Q&A – CPP Multitemas

Tema 2 – Otimização e Resposta Inteligente na Operação do Sistema de Transmissão

Questões Técnicas e Conceituais do Tema

1. Qual é o problema central no cenário atual ("As Is")?
   R.: A operação ainda depende fortemente de interpretação manual de alarmes e eventos com dados fragmentados e baixa correlação automática, aumentando carga cognitiva, tempo de resposta e risco de erro. As Ordens de Manobra (OMs) são elaboradas, executadas e registradas manualmente, com inconsistências e baixa rastreabilidade.

2. Para solucionar o problema vigente, qual é a principal entrega esperada?
   R.: O projeto deve entregar uma solução que modernize a operação em tempo real do sistema de transmissão, com foco em apoio inteligente à decisão, tratamento automatizado de alarmes e automatização das Ordens de Manobra, reduzindo carga cognitiva, riscos operacionais e erros humanos.

3. Qual é a visão do cenário futuro ("To Be") com a implantação do projeto?
   R.: Evolução para um ambiente digital, integrado e inteligente, no qual
   - alarmes são correlacionados e priorizados automaticamente;
   - diagnósticos são acelerados por IA;
   - OMs são geradas e validadas automaticamente (regras, permissivas, intertravamentos);
   - execução e registro integrados ao SCADA e sistemas corporativos.

   Além disso, ter um assistente operacional baseado em IA capaz de:
   - interpretar eventos em tempo real;
   - priorizar alarmes críticos;
   - sugerir ações operativas e validar condições antes da execução;
   - reduzir risco de interpretação equivocada e tempo de diagnóstico.

   Por fim, os principais resultados esperados são:
   - operação mais ágil, confiável e eficiente;
   - diagnósticos rápidos e alarmes priorizados automaticamente;
   - redução de erros humanos e consultas paralelas;
   - rastreabilidade ponta a ponta (operação e manutenção);
   - aumento da disponibilidade dos ativos e eficiência na recomposição.

4. Qual a expectativa sobre integração entre as áreas de Operação e Manutenção?
   R.: A solução deve encaminhar automaticamente, de forma rastreável e tempestiva, anomalias, restrições e indisponibilidades às equipes responsáveis, fortalecendo integração entre áreas.

5. Sobre as Ordens de Manobra realizadas no Centro de Operação da Transmissão, fazem-se os seguintes questionamentos:
    a. Como é o fluxo/processo de governança (criação, edição, aprovação, execução, encerramento) de OMs? Há dupla checagem, segregação de funções, perfis/roles? Há condições de exceção/urgência?
    b. Em que sistema a OM é mantida oficialmente? Há integração entre diferentes sistemas (Sigom/SAP/PowerDoc)?
    c. Quem assume a responsabilidade final em caso de falha?
    d. É obrigatório assinatura digital, carimbo de tempo e trilha de auditoria? Se sim, qual tecnologia/padrão de assinatura digital é utilizada e quais requisitos de retenção/auditoria devem ser atendidos?

    R.: As informações essenciais acerca das Ordens de Manobra são:
    a. Cada OM é executada por um operador, revisada por outro e por fim aprovada. Existem OMs que são criadas/aprovadas com o rito de programação (AT-O-PRE) e outras que são criadas/aprovadas com o rito em regime de urgência.
    b. O repositório oficial das OMs é o SIGOM.
    c. A responsabilidade final é do colaborador responsável pela aprovação.
    d. A validação/assinatura da OM está vinculada ao usuário logado no SIGOM. A solução deve apenas sugerir a OM e o colaborador aceitará ou modificará a OM. Portanto, a solução deve fornecer as ferramentas adequadas de certificação e rastreabilidade desde o momento da criação até o final da execução da OM.

6. Sobre a automação das Ordens de Manobra a serem propostas no projeto deste Tema da CPP, fazem-se os seguintes questionamentos:
    a. A geração automática de Ordens de Manobra será autônoma ou sempre com validação humana, com que níveis de aceite e segregação de funções?
    b. A solução poderá criar/abrir OM no sistema oficial ou apenas sugerir/rascunhar OM para que um humano registre/aprove? Em ambos os casos, quais campos mínimos e validações são exigidos? Qual é o nível de autonomia esperado para padronizar OMs?
    c. Qual o limite de automação permitido por fase, sugestão apenas, validação automática de permissivas, execução sob duplo aceite, execução autônoma em contingência?
    d. A automação das OMs deve considerar quais restrições?

    R.: As informações essenciais acerca da automação de Ordens de Manobra são:
    a. A geração de OM deve passar por validação humana, com níveis de aceite e segregação de funções ou papéis e responsabilidades específicos a depender do tipo de aprovação.
    b. A solução poderá criar uma OM em nível de sugestão e sempre validar com a ação humana para o devido registro/aprovação. Os campos

mínimos são os modelos de OM que devem ser treinados na solução. O nível de autonomia está atrelado aos modelos existentes na empresa a serem compartilhados oportunamente.

c. Sobre o limite de automação, a solução deve sugerir uma OM, e após confirmação do operador, executar a etapa autorizada.
d. Em resumo, as OM devem ser geradas e validadas conforme:
    - regras operativas padronizadas;
    - intertravamentos e permissivas;
    - restrições sistêmicas e condições de segurança;
    - histórico de manobras realizadas.

7. Em que sistema estão armazenados as regras operativas, código, motor de regras, base de conhecimento, e como será feito versionamento, rastreabilidade e processo de validação?
   R.: As regras normativas e procedimentos de operação estão armazenadas no sistema PowerDoc e serão disponibilizados oportunamente para a execução do projeto.

8. Sobre os alarmes presentes no Centro de Operação da Transmissão, fazem-se os seguintes questionamentos:
    a. Quais são os critérios formais de priorização de alarmes, definição de crítico, major, minor, e como essa taxonomia se alinha ao despacho e às normas internas?
    b. Há uma estratégia para lidar com alarmes espúrios, dados faltantes e mudanças topológicas frequentes, inclusive detecção e tratamento on-line?
    c. Quais exemplos de alarm flood podem ser citados? Com qual frequência e em que situações acontecem?

   R.: As informações essenciais acerca de alarmes são:
    a. Alarmes estão divididos em grupos de prioridade: PRIORIDADE 0, PRIORIDADE 1, PRIORIDADE 2, PRIORIDADE 3.
    b. A solução proposta deve contemplar esse tratamento.
    c. Como exemplos de alarm flood, podemos citar um desligamento sistêmico ocorrido em outubro/2025. Num período de 2 horas e 52 minutos, ocorreram 19.549 alarmes. No primeiro minuto após o desligamento ocorreram 4.209 alarmes, no segundo minuto 578 alarmes e no terceiro minuto 372 alarmes. Estes desligamentos grandes são mais raros e acontecem em torno de 6 vezes ao ano, mas desligamentos automáticos menores acontecem diariamente.

9. Quais métricas de sucesso e critérios de aceite, incluindo metas/thresholds esperados para cada KPI, estão previstos/serão utilizados? Taxa de alarmes perdidos, precisão de priorização, redução de retrabalho, metas numéricas por marco, tempo de diagnóstico, tempo de recomposição, redução de alarm flood, acurácia de correlação, taxa de recomendações aceitas, comparação com histórico?

   R.: A proposta pode oferecer as métricas de aceite e KPI, desde que validado com as áreas de Negócios. Como sugestão temos alguns critérios de aceite do piloto (condição de aprovação do MVP):

   A. Correlação e priorização de alarmes:
   - Acurácia de priorização dos alarmes (P0–P1): ≥ 85%
   - Redução do tempo de diagnóstico: ≥ 30%
   - Redução de alarm flood: ≥ 30%
   - Latência ponta a ponta (ingestão → exibição) para alarmes críticos: ≤ 2 s. (Atende necessidade de operação em tempo real.)

   B. Geração e validação de OM:
   - Cobertura de campos obrigatórios nas OMs do escopo: 100%
   - Taxa de retrabalho: (OMs corrigidas/OMs emitidas) x100: ≤ 50%
   - Checagem automática de permissivas/intertravamentos: 100% (sem violações — critério eliminatório)
   - Trilha/auditoria completa: criação → revisão → aprovação → execução, com retenção mínima de 5 anos
   - Redução do tempo de elaboração de OM: ≥ 50%

   C. Registros das OMs:
   - 100% dos campos definidos no escopo preenchidos corretamente;

   D. Execução das OMs:
   - 100% dos equipamentos telecomandados devem ser comandados executando a OM (dar play na etapa) com a validação pelo Operador. E taxa de erro deve ser zero
   - Sendo necessária pela Solução a validação prévia dos intertravamentos e condições operacionais da subestação
   - A medição deve contemplar índice de redução do tempo de execução do roteiro de manobras (a ser definido)

   E. Recomendações operativas (tensão/fluxo)
   - Taxa de recomendações aceitas: ≥ 70% (piloto).
   - Tempo (ingestão → recomendação): ≤ 5 s.
   - Explicabilidade: 100% das recomendações com justificativa clara (regras/estados/histórico utilizados).

   Considerando que a proposta deve contemplar sugestões de métricas de sucesso e comparação "As Is" × "To Be", e que há histórico amplo disponível para embasar metas, propõe-se o seguinte conjunto operacional de métricas com metas por fase (MVP → expansão):

A. Taxa de alarmes perdidos (missed alarms): ≤ 0,5% no MVP e ≤ 0,1% na expansão. (Garante ingestão/correlação completas.):

- Precisão de priorização (P0–P3): ≥ 85% (MVP) → ≥ 92% (expansão). (Aderente à taxonomia P0–P3 indicada.)
- Acurácia de correlação de alarmes: ≥ 80% (MVP) → ≥ 90% (expansão). (Agrupamento coerente de eventos correlatos.)
- Redução de alarm flood: ≥ 30% (MVP) → ≥ 50% (expansão). (Mitiga rajadas, melhora foco do operador.)

B. Ordens de Manobra (OMs):

- Redução de retrabalho em OM: ≥ 40% no MVP (pela padronização + validação automática).
- Tempo médio de elaboração de OM: redução ≥ 50% (com rascunho sugerido e checagens de permissivas/intertravamentos).
- Aderência a regras/intertravamentos: 100% de checagens aplicadas (critério "hard rule", sem exceção).

C. Apoio à decisão e eficiência:

- Tempo de diagnóstico de eventos: redução ≥ 35%. (IA auxilia interpretação e priorização.)
- Tempo de recomposição pós-distúrbio: redução ≥ 20%. (Sugestões operativas e organização do contexto.)
- Taxa de recomendações aceitas: ≥ 60% (MVP) → ≥ 75% (expansão). (Confiança do operador na recomendação com explicabilidade.)
- Explicabilidade mínima: 100% das recomendações com justificativa (regras acionadas, estados verificados, histórico).

Observação: Metas iniciais podem ser refinadas após baseline em dados históricos (SCADA/SIGOM/PowerDoc) e teste-sombra no MVP, conforme descrito em outras partes deste FAQ (proponente sugere metodologia e utiliza histórico disponível). Ressaltamos, novamente, que esses critérios são sugestões, e os parceiros têm liberdade para incrementar os critérios inicialmente apresentados, desde que validados pela CPFL.

10. No caso de histórico, como será feita a comparação (medição "antes e depois"), existe baseline histórico disponível (quais fontes/dados e quanto tempo), qual período de baseline será considerado (semanas/meses) e qual metodologia será usada para comparação (ex.: mesma regional, mesmos tipos de eventos, janelas equivalentes, controle de sazonalidade)?

R.: A metodologia propõe baseline pré-piloto e comparação controlada no piloto, utilizando dados históricos e ambientes de teste indicados no FAQ.

A. Fontes de baseline (dados "As Is")

- SCADA/SAGE (historiador): SOE, alarmes, analógicos, qualidade (em relação ao acesso via historiador e/ou dump para carga inicial).

- SIGOM: intervenções, OMs, tempos de criação/execução (em relação ao consumo via base de dados replicada Postgres).
- PowerDoc: procedimentos/versionamento aplicáveis às OMs.
- Outros (quando pertinente e/ou necessário): SAP (extrações D-1 via Databricks) para cruzamentos operativos.
- Amplitude histórica: há >15 anos de dados no Portal da Operação para alarmes e medidas analógicas, viabilizando análises robustas.

B. Período de baseline

- 3 meses: métricas de alto volume (latência, alarm flood, priorização).
- 6–12 meses: métricas de eventos menos frequentes (contingências, recomposição).
- ≥12 meses (opcional): controle de sazonalidade (clima/expansão do parque). A escolha é viabilizada pelo histórico amplo citado.

C. Metodologia de comparação

- Janelas equivalentes: comparar períodos com mesma os mesmos tipos de eventos e em ativos equivalentes.
- Normalização/controle de sazonalidade: ajustar por fatores climáticos e mudanças topológicas/expansão (quando aplicável).
- Shadow mode (A/B operacional): durante o piloto, a solução deve trazer sugestão e insights que auxiliem a pré-decisão (sem execução autônoma); registra-se a decisão humana vs. recomendação da IA para comparação de qualidade/tempo (Alinhado ao requisito de validação humana e explicabilidade).
- Medição direta pós-ativação (To Be): coletar tempos reais (diagnóstico, recomposição, elaboração de OM), acurácias (priorização/correlação) e indicadores de uso (taxa de recomendações aceitas).
- Auditoria e retenção: garantir trilha completa (sugestão → clique → comando → alteração), com retenção ≥5 anos para inspeções.

11. Qual é o conjunto mínimo viável de casos de uso que entrega valor, por exemplo, correlação de alarmes críticos, checklist de permissivas, geração de esboço de Ordem de Manobra?
    R.: Pode-se destacar correlação de alarme críticos, rascunho de Ordem de Manobras, sugestão de ações operativas de controle de tensão e fluxo de potência, execução de preparação de instalação após blecaute.

12. Quantos operadores simultâneos usam a solução (por turno) e, nos piores momentos, qual o volume de consultas por operador (por minuto/hora), incluindo quais telas/relatórios hoje geram maior carga (correlação, histórico, busca por ativo, busca por evento, navegação por diagrama)?

R.: Existem 8 posições operacionais na sala do COT CPFL-T, no pior caso considerar 8 operadores simultâneos.

13. Quais são as principais consultas críticas esperadas (por exemplo, "top 10"), incluindo filtros típicos (por ativo, alimentador, subestação, alarme, janela temporal, tipo etc.), e há necessidade de agregações pesadas (ex.: P95 de latência, contagens por tipo, correlação por janela)?
    R.: O projeto deverá propor necessidade, a qual será submetida a validação do CEPEL e avaliação de requisito disponível.

14. Qual é a política de atualização e retreinamento dos modelos, gatilhos, janelas de dados, aprovação por especialistas, teste A/B ou shadow e critérios de promover para produção?
    R.: É escopo do projeto definir a taxa se atualização e retreinamento necessária para garantir a confiabilidade e assertividade das respostas do modelo.

15. Como será a explicabilidade mínima das recomendações da IA para decisão operativa, exemplos, evidências, regras acionadas, estados verificados, trilha de auditoria?
    R.: A explicação deve ser uma recomendação, de modo a evoluirmos o desenvolvimento. Também pode ser informado que a recomendação está baseada na quantidade de histórico disponível.

16. O "assistente inteligente" será chat operacional, sistema especialista, LLM, ou combinação, e em quais jornadas cada componente é aplicado?
    R.: Não há uma predefinição sobre esse aspecto, assim, faz parte da proposta definir a solução a ser aplicada em cada caso.

Escopo e Estrutura de Projeto

17. Qual é a estrutura mínima de macro etapas esperadas para o projeto?
    R.: A proposta deve conter cronograma e estrutura com entregas mínimas, incluindo:
    - Planejamento e diagnóstico inicial (requisitos, riscos, arquitetura);
    - Desenvolvimento da solução (módulos, dashboards, trilhas de auditoria);
    - Ambiente de qualidade (produto mínimo viável (MVP), testes, validação);
    - Integração e testes em ambiente operacional;
    - Implantação e capacitação (manuais, treinamento, suporte assistido);
    - Avaliação de resultados e encerramento (indicadores, validação, relatório final).

18. O projeto pode (ou deve) ser fatiado em MVPs?
    R.: Sim. O Termo de Referência exige que o projeto inclua MVPs e checkpoints para avaliação de continuidade por métricas de avanço, com fluxo claro das fases e critérios de evolução.

19. Quais módulos podem compor o produto final?
    R.: O produto final é descrito como uma plataforma integrada, potencialmente composta por três módulos:
    - Assistente inteligente (IA) para diagnóstico e apoio à decisão em tempo real;
    - Módulo de otimização para automatização/validação de Ordens de Manobra;
    - Módulo de detecção automática de anomalias baseado em aprendizado de máquina.

20. Como parte da solução, há direcionamento acerca de otimização de rede em tempo real ou apenas sugestão, com simulação elétrica detalhada, fluxo de carga, curto-circuito ou heurística?
    R.: O SAGE é um SCADA EMS que possui modelagem elétrica. O registro em forma de onda (comtrade) de eventos de curto-circuito bem como a modelagem de proteção não estão disponíveis para este projeto.

21. Como se espera que ocorra o rollout: haverá piloto (ex.: 1 regional/1 subestação) seguido de expansão, e qual a estratégia/ritmo de expansão prevista?
    R.: O projeto deverá apresentar os custos e requisitos necessários para manter a solução em funcionamento, bem como plano de suporte e evolução da ferramenta. Este custo precisará ser avaliado por comitê competente para que o protótipo possa ser implementado para ambiente produtivo.

22. É permitido submeter projetos de desenvolvimento de dispositivos, especialmente sensores para monitoramento de linhas de transmissão?
    R.: Não é escopo deste tema da CPP a implantação ou desenvolvimento de novos sensores, bem como a intervenção local em qualquer instalação elétrica da CPFL-T como subestação e/ou linha de transmissão.

Dados – Estrutura, Disponibilidade e Variáveis de Interesse

23. Sobre o sistema SCADA, fazem-se os seguintes questionamentos:
    a. Qual o tamanho atual do ambiente em termos de quantidade de pontos?
    b. Qual a projeção de crescimento em 12/24/48 meses, incluindo expectativa de incorporar novas regiões/centros de operação?

c. Qual a frequência de amostragem do SCADA, volume e histórico disponível, existência de dados rotulados de falhas e alarmes críticos, e qualidade desses rótulos?
d. O SCADA será apenas provedor de dados ou também executor de comandos gerados externamente, e em quais condições?

R.: As informações essenciais acerca de alarmes são:

a. O sistema SCADA atualmente conta com 98.846 digitais, 14.371 analógicos, 9.165 comandos.
b. Considerar a taxa de crescimento de 10% ao ano.
c. O SCADA obtém dados em tempo real, tendo um histórico com volume atual de 11.9 TB.
d. Atualmente o SCADA provê dados, e executa comandos a partir de ação manual do operador.

24. Qual será o mecanismo de acesso aos dados do SCADA/historiador: streaming de eventos (push), consultas sob demanda (pull) ou híbrido (stream + lookup), e quais limites formais/operacionais existem para não degradar o SCADA (taxa máxima de leitura/rate limit, conexões simultâneas, consultas por segundo e tamanho máximo de resposta)?
R.: O projeto deverá propor necessidade, a qual será submetida a validação do CEPEL e avaliação de requisito disponível.

25. Quais formas de integração/exposição de dados a CPFL espera/aceita que a solução implemente (API REST/SOAP, acesso a banco, export batch, filas/mensageria, datalake, arquivos em blob storage), e no caso de arquivos: quais formatos/padrões são aceitos (CSV, JSON, Parquet, Avro etc.)?
R.: A integração deve ser proposta pelo projeto e será avaliada pelo time de arquitetura e/ou segurança cibernética conforme o caso.

26. Qual é o "ID mestre" (chave única) do ativo/equipamento e como essa chave se relaciona/mapeia entre SCADA, GIS/cadastro técnico, Sigom, SAP e PowerDoc (ex.: qual sistema é o "source of truth", quais chaves alternativas existem e como é feito o cross-reference)? Existem problemas conhecidos de inconsistência de identificação (ex.: mesmo ativo com IDs diferentes, duplicidades, divergência de nomenclatura/localização) e há regras oficiais para reconciliação (prioridade de fontes, critérios e exceções)?
R.: Não há um mapeamento de ativos entre as bases. Para alguns casos é possível mapeá-los pela posição operacional.

27. Quais dados externos são mandatórios para correlação/enriquecimento (topologia elétrica atual — rede energizada/aberta, cadastro técnico, GIS, ativos, manutenção, OMs passadas, permissões de manobra, outros), em quais sistemas estão e qual o nível de qualidade/atualização desses dados?

R.: SAGE (Sistema Aberto de Gerenciamento de Energia) que é o sistema SCADA da CPFL Transmissão; SIGOM (Sistema Integrado de Gerenciamento da Operação) responsável pela gestão de intervenções, ordens de manobras e registro de eventos do Sistema da Transmissão; PowerDoc que é o sistema responsável pela gestão dos diagramas unifilares, procedimentos e rotinas operativos da área de Transmissão; e Ordens de Manobras arquivadas na rede corporativa da CPFL Transmissão em formato Excel.

28. Existe catálogo de alarmes padronizado (prioridade, severidade, classe, causa provável, outros) e os alarmes já chegam com tipo/categoria consistente ou há muita variação por região/ativo?
    R.: Sim. O alarme está relacionado com a causa de defeito e/ou com a atuação proteção em específico de cada evento. O padrão é diverso conforme o histórico de implantação dos ativos, tendo sido padronizado nos últimos anos.

29. Há mapeamento confiável de pontos e ativos (equipamento real), localização (GIS) e existe dicionário/documentação de tags (naming convention) disponível?
    R.: Há mapeamento dos ativos e localização (GIS).

30. Os eventos têm ordem garantida (SOE sequencial) ou pode haver reordenação no caminho (ex.: atrasos, retransmissões, buffer)?
    R.: Pode haver atrasos, retransmissões, buffer, devido a diversidades de motivos.

31. Para cada ponto/telemetria, quais metadados vêm junto: timestamp de origem (SOE) ou apenas timestamp de chegada, e quality flag (good/bad/uncertain/substituted/others)?
    R.: Timestamp Origem (apenas).

32. Quais classes de dispositivos alimentam o SCADA (RTUs, IEDs de proteção/controle, religadores, chaves telecomandadas, medidores, concentradores, outros) e existe inventário por fabricante/modelo/firmware (ao menos por família)?
    R.: IEDs de proteção/controle, medidores, concentradores. Há inventário de fabricante, família e modelo.

33. Quais protocolos/padrões estão no caminho até o SAGE/SCADA (IEC 60870-5-104, DNP3, IEC 61850, Modbus, OPC, ICCP/TASE.2, outros) e qual será o mecanismo de integração "nativa ao SAGE" (API do fornecedor, banco/historiador, OPC, fila/mensageria, export de SOE)?

R.: Protocolos de comunicação entre Subestações e SAGE Centro IEC101, IEC104. O dado está disponível em banco SAGE Historiador. Poderá ser fornecido extração (DUMP).

34. Há necessidade de notificações push/event-driven ou é aceitável polling?
    R.: Não há uma definição sobre a forma de sincronização ou aquisição de dados, entendemos que essa arquitetura deve ser proposta pelo projeto, e validada pelos times de segurança da cibernética da CPFL em tempo de projeto.

35. Quais são os SLAs/tempos máximos aceitáveis para o fluxo desde a ingestão até a exibição (latência ponta a ponta), da ingestão até recomendação/diagnóstico e do fluxo criação, aprovação, execução de ordem de manobra, e quais metas de disponibilidade são esperadas (99,5%, 99,9%, 24x7)?
    R.: Disponibilidade 24x7. Tempo máximo depende se for pra pré ou para o tempo real.

36. Quais tipos/categorias de eventos estão no escopo (alarmes e prioridades, mudanças de estado/SOE, medições analógicas/qualidade, telecom, falhas de IED/RTU) e qual o tamanho típico do payload por evento (quais campos relevantes), além do volume total estimado em KB/MB por dia?
    R.: Não há como prever um volume por evento. Dada a diversidade do parque, no entanto o crescimento do banco de dados é da ordem 343 GB por Mês, em torno de 11,4 GB por dia.

37. Qual a política de retenção para eventos brutos (SOE/alarme), eventos enriquecidos/correlacionados e logs/auditoria (ordem de manobra, comandos, aprovações), e qual a janela típica de investigação (24h, 7 dias, 90 dias, 2 anos)?
    R.: A ANEEL não estabelece prazos próprios específicos, mas exige que todas as evidências necessárias para auditorias e fiscalizações estejam disponíveis, o que na prática leva muitas transmissoras a manter arquivos por 5 até 10 anos.

38. Qual o volume médio de eventos/alarmes (por minuto/hora/dia/mês) e qual o pico observado (P95/P99) , em que situações ocorre (chuva, tempestade, manobras programadas, contingência etc.) e se o padrão de chegada é burst/rajadas ou fluxo estável?
    R.: Em condições operativas normais, o volume de alarmes diário fica em torno de 40.000, isto dá em torno de 30 alarmes por minuto. Dentre estes, há alarmes espúrios, alarmes falsos, etc. Em ocorrências de grande vulto, quando há vários desligamentos simultâneos, ocorre uma enxurrada de alarmes em curtos períodos de tempo (burst/rajadas), nos primeiros minutos após a ocorrência. Estes são desligamentos automáticos que ocorrem por atuação de proteção do

sistema elétrico. Nesses casos pode ocorrer mais de 4.000 alarmes em um minuto.

Tecnologia da Informação

39. A solução precisa ser integrada a quais sistemas?
    R: É necessário que a solução opere em ambiente integrado, eliminando consultas paralelas, com integração ao SAGE/SCADA e conexão estruturada com sistemas corporativos e operacionais como Sigom, PowerDoc e SAP.

40. Existem APIs estáveis para SCADA, Sigom, PowerDoc, SAP, com limites de taxa, modos síncronos ou assíncronos e SLAs, ou será necessário middleware dedicado?
    R.: Atualmente temos disponíveis da seguinte forma:
    - SCADA – Acesso via Historiador ou DUMP
    - SIGOM – Base replicada em postgre disponível para conexão atualizado a cada 15min
    - SAP – Estrações disponíveis em (d-1) via dataBricks

41. Há integrações com Sigom, PowerDoc e SAP, existem APIs, são síncronas ou assíncronas, e há restrições contratuais ou de licenciamento?
    R.: Não existem APIs ou integrações disponíveis entre as bases.

42. Do ponto de vista de UX e operação, a solução deve ser integrada ao ambiente do operador (dentro do SCADA/console) ou pode ser uma aplicação paralela (ex.: web), e existem restrições mandatórias de UI/uso (idioma, layout, número máximo de cliques, atalhos, dark mode e outras)?
    R.: Deve ser integrada aos ambientes de Gerenciamento da Intervenção e passando para a execução do operador (dentro do SCADA).

43. Existem restrições e/ou boas práticas impostas pelo fornecedor do SCADA (SAGE) para operações de leitura e escrita (ex.: limites de taxa, janelas, objetos permitidos, segurança, auditoria)? Quais estratégias de performance são aceitas para atender consultas sem impactar o SCADA: uso de cache (memória/Redis), indexação em motor de busca e/ou replicação/espelhamento de dados do SCADA para um datastore dedicado de leitura (ex.: CQRS)? Caso seja permitido replicar/espelhar dados para leitura, quais requisitos devem ser atendidos quanto à consistência (eventual vs. forte) e qual o atraso máximo tolerado (staleness/lag) entre o SCADA e o datastore replicado?
    R.: O projeto deverá propor necessidade, a qual será submetida a validação do CEPEL e avaliação de requisito disponível.

44. Qual é o plano de tolerância a falhas e fallback operacional, modo sombra, modo sugestão, congelamento de automações, reversão de manobras, e tempos máximos de recuperação?
    R.: A estratégia de tolerância a falhas do SAGE é baseada em uma arquitetura de alta disponibilidade com múltiplos servidores distribuídos em data centers distintos, operando em modelo hot-hot, com múltiplas rotas de comunicação independentes, utilizando diferentes protocolos e meios físicos. Essa abordagem garante a continuidade da aplicação mesmo em cenários de falha parcial de infraestrutura, da mesma forma nas SEs possuímos redundância de equipamentos de controle, automação e proteção.

45. Existem limites de consulta/concorrência e boas práticas obrigatórias por sistema (com destaque para SAP), incluindo rate limits, janelas de execução, volumes máximos e requisitos de aprovação para integrações/queries?
    R.: Para o SAP as extrações devem ser realizadas via dataBricks, sendo que as consultas e a frequência devem compor a proposta e serão validadas pelo time de big data da CPFL.

46. Existem ambientes de homologação/teste para cada sistema/canal de integração (SCADA, GIS/cadastro, Sigom, SAP, PowerDoc e canais como API/banco/fila/datalake), e quais são as diferenças relevantes para produção (dados mascarados, limites, disponibilidade)?
    R.: Existem ambientes de teste para as aplicações SAGE, SIGOM e PowerDoc. A diferença fundamental é a versão dos dados ser defasada em relação à base produtiva.

47. Em telemetria/observabilidade, quais dashboards e indicadores de saúde são requeridos (ex.: atraso de ingestão, fila/backlog, erros de integração, latência de consulta e outros), quais alertas devem existir e qual ferramenta padrão corporativa deve ser usada (se houver)?
    R.: A CPFL utiliza um modelo integrado de observabilidade, com Dynatrace, SolarWinds, Zabbix e Grafana de forma complementar. São utilizados dashboards de saúde com indicadores diversos aplicados a cada de forma a garantir a disponibilidade e performance de sistemas e infraestrutura.

48. A CPFL possui um historiador corporativo já em operação que possa ser utilizado pela solução (por exemplo, historiador de SCADA/telemetria/SOE)? Em caso positivo, por favor informar qual produto/sistema é e como ele pode ser acessado de forma suportada (ex.: API/SDK, consultas SQL/ODBC, OPC/HDA, exportações, arquivos, fila/mensageria), incluindo quais dados estão disponíveis (SOE, alarmes, analógicos, qualidade etc.), limites de uso (taxa de consultas, janelas de tempo, concorrência, quotas)?

R.: A CPFL-T possui historiador que registra SOE, alarmes, analógicas, qualidade etc. Há a possibilidade de um dump para a exportação inicial dos dados. A arquitetura para o sincronismo ou API para coleta de dados deve compor a proposta e será validada pelo time de arquitetura e segurança cibernética da CPFL.

49. Em qual modelo de implantação a solução pode/deve rodar: on-prem (centro de dados da CPFL), cloud privada e/ou cloud pública (Azure/AWS/GCP)? Se cloud pública for permitida, em qual modelo (IaaS/PaaS/SaaS) e qual provider é aceito/preferencial? Se cloud não for permitido, teremos de listar os equipamentos a serem adquiridos ou usaremos recursos já disponíveis no centro de dados da CPFL? Há possibilidade de ser híbrido? Qual a possível razão para um ambiente híbrido? A infraestrutura estará no mesmo domínio que o SCADA ou em zona segregada com DMZ e data diodes?
    R.: É escopo do projeto propor a infraestrutura necessária conforme estratégia de solução. Para o caso de necessidade de utilização de infraestrutura on premisses CPFL a mesma precisa ser especificada, e proposta pelo projeto para que seja avaliada a disponibilidade ou estratégia de ampliação. De todo modo, a proposta será validada pelo time de tecnologia da informação da CPFL.

50. Em aquisição/orçamento, o que a CPFL espera que a proponente inclua (servidores, storage, licenças, links, appliances) e há catálogo/fornecedores homologados que possa ser disponibilizado?
    R.: É esperado que o projeto seja autocontido durante o prazo de execução, ou seja todo recurso utilizado precisa ser adquirido ou custeado pelo projeto. Eventuais parcerias nesse sentido para compor a proposta, também são de responsabilidade dos parceiros.

51. Existem limitações para uso de ferramentas open-source por razões de segurança/compliance (ex.: exigências de hardening, SBOM, versões suportadas, restrições de licença)?
    R.: Cabe ao projeto propor a solução a qual será avaliada pelo time de segurança cibernética, e submetida a testes de vulnerabilidade.

52. Existirão ambientes separados ao longo do ciclo de vida (dev/homolog/pré-prod/prod)? Quais exatamente serão disponibilizados/exigidos? Qual o mínimo e/ou o ideal? Quem provisiona e mantém cada um dos ambientes (CPFL ou a proponente) e quais são as responsabilidades de cada parte (infra, rede, segurança, backups, observabilidade)?
    R.: Durante o ciclo de vida do projeto o ambiente será provido e mantido pelo proponente. O qual deve avaliar melhor arquitetura, e propor para avaliação. Por padrão a CPFL possui ambientes Produtivos de Desenvolvimento e políticas de backup. Além disso, o ideal seria ter ambientes de Desenvolvimento,

Qualidade e Prod. O ambiente de QA deverá ser o detentor da versão mais atualizada e consolidada, sendo necessário que o pacote esteja fechado e já atualizado na branch correta. Provisionamento de ambientes CPFL são de gestão de um fornecedor da CPFL, ambientes de plataformas SaaS ou PaaS são de gestão da fornecedora que é responsável pelo contrato.

53. Haverá ambiente de simulação para testes sem risco (SCADA simulado e/ou replay de eventos)? Em caso positivo, qual o nível de fidelidade esperado e quais dados/mecanismos estarão disponíveis para simulação/replay? Em caso negativo, a proponente terá de criar as réplicas destes serviços ou a CPFL vai tratar isso de alguma outra forma?
    R.: Existe para o SCADA um ambiente de simulação utilizado para treinamento. A utilização deste ambiente para simulação / teste precisa ser proposta para avaliarmos junto ao CEPEL.

54. Há restrições corporativas obrigatórias de tecnologia (sistema operacional, banco de dados, runtime, container engine) e é permitido uso de GPU (caso necessário)? Será permitido introduzir componentes de plataforma como Kafka/RabbitMQ, Redis, Elasticsearch/OpenSearch, TSDB como Influx/Timescale, Prometheus/Grafana e há padrões corporativos mandatórios?
    R.: Cabe ao projeto propor a solução a qual será avaliada pelo time de segurança cibernética, e submetida a testes de vulnerabilidade.

55. Quais são as exigências de segregação entre IT, OT (incluindo restrições de conectividade, tráfego e integrações entre as redes) e outras redes? Que tipo de acessos são permitidos? Podemos solicitar liberação de algum tipo de acesso específico? Qual seria o procedimento e o tempo necessário para isso? Seria interessante compreender minimamente a topologia com a qual teremos de trabalhar, os limites de tráfego entre esses segmentos e os processos burocráticos da CPFL para as atividades mais comuns: solicitação de acesso, liberação de origem/destino/porta, solicitação de verificação de problemas de conectividade etc.
    R.: Cabe ao projeto propor a solução a qual será avaliada pelo time de segurança cibernética, e submetida a testes de vulnerabilidade.

56. Qual é o processo e o tempo típico para liberação de acesso dos profissionais da proponente? Qual é o processo e o tempo típico de aprovação para adoção de novas tecnologias/componentes (incluindo avaliação de segurança/compliance)?
    R.: Para acessos o SLA é de 3 dias solicitados via ITSM CPFL. Para novos sistemas ou arquiteturas é preciso submeter a avaliação de arquitetura e segurança cibernética. Proposições de novas tecnologias dependem de um

estudo da arquitetura e também de SI para possíveis riscos. A avaliação de propostas também vai incluir a aceitação de tecnologias.

57. Como funcionará o acesso remoto para operação e desenvolvimento (VPN/bastion/jump server, MFA, perfis/segregação de acesso) e quais são as restrições para dados sensíveis (ex.: classificação, mascaramento, auditoria) e para tráfego/armazenamento fora do Brasil (data residency)?
    R.: Acesso via VPN, para acesso a servidor CPFL; para acesso a servidor utilizamos a plataforma senha segura; todos os acessos utilizam MFA.

58. Existe inspeção TLS/SSL no caminho que possa impactar certificados (ex.: MITM corporativo), e como deve ser o modelo de certificados: quem emite/gerencia (CPFL, proponente ou colaboração), requisitos de CA, rotação, e onde os certificados devem ficar armazenados?
    R.: Para o caso de outra estratégia de acesso pode-se empregar o uso de certificado.

59. Existe janela de manutenção planejada para rede/SCADA (frequência e horários) que deva ser considerada para deploys, testes e mudanças? Alguma outra atividade frequente que possa impactar nas atividades de desenvolvimento?
    R.: Do ponto de vista da Operação, as atualizações devem ser realizadas preferencialmente fora das seguintes janelas 07:30-10:30; 14:00-15:30; 16:30-18:00. há janelas de parada técnica toda a semana agendadas nas quartas ou quintas feiras para troca de base de pontos SCADA.

60. Quais são os parâmetros típicos e de pior caso de conectividade entre a solução e o SCADA (latência e banda disponível), existe redundância de links e como é tratada queda parcial/intermitência (failover, degradação, reprocesso)?
    R.: Existem sites redundantes; os links existentes suportam a aplicação sem degradação.

61. Quais requisitos de continuidade/contingência e DR devem ser atendidos (RPO/RTO), e qual deve ser o comportamento em falha para garantir fail-safe: em caso de indisponibilidade da solução, o operador consegue voltar ao processo manual/SCADA sem perda de rastreabilidade e sem risco operacional (e como isso deve ser implementado/validado)?
    R.: Os servidores SCADA funcionam de forma redundante em 2 sites e 2 servidores por site. Com estratégia de sincronização nativa intra site.

62. Em relação a comandos/ações operacionais: é permitido enviar comandos automaticamente ou apenas com confirmação humana? Quais intertravamentos e regras de segurança "hard rules" são obrigatórios e nunca podem ser violados (incluindo validações pré-comando e bloqueios por condição)?
    R.: A solução deve ser desenhada pensando-se sempre nessa interação sugestão-confirmação humana, não se espera uma execução autônoma por parte do software. Do ponto de vista elétrico, a reposta é sim, existem intertravamentos e condições lógicas que devem ser respeitados – todas essas lógicas devem mapeadas durante o desenvolvimento da solução.

63. Existem requisitos formais de segurança OT a cumprir (ex.: IEC 62443, políticas internas "NERC-like" ou equivalentes), incluindo controles mínimos obrigatórios (hardening, segmentação, contas, gestão de vulnerabilidades, logging) aplicáveis à solução?
    R.: Seguimos políticas internas que compartilharemos para a execução do projeto. De todo modo, deve ser seguido IEC 62443 e todas as normativas de cibersegurança previstas no ONS/ARCiber.

64. Quais eventos precisam ser auditados e com que nível de detalhe (cada recomendação gerada, cada clique/ação do operador, cada comando enviado ao SCADA, alterações de configuração/modelo/regras), e quais são os requisitos de retenção e imutabilidade dos logs, além de requisitos de consulta/exportação para auditoria?
    R.: A operação do sistema de transmissão em âmbito nacional é extremamente regulada, portanto, cada sugestão por parte da solução, clique, comando, alteração de topologia e regras devem ser mantidos (guardados) por no mínimo 5 anos.

65. Qual é o modelo de autenticação e autorização exigido (IAM corporativo: AD/LDAP/SSO), há exigência de MFA e quais são os perfis/roles típicos esperados (operador, supervisor, engenharia, manutenção, auditor etc.)? Existe necessidade de segregação/visibilidade por regional (RBAC/ABAC por região)?
    R.: SSO integrado ao Azure AD para o ambiente corporativo, operativo deve ser proposto no escopo do projeto para validação de S.I. As roles também deverão ser avaliadas durante o projeto dado o nível de perfis que serão necessário a criação. A ferramenta deve permitir possível criação de perfis.