietários.

O grupo Equatorial é uma holding multiserviço no Brasil, abrangendo os segmentos de transmissão, distribuição de energia elétrica, renováveis, geração distribuída, saneamento, comercialização de energia, telecomunicações e serviços. A Figura 1 apresenta a presença do grupo no Brasil, atuando de norte ao sul do país em 31% do território (EQUATORIAL, 2024). Tendo em vista a importância do grupo ao setor de energia do Brasil, aumento de ataques cibernéticos no Brasil e no mundo, e a regulamentação de cibersegurança pela ANEEL, há a necessidade de implantação de sistemas e ferramentas que permitam a continuidade da operacionalização do sistema em conjunto com garantia de segurança da rede.



Este trabalho tem como objetivo apresentar o processo de implantação do SAGA (Sistema de Acesso e Gerenciamento da Automação) para gerenciar o acesso de usuários aos ativos de automação com o mínimo de informações sobre os dados de rede e credenciais dos equipamentos e executar coleta de

oscilografias, eventos e configurações sem acesso direto ao dispositivo para o segmento de distribuição de energia do grupo Equatorial.

A implantação do sistema resultou na integração inicial massiva de mais de 4 mil equipamentos no sistema, além de possibilitar cargas individuais de mais de 700 dispositivos após a homologação do ambiente.

Este sistema não apenas atende à norma, garantindo a segurança por meio da troca automática de senhas dos relés de proteção e outros equipamentos, mas também aprimora a gestão dos ativos de automação do grupo, por meio da: coleta de eventos e de oscilografias, realização de backups, gestão de ativos e rastreabilidade de acessos e modificações.

2. Desenvolvimento

Antes da publicação da resolução, o time de Automação do grupo iniciou o estudo de tecnologias que atendessem às necessidades do grupo em relação à segurança dos equipamentos, gestão de ativos e coleta de dados dos dispositivos.

Inicialmente, buscou-se entender as necessidades do grupo e as soluções disponíveis no mercado que pudessem atender à demanda. O trabalho de (HEINISCH, 2012, p. 4-6) apresenta um estudo sobre os processos importantes para a automação e os pontos de vulnerabilidade, além de propor o desenvolvimento de uma ferramenta para gestão dessas proteções.

O suporte necessário aos Dispositivos Eletrônicos Inteligentes (IEDs) dentro e fora da subestação tinha que ser multifornecedor. As necessidades do grupo incluem dispositivos de mais de 10 fornecedores e mais de 33 modelos de dispositivos. Alguns dos principais fornecedores de dispositivos incluem: SEL, NOJA Power, Schneider/NULEC, ELTEK.

Escopo

No trabalho de (HEINISCH, 2012, p. 4-6), explica-se o conceito de perímetro de segurança e domínio de segurança. O perímetro de segurança consiste em um limite físico protegido que gerencia recursos de rede, computação e dispositivos físicos, assegurados por políticas e processos de segurança. Ele é responsável pela proteção de ativos, políticas, monitoramento e treinamento. Por sua vez, o domínio de segurança é um processo de automação que atravessa múltiplos perímetros, gerenciando recursos com políticas de segurança para funções específicas.

No presente trabalho, a segurança aplicada ocorre no nível do domínio de segurança associado à automação de dispositivos eletrônicos inteligentes (IEDs) da rede elétrica. Os processos são categorizados como:

- Oscilografias de IEDs;
- Eventos de IEDs;
- Configurações de IEDs;
- Proteções de IEDs;
- Acessos de IEDs.

Além desses processos, voltados ao domínio de segurança dos IEDs, há procedimentos adicionais para garantir acessibilidade, persistência, confiabilidade, rastreabilidade e segurança dos dados:

- Backup das configurações;
- Gestão de senhas;
- Registro de acesso e modificações;

- Armazenamento em banco de dados;
- Gestão de ativos;
- Acesso ao IED com informações mínimas.

Solução

O sistema SAGA é o sistema proposto como solução para as necessidades do grupo nas áreas de gestão de acesso, automatização de tarefas dos dispositivos e integração com múltiplos fornecedores. No trabalho de (LOUREIRO, 2024, p. 1-3), são apresentadas as funcionalidades do sistema para o caso de uso do grupo Equatorial:

- Configuração de perfis de usuários;
- Acesso mínimo a dados sensíveis dos equipamentos (como IP de acesso, porta de acesso, usuário e senha);
- Conexão com o IED aberta apenas durante a coleta de novos dados;
- Troca de senhas;
- Identificação de arquivos alterados em relação ao padrão;
- Agendamento de tarefas;
- Coleta e análise de eventos e oscilografias.
- Integração com múltiplos fornecedores e modelos

A solução se soma às políticas de segurança já existentes implementadas pelo time de TI do grupo na rede administrativa e operacional, atuando no nível de gestão de credenciais dos equipamentos. Ou seja, o sistema é responsável por armazenar os usuários e senhas de todos os ativos e realizar trocas sistematizadas com níveis de complexidade personalizados.

Dessa forma, mesmo que haja conectividade com os equipamentos, os acessos são impossibilitados devido à falta de conhecimento das credenciais de acesso. O conhecimento desses dados só é possível ao acessar o SAGA e ter privilégios suficientes. Mesmo assim, sempre que as credenciais são reveladas para a execução de uma atividade específica, elas podem ser substituídas logo em seguida.

Centralizando todos os acessos por meio desse sistema, ele rastreia quando um usuário acessa o sistema, acessa o ativo, realiza alguma atividade específica, revela a senha temporária (com privilégios específicos) ou realiza ajustes.

Apesar de não ser necessário o conhecimento das credenciais, esse fator não afeta as atividades de rotina das equipes, pois o usuário tem conhecimento sobre o equipamento, mas não sobre sua conectividade, sendo essa responsabilidade do SAGA. O usuário apenas precisa indicar qual equipamento deseja acessar ou qual tarefa deseja executar para o equipamento, e o SAGA entrega o resultado, tornando o processo de conexão totalmente transparente.

Implantação

No levantamento de risco dos processos de automação apresentado em (HEINISCH, 2012, p. 5-6), percebe-se que as atividades de automação são, em sua maioria, vitais e importantes. Dessa forma, o sistema precisa ser configurado para garantir alta disponibilidade. Uma falha na disponibilidade do sistema afetaria a atividade operacional do grupo.

A arquitetura base do sistema é composta por um Servidor de Usuários (SU), um Servidor de Dispositivos (SD) e um Servidor de Banco de Dados (SBD). Os clientes se conectam ao SU, e, a partir desse ambiente, utilizam uma conexão HTTP com o servidor SD.

Assim, um usuário que se conecta ao sistema por meio do SU somente conseguirá acessar os equipamentos através da aplicação web, que estabelece conexão com o servidor SD. Isso ocorre porque o servidor SU não possui conectividade direta com a rede de TO. A Figura 2 representa esta conexão.

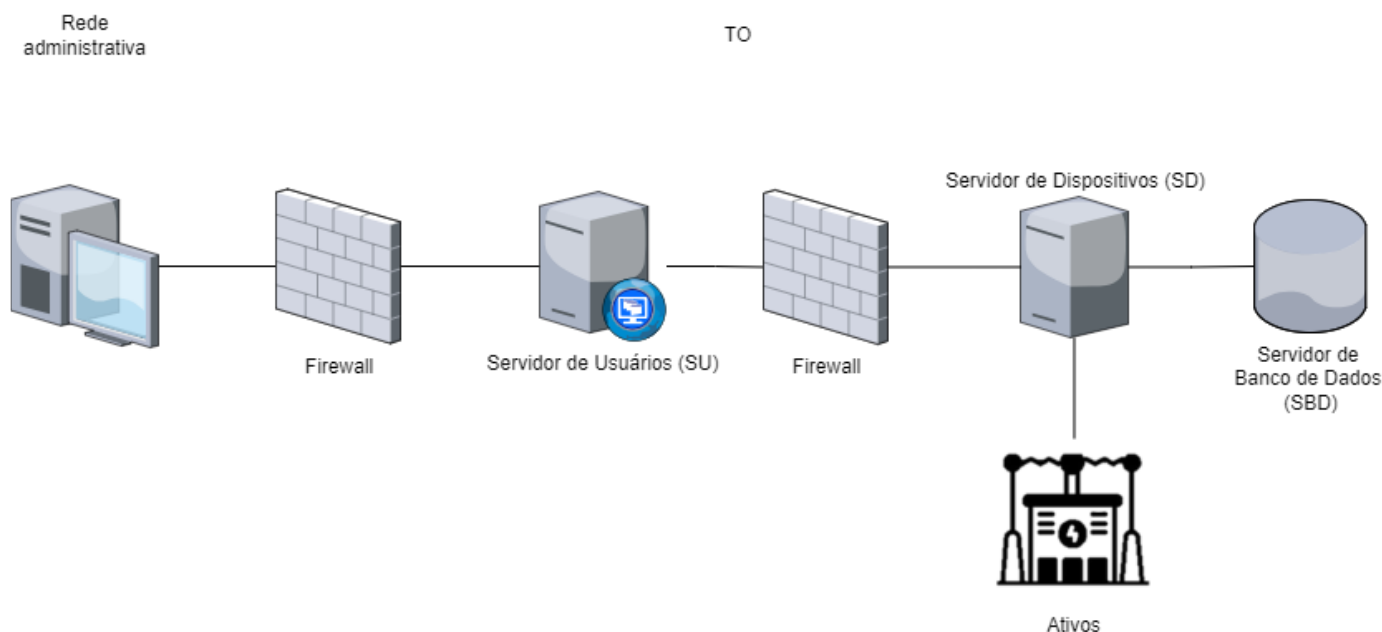


Figura 2 - Arquitetura mínima para implantação da solução SAGA. Fonte: Autor.

A alta disponibilidade é realizada pela redundância de servidores de SU, SD e SBD. Assim, quanto maior a quantidade de servidores disponíveis para essas funções, menor será a probabilidade de perda total do ambiente.

Durante o processo de implantação, houve 5 fases principais: Ambiente de homologação, Ambiente de produção e conectividade, Homologação de equipamentos, Gestão de credenciais e Go-live (ativação do sistema para todos os usuários).

Ambiente de Homologação O ambiente de homologação possui a arquitetura mínima que permite o funcionamento em menor escala do que rodará em produção, como mostrado na Figura 2. Assim, a primeira etapa foi responsável pela disponibilização de uma arquitetura viável, instalação do serviço PSC e execução de testes de sistema e equipamentos. Este ambiente foi dimensionado para conectar-se a poucos equipamentos ao mesmo tempo, além da liberação de regras de rede mínima que permitissem conexão direta com as redes de laboratório do Grupo Equatorial, (LOUREIRO, 2024, p. 1-3).

O ambiente de homologação tem como objetivo os testes dos desenvolvimentos de novos drivers de conexão com os equipamentos e do desenvolvimento de novas funcionalidades e versões do sistema. Uma vez testadas, as atualizações são aplicadas em produção.

Ambiente de Produção e Conectividade O ambiente de produção possui uma arquitetura de alta disponibilidade, onde cada servidor da arquitetura mínima, Figura 2, foi duplicado. Além disso, o ambiente de produção está preparado para a execução de backups diários dos sistemas operacionais e dos bancos de dados, monitoramento de recursos computacionais dos servidores, sistema de balanceamento de carga de usuários e serviço de e-mail.

Após a disponibilização do ambiente produtivo, iniciou-se a atividade de conexão do ambiente com a rede de TO. Inicialmente, foram levantadas todas as redes de TO, por meio do controle existente no SCADA e no controle de TI. Todas as redes foram liberadas gradualmente após elas serem estudadas e avaliadas em relação a protocolos de rede, tipo de tráfego, complexidade da rede, criticidade para o negócio, latência,

disponibilidade e regulação. Elas foram testadas por meio de programas de varredura pelo protocolo TCP/IP, assim como utilizando as portas específicas dos equipamentos de TO, pelo próprio SAGA.

O tráfego gerado por essas aplicações está sendo tratado e monitorado de acordo com suas respectivas especificidades através de regras de firewall ou políticas de firewall (conjunto de regras e normas elaboradas para controlar o tráfego de rede entre a rede interna de uma organização e a Internet). O processo de criação e execução de regras de firewall seguiu as diretrizes de gestão de mudanças do ITIL (Information Technology Infrastructure Library), um conjunto de boas práticas para a gestão de serviços de TI garantindo organização e minimização de impacto para a operação.

A execução seguiu os seguintes passos: Descrição e justificativa resumida das regras; descrição completa das regras, com plano de backup, informação dos dispositivos e equipamentos afetados, análise de risco e impacto, plano de teste e plano de retorno (rollback); aprovação do planejamento em comitê técnico e em comitê de gestão de mudanças para verificar o impacto da mudança em outros sistemas e na infraestrutura de TI; execução da regra; validação e revisão; atualização de documentação e encerramento.

Homologação dos Equipamentos

O sistema permite a criação de modelos de equipamentos. Durante a implantação, o sistema oferece a possibilidade de incluir mais de 50 modelos de equipamentos de diferentes fornecedores. Cada equipamento criado no ambiente possui um modelo, e cada modelo precisa ser validado para garantir que todo equipamento instanciado a partir desse modelo não apresente erros. Este fluxo é apresentado na Figura 3.

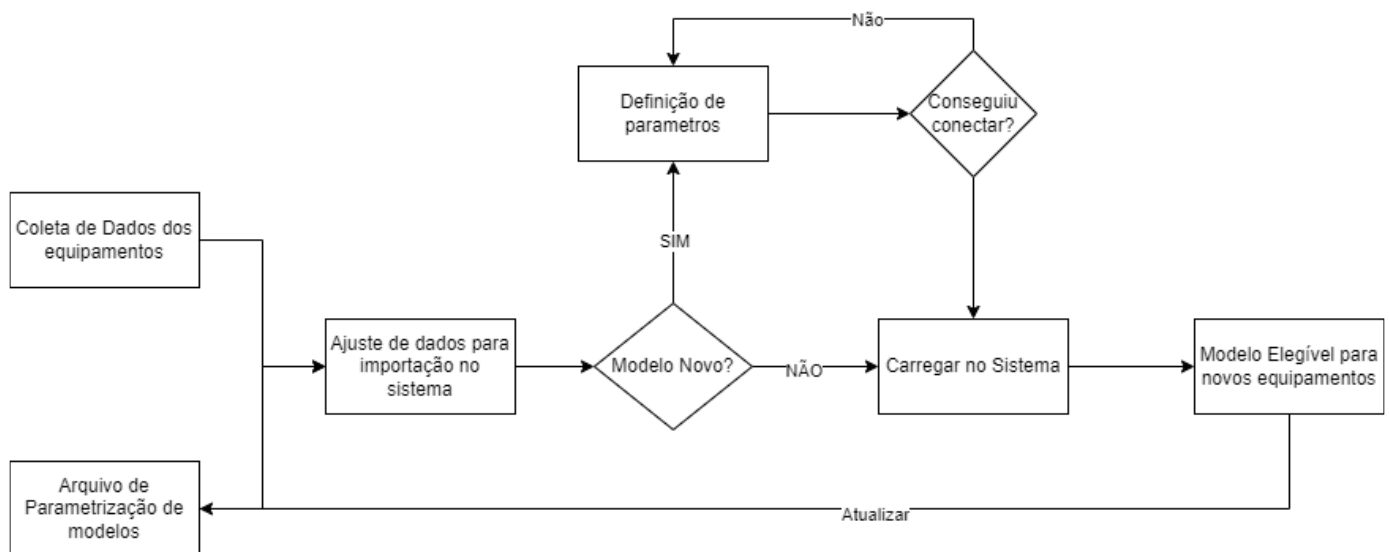


Figura 3 - Fluxograma de homologação de modelos. Fonte: Autor.

A coleta de dados dos equipamentos é o processo de obtenção das informações de conexão com o ativo de automação. Nessa etapa, obtemos as principais informações de conexão: IP, porta, firmware, usuário e senha. Este processo foi realizado por meio de idas ao campo, acesso remoto automatizado, planilhas distribuídas entre colaboradores e dados cadastrados no sistema SCADA. Sem essa etapa, não seria possível conectar aos ativos pelo sistema.

O arquivo de parametrização de modelos é o arquivo que contém todas as configurações de modelos já validados. Este arquivo contém informações importantes para o sistema, permitindo a criação correta de um equipamento com base em um modelo.

Uma vez que existem duas fontes de informação (um arquivo com as informações de conectividade e um arquivo com os parâmetros de configuração do equipamento no sistema), a etapa de Ajuste de Dados para Importação irá uni-los em um único arquivo para importação no sistema.

Se o equipamento possui um novo modelo e não há uma parametrização consolidada que garanta que todas as funções do SAGA sejam executadas corretamente, a etapa de Definição de Parâmetros será realizada até que seja encontrada a melhor configuração para o modelo. Uma vez validado, o equipamento é carregado no sistema e o modelo é categorizado como elegível, permitindo que novos equipamentos desse modelo sejam instanciados sem precisar passar por esse processo novamente. Em situações onde os modelos são incompatíveis, a empresa fornecedora é acionada para o desenvolvimento do driver de conexão.

Go Live

O Go Live resultou na liberação do acesso ao sistema para todo o grupo que precisa dos dados fornecidos pelos ativos de automação. Com a entrada do sistema, iniciou-se a avaliação de performance do ambiente para um uso esperado de mais de 80 usuários diariamente.

Foram identificados 5 perfis de usuários no domínio de segurança de IEDs, e para cada perfil, foi analisado o tipo de funções e informações que cada um necessita. Com base nos perfis, foram criados 5 grupos de acesso no sistema e no Active Directory (AD) da companhia. Com isso, foi possível selecionar as funções do sistema que podem ser executadas por perfil de usuário, limitando o acesso a informações sensíveis, garantindo que quem precisa manter o ambiente tenha acesso a essas funções, enquanto quem precisa apenas utilizá-lo tenha acesso restrito.

O grupo de administradores do sistema tem privilégio total ao sistema, pois é o time responsável pela sustentação do aplicativo na distribuidora. São as pessoas que irão criar rotinas, políticas, homologar modelos e garantir a integridade do sistema.

O grupo de estudos foca na coleta de oscilografias, ajustes dos relés e leitura de eventos antes e após ocorrências. O grupo de automação atuará apenas em garantir a integridade das informações.

O grupo COI foi criado para o uso operacional dos ativos: coleta de eventos, liberação de atividades e conectividade com os equipamentos. E, por fim, o grupo de manutenção faz uso do sistema como regularizadores dos ativos em campo.

Os usuários requisitam o acesso via sistema de gestão de chamados da companhia e, após a aprovação de pessoas-chave do processo, o usuário é cadastrado nos grupos de acesso requisitados por meio de um processo automatizado, sendo ele não limitado a apenas um grupo. O Go Live contou com a participação de todas as áreas envolvidas: automação, time de projetos, empresa fornecedora, TI infraestrutura, TI redes e TI banco de dados. Todas as áreas acompanharam por 2 semanas o lançamento do novo sistema, e durante o período, não houve ocorrências de perda do sistema, de dados ou de comunicação.

Resultados

Durante o período de teste no ambiente de homologação, foi possível testar cerca de 10 modelos distribuídos em 15 equipamentos, incluindo equipamentos de 1 subestação e equipamentos de laboratório. Com o sucesso desta etapa, a próxima foi a execução dos mesmos testes em ambiente de produção.

Após a entrega do ambiente de produção e com os dados iniciais das redes de TO (cadastrados entre os sistemas da companhia de TI, SCADA e colaboradores chave de outras áreas), foi possível realizar 2 tipos de testes. O primeiro teste foi de conectividade dos servidores às redes e o segundo, de conectividade com os equipamentos de TO.

O primeiro teste resultou na liberação da rede de TO de cada distribuidora ao ambiente SAGA. Mais de 500 regras de rede foram analisadas e blindadas para comunicar com o novo ambiente. Este teste foi validado utilizando os resultados de programas de varredura de IPs liberados durante a execução do projeto.

Para o segundo teste, e conhecendo as redes de TO, o processo de coleta de dados dos ativos resultou em um algoritmo em Python para acessar os ativos de automação e coletar as informações dos equipamentos que estavam na rede. Neste processo, mais de 4 mil equipamentos foram identificados, incluindo remotas,

relés e switches. Outro método, mais manual, buscou os mesmos tipos de dados em arquivos compartilhados entre colaboradores.

Todos os equipamentos coletados foram cadastrados no sistema, e utilizou-se a ferramenta de Teste de Aceitação do Usuário (UAT – User Acceptance Test) para extrair o resultado da conexão TCP/IP e das portas proprietárias de cada equipamento. Outro produto resultante desse trabalho foi a entrega do painel para acompanhamento da implantação (Figura 4). Este relatório facilitava, também, a identificação dos tipos de problemas de integração, permitindo correções imediatas.

Entre os principais problemas encontrados durante a integração de equipamentos ao sistema, pode-se caracterizá-los de acordo com os cenários abaixo e as possíveis formas de solução:

- Cenário 1: Se todas as tarefas de todos os equipamentos de uma subestação falharam, havia um problema de conectividade entre os servidores SAGA e a rede da subestação. Essa falha poderia ser momentânea ou relacionada às regras de rede. Esses pontos eram mapeados e corrigidos por um time em campo (no caso de falha geral de comunicação da subestação) ou pelo time de redes (em falha por regra de rede).
- Cenário 2: Se todas as tarefas que utilizavam uma porta específica falharam em uma subestação e os equipamentos estavam comunicando, o problema estava relacionado à liberação de regra de rede para a porta necessária. Dessa forma, o time de redes era acionado para corrigir as regras.
- Cenário 3: Se todas as tarefas de um modelo falharam e os equipamentos possuíam conexão com o SAGA, havia um problema de configuração na parametrização dele dentro do sistema. Assim, era necessário reconfigurar os parâmetros e aplicá-los como padrão para todos os equipamentos do mesmo modelo que fossem implantados no futuro.
- Cenário 4: Se um equipamento falhava ao se conectar ao SAGA, mesmo sendo baseado em um modelo já validado e com conexão existente, havia a possibilidade de um problema local no equipamento que impedia a coleta. Esse cenário era comum em modelos seriais, nos quais a falha encontrava-se no conversor serial para Ethernet ou nas informações cadastrais do equipamento, como IP, porta, usuário e senha.

A Figura 4 apresenta uma sessão do painel, mostrando quantos testes foram executados no fim da homologação. Mais de 36 mil testes foram realizados, com um tempo médio de 1 minuto por teste e uma taxa de falha de 11% entre as opções apresentadas anteriormente.

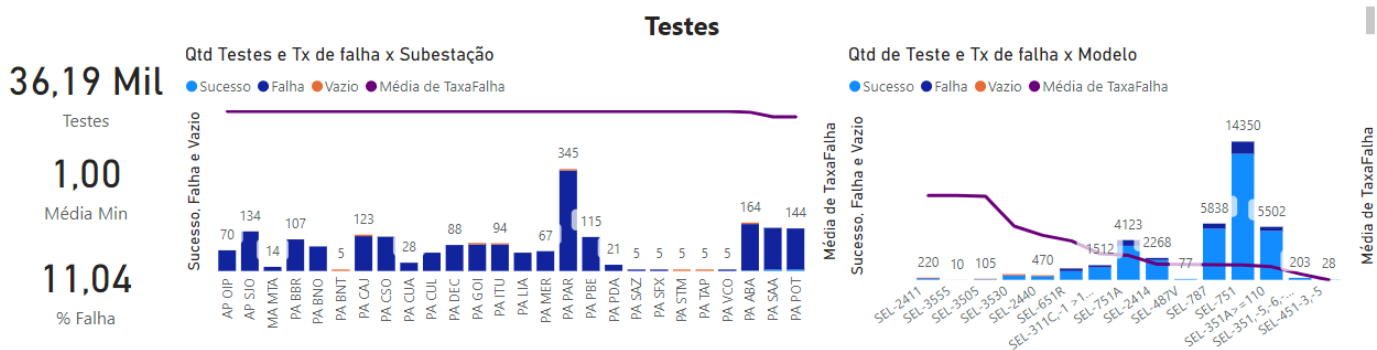


Figura 4 - visão do painel de de acompanhamento dos testes de homologação de equipamentos. Fonte: Autor.

Outro exemplo de análise para auxiliar no dimensionamento de funcionalidades está apresentado na Figura 5. Neste gráfico, podemos ver as diferentes tarefas executadas pelo sistema no eixo X, a duração média da execução dessas tarefas em minutos no eixo Y à esquerda e a taxa de falha por categoria no eixo Y à direita.

Cada item do gráfico refere-se às diferentes portas de comunicação proprietária com os equipamentos. A tarefa de leitura de configurações é a mais demorada entre todas as portas proprietárias, sendo a porta proprietária propr2 a mais impactante.

Duração os serviços e Tx de falha

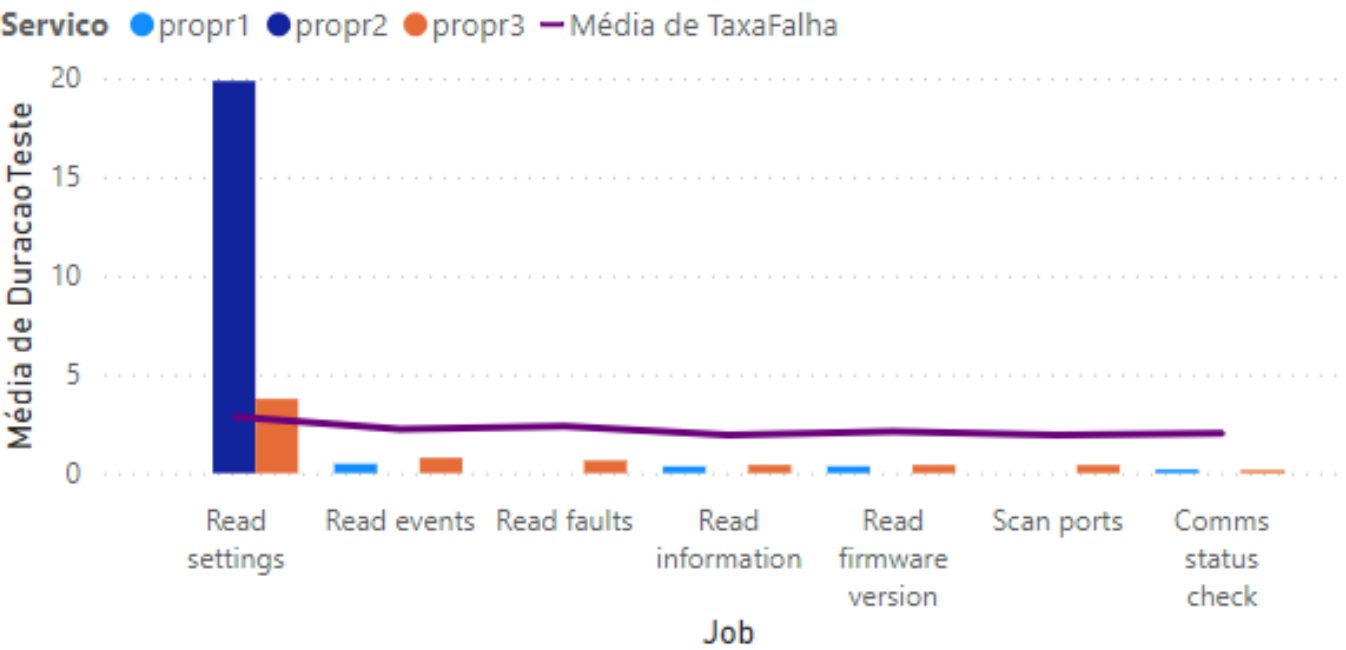


Figura 5. Média de duração dos serviços executados pelo sistema para identificação de gargalos.Fonte: Autor.

Desta forma, ao aplicar as rotinas de coleta automática de eventos e oscilografias, elas não podem ser executadas junto às leituras de configurações. Sendo necessário segregar as tarefas dentro do sistema. O ambiente está preparado para realizar as rotinas de troca de senhas, aplicando a camada final de segurança. Entretanto, a atividade está sendo planejada para execução gradual nos ativos do grupo. Por se tratar de uma atividade crítica, é necessário que os usuários estejam previamente familiarizados com a ferramenta e que o sistema tenha sido submetido a períodos críticos de carga de acesso. Após a entrega, o ambiente conta com 4.700 equipamentos cadastrados, sendo que os equipamentos, após a carga inicial, estão sendo cadastrados manualmente por meio de um outro projeto de cadastro de ativos. Além do cadastro de novos equipamentos, este time também mantém a integridade dos dados e realiza ajustes no nome dos equipamentos, com um total de mais de 2 mil intervenções no sistema. A integração desses equipamentos permite a execução de rotinas automáticas de coleta de eventos. Estes equipamentos já possuem cerca de 40 mil arquivos de oscilografias e 580 mil eventos salvos, que não serão sobrescritos. Os dados estão sendo salvos em um banco de dados com rotinas de backup diárias, mensais e anuais. Atualmente, as rotinas de coleta automática têm duração de 1 semana, com o objetivo de reduzir esse tempo para que a coleta seja executada diariamente. A Figura 5 acima se torna importante para os estudos de redução de tempo. O ambiente conta com 10 a 20 pessoas com acesso diário. A adesão ao sistema está sendo feita de forma gradual à medida que a necessidade de trabalhar com históricos de eventos, oscilografias e backups de configurações dos equipamentos aumenta, além da execução gradativa de treinamentos sobre o uso do ambiente.

3. Conclusão

A implantação do sistema de automação e monitoramento dos ativos de automação foi um processo desafiador, marcado por diversas etapas, desde a homologação até o Go Live. Durante a fase de implementação, os principais desafios foram relacionados à parametrização e validação dos modelos de equipamentos, à configuração das redes de comunicação e à realização de testes para garantir a conectividade entre os servidores e os equipamentos de automação. Esses desafios exigiram ajustes contínuos e uma análise detalhada para assegurar que o ambiente fosse robusto e capaz de suportar a demanda de operações em larga escala.

Os resultados obtidos até o momento demonstram que a implantação foi bem-sucedida. Mais de 4.700 equipamentos foram cadastrados e estão operando com sucesso no sistema. A coleta automática de eventos e oscilografias já é realizada de maneira eficiente, com um grande volume de dados sendo armazenado de forma segura e organizada. A realização de mais de 36 mil testes, com uma taxa de falha de 11%, forneceu informações valiosas sobre os processos que necessitam de melhorias, como a configuração das portas de comunicação e a segregação das tarefas dentro do sistema para otimizar o desempenho.

Entretanto, ainda existem pontos de melhoria e próximos passos importantes a serem seguidos. A continuidade dos treinamentos será essencial para aumentar a adesão ao sistema, reduzir o impacto operacional e garantir o uso eficiente da ferramenta. A redução do tempo de coleta automática de dados, com o objetivo de realizar essa coleta em um único dia, é uma prioridade para garantir informações mais rápidas e precisas. Além disso, a implementação de um plano para troca automática de senhas, a inclusão de novos equipamentos e a criação de novos modelos são fundamentais para garantir a escalabilidade e a segurança do sistema.

Com a superação dos desafios iniciais e o foco nos próximos passos, o sistema de automação está bem posicionado para oferecer um suporte contínuo e eficiente na segurança cibernética na rede de TO, na gestão dos ativos, além de contribuir para a melhoria das operações da empresa.

4. Referências bibliográficas

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA (ANEEL). Resolução Normativa ANEEL n.º 964, de 14 de dezembro de 2021. Diário Oficial da União, Brasília, 15 dez. 2021. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-%20de-2021-369359262>. Acesso em: 2 dez. 2024.

HEINISCH, Astrid et al. Segurança cibernética para processos operativos em sistemas de energia elétrica. Publicado no Centro de Gestão de Tecnologia e Inovação – CGTI, 2012.

ROSERO, Oscar Andrés Tobar et al. Digital Substations and Cybersecurity in the Transformation of the Electricity Sector. In: 2023 IEEE Colombian Caribbean Conference (C3). IEEE, 2023. p. 1-6.

Loureiro R, Mendes G, Rodrigues da Silva R, Nogueira H, Restrepo K, “Automation & Security of OT Data Network”, IEEE Mexico.

EQUATORIAL. Regiões de Atuação. Disponível em: <https://www.equatorialenergia.com.br/grupo-equatorial/regioes-de-atuacao/>. Acesso em: 8 dez. 2024.