ÍNDICE DE REVISÕES

REV.	DESCRIÇÃO E/OU FOLHAS ATINGIDAS
0	EMISSÃO ORIGINAL
A	REVISADO ONDE INDICADO. PARA COTAÇÃO / COMPRA IN-5240-24-441

	REV. 0	REV. A	REV. B	REV. C	REV. D	REV. E	REV. F	REV. G	REV. H
DATA	24/07/2024	09/01/2026							
PROJETO	REFAP	REFAP							
EXECUÇÃO	ZOZULA	MOLINARO							
VERIFICAÇÃO	LEONARDO	LUCAS							
APROVAÇÃO	LEONARDO	LEONARDO							

AS INFORMAÇÕES DESTE DOCUMENTO SÃO PROPRIEDADE DA PETROBRAS, SENDO PROIBIDA A UTILIZAÇÃO FORA DA SUA FINALIDADE.

FORMULÁRIO PERTENCENTE À PETROBRAS N-381.

SUMÁRIO

1. OBJETIVO 3
2. DOCUMENTOS DE REFERÊNCIA 3
3. DISPOSIÇÕES GERAIS 4
4. ESCOPO DE FORNECIMENTO 7
5. REQUISITOS GERAIS PARA O SIS 8
6. REQUISITOS TÉCNICOS DOS EQUIPAMENTOS E SOFTWARES 11
7. PROJETO DO PAINEL SIS (1248-SIS-21) 19
8. TESTE DE ACEITAÇÃO DE FÁBRICA (TAF) 27
9. SERVIÇOS DE CONFIGURAÇÃO E CAMPO 30
10. TESTE DE INTEGRAÇÃO DOS SISTEMAS 30
11. TESTE DE ACEITAÇÃO DE CAMPO (TAC) 31
12. VALIDAÇÃO DE SEGURANÇA PRÉ-PARTIDA 33
13. DESENHOS E DOCUMENTAÇÃO 33
14. SOBRESSALENTES 34
15. GARANTIA 35
16. REQUISITOS DE QUALIDADE INDUSTRIAL 35
17. TRANSPORTE DOS EQUIPAMENTOS 36
18. SERVIÇOS NAS INSTALAÇÕES DA REFAP 36
19. ANEXOS 37

1. OBJETIVO

Esta Especificação Técnica tem por finalidade determinar as premissas básicas para fornecimento e comissionamento do novo painel – 1248-SIS-21 (Painel de Sistema Instrumentado de Segurança) no site da Refinaria Alberto Pasqualini (REFAP) em Canoas - RS.

2. DOCUMENTOS DE REFERÊNCIA

Sempre que explicitamente especificado, prevalecerão os dimensionamentos, concepções e procedimentos contidos nas especificações ou normas da PETROBRAS. Quando não for explicitamente especificado, e para os assuntos não abrangidos pelas Normas Brasileiras da ABNT, prevalecerão as normas do IEC e IEEE. Caso os equipamentos ou materiais não sejam abrangidos pelas normas acima, o proponente poderá utilizar a norma do país de origem, devendo encaminhar cópia da mesma junto com as demais documentações.

2.1. PADRÕES NORMATIVOS, PROCEDIMENTOS E INSTRUÇÕES DE TRABALHO

2.1.1. Normas ABNT

- NBR-5410 – Instalações elétricas de baixa tensão.

2.1.2. Normas Internacionais

- IEC 60079-1 - Explosive atmospheres – Part 1: Equipment protection by flameproof enclosures "d";
- API RP 552 Transmission Systems;
- IEC 61508 Functional Safety of Electrical/ Electronic Safety Related Systems;
- IEC 61511 Functional safety - Safety instrumented systems for the process industry sector;
- IEC 60529 - Degrees of Protection Provided by Enclosures (IP Code);
- IEC 61131-2 - Industrial-process measurement and control – Programmable Controllers – Part 2: Equipment requirements and tests;
- IEC 61131-3 Programmable Controllers – Part 3: Programming languages;
- API RP 2218 - Fireproofing Practices in Petroleum and Petrochemical Processing Plants;
- IEC 60331 - Tests for Electric Cables under Fire Conditions - Circuit Integrity, parts 1 and 11;

- IEC 62443 – Industrial communication networks – Network and system security;
- IEC 61000 - Electromagnetic Compatibility (EMC);
- IEC-61918 - Industrial Communication Networks – Installation of Communication Networks in Industrial Premises.

2.1.3. Normas brasileiras

- NR-10 – Segurança em instalações e serviços em eletricidade.

2.1.4. Normas Petrobras

- N-381 – Formulário para emissão de documentos técnicos de engenharia;
- N-1710 - Codificação de Documentos técnicos de Engenharia;
- N-1735 – Pintura de Máquinas, Equipamentos Elétricos e Instrumentos;
- N-1882 - Critérios para elaboração de Projetos de Instrumentação;
- N-1883 - Apresentação de Projeto de Instrumentação/Automação;
- N-2595 – Critérios de Projeto, Operação e Manutenção de Sistemas Instrumentados de Segurança em Unidades Industriais;
- N-2933 – Automação de sistemas elétricos – Requisitos de projeto, equipamentos, testes e comissionamento;
- ET-5000.00-0000-800-PDI-0001 - Critérios de Projeto de Engenharia - Instrumentação e Automação;

2.2. INTRODUÇÃO

O sistema de intertravamento e controle da caldeira D-321 é obsoleto – dado basicamente através dos painéis 1248-PN-02 (Painel de Relés) e 1248-ACN-01 (Gabinete SDCD).

Considerando que o sistema de vapor é fundamental para o funcionamento da refinaria e qualquer parada inesperada de caldeira implica em prejuízos diretos para a produção, foi decidido pela implementação de novo sistema de intertravamento e controle. Tal melhoria eleva o nível de segurança e confiabilidade praticado no Refino, além de garantir, até onde for possível, que uma caldeira não seja desligada acidentalmente por falha do sistema de segurança ou controle.

3. DISPOSIÇÕES GERAIS

3.1. CONSIDERAÇÕES ADICIONAIS / PREMISSAS

São parte integrante desta Especificação Técnica os documentos listados no item 2 (Documentos de Referência), nas versões vigentes no momento da apresentação da proposta. Propostas baseadas em versões superadas dos documentos listados devem ser tratadas como desvios.

A Especificação Técnica deve ser atendida de forma integral. Quando houver divergência entre requisitos constantes nos documentos, a PETROBRAS deve ser consultada e determinará qual requisito deve prevalecer.

Os requisitos aqui descritos são de caráter mínimo, não eximindo o fornecedor da total responsabilidade e garantia de todas as características construtivas e de desempenho do sistema sobre os itens de sua responsabilidade.

O fornecedor deve declarar explicitamente em sua proposta técnica, em item próprio intitulado “desvios ou alternativas”, qualquer desvio de atendimento a esta Especificação Técnica. A não declaração de desvios durante a fase de propostas será considerada como confirmação de atendimento integral aos requisitos.

A PETROBRAS se reserva o direito de recusar, a qualquer tempo, equipamentos e material que não atendam aos requisitos mínimos desta Especificação Técnica ou que apresentem desvios que não tenham sido explicitamente declarados pelo fornecedor durante a fase de propostas e aceitos pela PETROBRAS através de parecer técnico.

O fornecedor do sistema, na etapa de Parecer Técnico, deve informar as necessidades de aterramento para o sistema que está ofertando, para que REFAP possa avaliar a disponibilidade em suas instalações.

O fornecedor do sistema, na etapa de Parecer Técnico, deve informar as necessidades de alimentação elétrica para operação do sistema, para que REFAP possa avaliar a disponibilidade em suas instalações.

O fornecedor, na etapa de Parecer Técnico, deve informar quaisquer necessidades de apoio da equipe de manutenção, operação, automação da REFAP. De forma, que o planejamento REFAP disponibilize recurso para estes apoios.

No que tange ao Executor de Lógica do SIS, esta especificação atende a norma Petrobras N-2595. Esta especificação define os requisitos mínimos do Executor de Lógica do SIS. Recursos alternativos podem ser propostos como opcionais.

Como o conceito aplicado no projeto, prevê que sinais críticos / de intertravamento são sempre do tipo “hardwired”. Sinais compartilhados entre sistemas via rede são aplicados apenas para monitoração e status.

O fornecedor deverá comprovar com certificados da TUV Renhiland o atendimento a norma IEC 61508 para aplicações SIL 3 e certificados de pessoal qualificado para execução com certificado FSeng ou CFSE.

Na etapa de Parecer Técnico, proponente deve enviar Certificados de atendimento a IEC 61508, bem como, relatórios anexos.

3.1.1. Considerações sobre a alimentação elétrica

- Alimentação AC
  - Uma alimentação 127 Vca (auxiliar) não redundante para iluminação, tomada de serviços e ventiladores.
- Alimentação DC
  - Duas alimentações 125 Vcc redundantes para alimentação do hardware;
  - A alimentação 24 Vcc necessária para os equipamentos do sistema deve ser derivada da fonte de entrada em 125Vcc.

3.2. LOCAL DE INSTALAÇÃO

Localização:

- A REFAP localiza-se na Av. Presidente Vargas, nº 11001, no município de Canoas/RS.

Dados meteorológicos:

- Temperatura ambiente:
  - Mínima: 2ºC;
  - Normal: 19ºC;
  - Máxima: 41ºC;
  - Média das máximas: 38,8ºC;
  - Média das mínimas: 8,7ºC.
- Umidade relativa do ar:
  - Valor médio: 75,9%;
  - Média mensal máxima: 98,8%;
  - Média mensal mínima: 56,7%.
- Altitude: 13,00.

Local de Instalação do PN:

- Dentro da Sala de Painéis da CAFOR, em ambiente fechado e protegido de chuva, com temperatura média de 30°C, sem sistema de refrigeração, ventilação forçada e exaustão;

- Classificação de área: Não Classificada;
- Ambiente suscetível a interferências eletromagnéticas com uma intensidade de campo elétrico de 10V/m em uma faixa de frequências de 26 MHz a 1000 MHz.

4. ESCOPO DE FORNECIMENTO

Um novo painel de SIS (1248-SIS-21), responsável por controlar e monitorar as variáveis críticas de processo da caldeira D-321. O novo painel de SIS microprocessado substitui o painel de relés (1248-PN-02) obsoleto, que atualmente, realiza os intertravamentos de processo da caldeira de CO.

O sistema ofertado deve ser capaz de se comunicar com a rede de automação superior para monitoração, através de protocolo Modbus TCP/IP e Modbus RTU.

O seguinte deve ser considerado:

- Painéis para suportar e interconectar os módulos;
- Módulo de processador;
- Módulos de comunicação;
- Módulos de I/O + Terminal Blocks (Borneiras de terminação);
- Módulos de fonte de alimentação;
- Cabos diversos para conexão entre equipamentos;
- Elementos de proteção dos circuitos como: disjuntores, bornes seccionadores, isoladores ópticos, fusíveis e etc;
- Todos os elementos de rede e conexão (cabos, multicabos, fibras-ópitcas, conversores, sensores, switches, etc.) necessários para a integração e interligação do Executor de Lógica entre seus próprios módulos;
- Software para a comunicação e configuração do Executor da Lógica;
- Serviços de configuração;
- TAF de hardware e software.
- TAC;
- Treinamentos;
- Sobressalentes para partida (conforme item 14);
- Serviços de integração total ao sistema de automação da REFAP;
- Serviços de integração total ao sistema de manutenção da REFAP.

Não fazem parte do escopo de fornecimento:

- Serviços de montagem em campo;
- Lançamento de cabos e interligações;

- Instalação dos PNs;
- Montagem de Andaimes;
- Demais itens não constantes nesta especificação.

5. REQUISITOS GERAIS PARA O SIS

5.1. REQUISITOS DE CONFIABILIDADE

O Executor da Lógica fornecido deve ser um sistema baseado em microprocessador de alta confiabilidade e disponibilidade, com capacidades de autoteste e autodiagnóstico, em conformidade com a norma IEC 61508. Deve ser aprovado por entidade certificadora reconhecida internacionalmente para o uso em aplicações que exijam nível de integridade SIL 3 (IEC 61508) e mantendo a certificação SIL3.

Qualquer falha singela no Executor da Lógica não deverá afetar a disponibilidade de segurança do sistema e ele deverá continuar a operar sem qualquer restrição de tempo e manter, no mínimo, a certificação SIL3. Os módulos de IO e CPU devem atender tripla redundância.

O critério de votação da disponibilidade operacional de cada módulo de IO e CPU deverá seguir a regra de degradação de seus circuitos em 3-2-1-0. Em outras palavras, o módulo não incorrerá em sua falha operacional até que todos os seus circuitos estejam em falha.

Cada equipamento eletrônico microprocessado que compõe o SIS deverá ter como base um projeto com um microprocessador tolerante a falhas, que proteja o processo sob controle contra falhas de sistema intermitentes, transitórias ou permanentes.

Os dados e cálculos que garantem a tolerância a falhas devem ser certificados por uma agência de terceiros independente e com credibilidade internacional.

Deve ser possível substituir e reparar qualquer um dos componentes do Executor da Lógica sem incorrer em qualquer degradação de segurança do sistema ou exigir um desligamento dele (hot swapping). O reparo não deve causar interrupção no processo de leitura (scan) das entradas nem congelar as saídas. Nenhuma ação do operador que não seja a substituição de módulos deverá ser necessária para retornar o sistema para operação normal. A substituição dos módulos (hot swapping) deve ocorrer sem a necessidade de conexão de cabos para realizar a troca, deve ser executada através de slot adjacente ao módulo em seu próprio chassis.

Os módulos de CPU triplo redundantes devem ser dispostos em invólucros separados um a um, de tal forma que permita a substituição (hot swapping) do circuito em falha de maneira individual, substituindo apenas aquele que estiver em falha.

5.2. CERTIFICAÇÃO DE ANÁLISE DE SEGURANÇA

Interfaces entre o Executor de Lógica SIS e outros sistemas devem ser minimizadas. A implementação da segurança cibernética no Executor de Lógica SIS deve estar em conformidade com a IEC 62443 e anteder no mínimo Security Level 1 (SL1) conforme IEC 62443-4-1. Estar aderente também a ISASecure EDSA 311:2010 e ISASecure EDSA 312:2010.

Caso seja necessária a comunicação com o SDCD ou outro sistema deverá ocorrer por "conduit (IEC 62443)" totalmente independente de outro sistema e dedicado, sem outros elementos na mesma rede. Deverá utilizar protocolo aberto e conhecido de fácil monitoração, MODBUS TCP e RTU.

Estações de Engenharia ou de Manutenção temporárias (por exemplo, laptops de fornecedores) não devem estar conectadas ao Executor da Lógica SIS até que tenha sido verificado que o software antivírus está instalado e totalmente atualizado e que uma verificação completa do sistema tenha sido realizada mostrando que mesmo está livre de malware / infecção. A comunicação com a estação de engenharia ou de manutenção deve permitir comunicação por criptografia com uso de Certificados privados.

O Executor da Lógica do SIS deve estar sujeito aos seguintes controles de acesso:

- Físico - por gabinete trancado com chave;
- Lógico - por meio de uma senha forte.

5.3. TESTES AUTOMÁTICOS E DIAGNÓSTICOS

O Executor da Lógica deve possuir capacidades de autodiagnóstico (integradas nos processadores principais) executadas independentemente dos programas aplicativos e de forma contínua, com capacidade de detecção de falhas até o nível dos canais individuais dos módulos de I/O.

O Executor da Lógica deve incorporar capacidades de autodiagnóstico abrangendo falhas permanentes e transitórias. As falhas devem ser identificadas, alarmadas e reportadas ao SDCD.

Os autodiagnósticos devem ser capazes de identificar, localizar e relatar no mínimo as seguintes falhas:

- Falha na varredura do processador principal e dos processadores de I/O;
- Falhas no processador principal e nos processadores de I/O;
- Falhas de memória, falhas no clock de tempo real e etc.;
- Falhas de comunicação;
- Discrepâncias de configuração entre o programa aplicativo/sistema operacional e o hardware;
- Falhas nos módulos de I/O;
- Falhas na Interface de I/O ou de endereçamento;
- Discrepância nos sinais de entrada ou saída;
- Detecção de condição de "Stuck on" nas entradas ou saídas discretas;
- Detecção de condição de "Stuck off" de uma saída discreta;
- Falhas de fonte de alimentação ou fusíveis;
- Condições de temperatura excessiva.

A identificação e a localização das falhas e do status devem ser automáticas, visualizadas por meio de indicadores (LED) localizados em cada módulo com alarme de falha comum e status no SDCD por meio de link de comunicação segura redundante.

O Executor da Lógica deve ser auto verificável. O módulo do processador deve executar diagnósticos entre as execuções do programa aplicativo, de forma a não interferir com o ciclo básico de operação de qualquer programa. O diagnóstico on-line deve realizar no mínimo o seguinte:

- Verificar os circuitos de votação e detecção de falhas;
- Votar e verificar todos os controles das memórias RAM e ROM;
- Votar e verificar todas as entradas e saídas;
- Verificar o funcionamento do sistema operacional e programa aplicativo;
- Disponibilizar informações de falhas para o sistema de anunciação do usuário;
- Revelar todas as falhas ocultas detectáveis ou o potencial de uma ocorrência de falha e fornecer aviso suficiente para equipe de manutenção da planta corrigir a situação antes que uma falha no sistema ocorra.

A manutenção deve ser executada por ferramenta sem interferência na lógica do controlador. Não deve existir o risco da ferramenta, mesmo com senha, alterar, paralisar ou modificar o processamento do SIS.

Qualquer componente de comunicação redundante (cabo, interfaces etc.) deve ser testado automática e periodicamente para garantir que eles não estejam fora de serviço e um alarme no SDCD deve ser gerado em caso de falha.

6. REQUISITOS TÉCNICOS DOS EQUIPAMENTOS E SOFTWARES

6.1. REQUISITOS GERAIS DE HARDWARE

O hardware do Executor da Lógica deve obedecer às seguintes especificações, pelo menos:

- Totalmente composto por dispositivos eletrônicos de estado sólido com projeto modular, consistindo em placas de circuito impresso com os componentes eletrônicos;
- Todos os módulos devem estar equipados com bloqueio mecânico para evitar a inserção incorreta e equipados com dispositivos para fácil remoção;
- Cada módulo deve conter LEDs indicando o respectivo estado operacional;
- Placas de circuitos impressos tratadas para evitar o aparecimento de fungos ou danos causados por umidade ou oxidação (ou seja, tropicalização);
- Todos os módulos devem ser intercambiáveis a quente sem afetar a funcionalidade de saída do Executor da Lógica;
- Os circuitos devem ter sido submetidos a um processo de envelhecimento durante a fase de fabricação;
- Os circuitos devem ter sido concebidos de modo a evitar que uma possível falha em uma placa de circuito impresso se propague e induza outro tipo de falha nas demais placas;
- Os cartões deverão possuir proteção por sobrecorrente independente para cada cartão;
- Aterramento apropriado para proteger contra os efeitos de surtos de eletricidade estática;
- A operação do Executor da Lógica não deverá ser afetada por quaisquer transientes e ruídos elétricos presentes normalmente em grandes sistemas industriais;
- Abaixo estão descritos os quantitativos e folgas de alguns itens específicos que deverão ser fornecidos:

Item	Básico	Folga Instalada (*)
Painel	70%	30%
I/O do executor de lógica	Conforme item 7.3	Conforme item 7.3
Memória e Capacidade de processamento do Executor de Lógica	60%	40%
Capacidade de comunicação do Executor de lógica	60%	40%

(*) As folgas instaladas apresentadas neste documento são mandatórias em relação as informações de mesmo tipo citadas em documentos de referência.

6.2. REQUISITOS GERAIS DO EXECUTOR DA LÓGICA

O Executor da Lógica é o componente SIS que executa as lógicas de aplicação das Funções Instrumentadas de Segurança desejadas. Algumas funcionalidades exigidas, pelo menos, conforme subitens abaixo:

- O Executor da Lógica deve, no mínimo, ser certificado SIL3 por entidade certificadora reconhecida internacionalmente e com uso comprovado em campo por um ano ou mais;
- O Executor da Lógica deve suportar todos os sinais de I/O necessários para o presente projeto e futuras expansões;
- Tanto as entradas de sensores redundantes, quanto as saídas para elementos finais redundantes devem utilizar módulos de I/O distintos;
- O Executor da Lógica do SIS deve manter um clock interno com resolução de 1 milissegundo. Este clock deve poder ser resetado a partir do gabinete do Executor da Lógica ou a partir de uma Estação de Engenharia do SIS. O clock do Executor da lógica pode ser sincronizado por servidor NTP ou SNTP (Ssimple Netwarok Time Protocol);
- A Segurança de Acesso (por exemplo, através de diferentes níveis de senhas, chaves físicas etc.) deve ser implementada para limitar o acesso ao software do Executor da Lógica e assim protegê-lo de modificações não autorizadas ou acidentais;
- O Executor da Lógica deve ser projetado para garantir que o processo não seja reiniciado automaticamente em situações em que a perda de energia tenha resultado em um trip;
- Os componentes do Executor da Lógica devem manter toda sua programação e informação internas em situações de perda de alimentação elétrica, sem a necessidade de reiniciar o sistema;
- O Executor da Lógica deve possuir uma funcionalidade que permita extrair um relatório de testes das malhas de segurança implementadas no SIS;
- A respeito do Hardware do Módulo do Processador, o seguinte deve ser atendido:
    - Cada processador deve ser capaz de executar varredura, atualizar I/Os e executar a lógica implementada, pelo menos 4 (quatro) vezes por segundo;
    - O módulo do processador deve utilizar memória com dados e programa mantida por bateria por até 6 meses;

- A taxa de ocupação da memória do usuário deve ser no máximo de 60% do total. Isso inclui todos os endereços para varredura e atualização de I/Os, todas as variáveis para comunicações com o SDCD e todas as lógicas definidas pelo usuário;
- O módulo do processador em operação, sem interromper ou perturbar o desempenho normal, deve permitir a conexão da Estação de Engenharia para:
  - Forçar entradas, saídas e tabelas de status;
  - Leitura, carregamento, modificação, depuração e impressão do programa aplicativo no modo on-line;
  - Leitura, carregamento, modificação, depuração e impressão de qualquer programa no modo off-line.
- A detecção de estado anormal pelo sistema de autodiagnóstico, levando à falha em uma das CPUs, deve:
  - Isolar o processamento da CPU em falha;
  - Executar rotinas de tratamento de erros;
  - Gerar alarmes de indicação da identificação da falha;
  - Continuar a execução das rotinas de segurança, mantendo a integridade SIL 3 até que seja realizado o reparo;
  - O sistema só deve conduzir as saídas para um status previamente determinado em caso de falha de todas as CPUS do sistema.
- Os processadores principais devem ser redundantes operando em paralelo como uma unidade integrada com cada um dos processadores controlando o barramento de I/O (isto é, a operação dos processadores deve ser transparente para o usuário);
- O módulo do processador deve ser fornecido com backup individual para manter sua memória por seis (6) meses em caso de perda da alimentação elétrica. A degradação da bateria deve ser incluída como parte do alarme de diagnóstico;
- Dois (2) tipos de controles básicos devem ser suportados pelo módulo do processador: lógico e sequencial. Este domínio de controle deve coexistir dentro do processador. Como mínimo, o processador deve conter as seguintes funções configuráveis armazenadas em memória não volátil:
  - Seleção: alta, baixa, média;
  - Computação de Matemática: Adicionar / Subtrair, Multiplicar / Divisão, Raiz Quadrada;
  - I/O: Entrada/Saída Analógica, Entrada/Saída de Contato, Linearização, Raiz Quadrada;
  - Booleano: E, Ou, Nand, Nor, Xor, Nxor;

- Diversos: temporizador, contador de atraso, sequenciador, memória de flip-flop;
- Simbologia Ladder: Contato NA, Contato NF, Módulo de Entrada e Saída Energizado/Desenergizado, Latch/Unlatch, Liga/Desliga Temporizador de atraso, contador, etc.

6.3. REQUISITOS GERAIS PARA INTERFACES E COMUNICAÇÕES DE DADOS

O Executor da Lógica deve ser integrada a rede de automação de processo e manutenção REFAP. Algumas funcionalidades exigidas, pelo menos, estão listadas abaixo:

- O projeto das interfaces de comunicação deve garantir a integridade dos dados e segurança operacional utilizando ferramentas proprietárias, se necessário;
- Os sinais de shutdown entre o Executor de Lógica do SIS e outros sistemas (por exemplo, CCM) e devem ser fiados (hardwired) a fim de atender o determinado na N-2595;
- As interfaces de comunicação devem ser concebidas de forma que a falha das interfaces não afete negativamente a capacidade do SIS de levar o processo a um estado seguro;
- As interfaces de comunicação devem ser projetadas de tal forma que a falha das interfaces não crie uma falha no SIS que causará um desligamento espúrio da unidade de processo;
- Os sinais de comunicação devem prever isolamento óptico para proteção intrínseca de outras fontes de energia que possam interferir com os sinais;
- A interface entre SIS e SDCD deve no mínimo atender ao seguinte:
    - O SDCD deve ler informações do Executor da Lógica (variáveis analógicas e digitais, alarmes, status de eventos, modo e etc.);
    - O SDCD deve permitir a gravação de informações no Executor da Lógica apenas para fins de resets lógicos e by-pass de manutenção;
    - Se a comunicação entre os dois sistemas for perdida durante os modos de Partida ou Contorno para Teste, as informações devem ser retidas no Executor da Lógica, de modo que o SIS mantenha o último valor durante a interrupção da comunicação e durante o restabelecimento das comunicações;
    - Os set-points de pré-trip e trip do SIS devem ser definidos diretamente no Executor da Lógica e não através do SDCD;

6.4. REQUISITOS GERAIS PARA SOFTWARE APLICATIVO E PROGRAMAÇÃO

A seguir, estão alguns dos principais requisitos de projeto para o programa aplicativo, simulações etc., que se aplicam ao projeto do Executor da Lógica, a saber:

- Os requisitos estabelecidos na IEC-61511 devem ser seguidos;
- O programa aplicativo refere-se à lógica implementada no Executor da Lógica baseado em microprocessador, projetada para interpretar as informações dos sensores do Executor e acionar os módulos de saída do Executor da Lógica do SIS para tomar as ações apropriadas descritas na Matriz de Causa e Efeito e nos diagramas lógicos;
- Realizar simulação antecipada da aplicação em fábrica, com o objetivo de simular os cenários de intertravamento num cenário mais realista possível. Assim, minimizar problemas / incompatibilidades de lógica na etapa de comissionamento;
- O Executor de Lógica SIS deve ser fornecido com uma ferramenta integrada (software de programação) para desenvolver, testar e documentar aplicações de segurança e controle crítico. O software deve ser compatível com a norma IEC 61131-3 (Programmable Controllers - Part 3: Programming languages);
- Este software de programação, se necessário, serão instalados nas estações de Engenharia na CIC da Refap. Essas estações vão acessar o Executor de Lógica através da Rede das Estações de Engenharia. Caso o software de programação não seja compatível com as estações mencionadas, uma nova estação deve ser fornecida e instalada no CIC;
- As licenças do software de programação devem ser originais e certificadas pelo fabricante do Executor da Lógica. O mesmo se aplica a qualquer outro software necessário para a operação adequada do Executor de Lógica SIS, tais como: sistema operacional (cliente/servidor), OPC (cliente/servidor), antivírus, etc;
- O programa aplicativo deve usar “Function Blocks” (blocos de função - IEC 61131-3) como linguagem de programação;
- O programa aplicativo deve ser escrito por programadores experientes. O programa aplicativo deve ser formalmente estruturado. A estrutura deve ser projetada para um fluxo claro dos principais caminhos lógicos de modo a facilitar a legibilidade. O programa deve ser claro, conciso e a lógica fácil de ser acompanhada;
- O programa aplicativo deve estar bem documentado. Todos os pontos devem ser claramente descritos e o propósito de todas as seções lógicas ser claramente explicado;
- Os atrasos de tempo (time delays), set-points de trip analógicos e outras variáveis designadas devem ser atribuídos e acessados através de registradores na memória

interna. Essas variáveis devem receber nomes e valores no início do programa. As variáveis devem ser usadas no programa para que seus valores apenas sejam alterados em um local no programa aplicativo;

- O programa aplicativo deve fornecer facilidade para captura do primeiro evento de trip ("first-out") para cada sensor (iniciador de trip) e elemento final. Esta informação deve ser enviada ao SDCD para exibição e alarme, bem como para o Servidor do Sequenciador de Eventos;
- Permitir downloads online;
- Níveis de Revisão:
    - O software padrão do sistema operacional do Executor da Lógica entregue no local de instalação deve estar no nível de revisão testada em campo mais recente e disponível no início do Teste de Aceitação de Fábrica. Salvo indicação em contrário pela Petrobras, o software do sistema operacional do fabricante do Executor da Lógica fornecido no momento da colocação do contrato ou ordem de compra deve ser atualizado para a revisão do TAF antes do início do mesmo;
    - Softwares de terceiros devem estar no nível de revisão de campo mais recente disponível no momento da colocação do contrato ou da ordem de compra. Não serão utilizadas revisões ou atualizações de software após esse período sem aprovação por escrito da Petrobras;
    - O fabricante do Executor da Lógica deve ter disponíveis os softwares conversores necessários para traduzir os dados do sistema e torná-los compatíveis com as novas versões dos softwares do sistema;
    - O programa aplicativo não deve exigir modificações para ser executado em novas versões do software padrão do sistema operacional do Executor da Lógica. Caso sejam necessárias modificações, o fabricante deve dispor da documentação de suporte para que a Petrobras realize o trabalho;
    - O sistema deve fornecer indicação quando houver diferenças nos softwares dos sistemas operacionais de unidades redundantes;
    - Não são permitidas revisões ou atualizações de software após a conclusão do TAF sem a aprovação por escrito da Petrobras;
    - O software padrão do sistema operacional do Executor da Lógica deve criar e manter um histórico de mudanças de programação para itens tais como: módulos, contas de usuários etc. com marcação de hora, usuário que realizou a mudança e motivo da mudança comentado para os seguintes pontos:
        - Mudanças de programação;
        - Diferenças entre diferentes versões de um item de programação;

- Retorno de um item individual ou de toda a base de dados para uma versão anterior;
- Criação de relatórios de gerenciamento de mudanças.

- Todas as mudanças de banco de dados e programação on-line devem ser adicionadas a um arquivo de histórico. Este arquivo deve armazenar pelo menos as últimas 20 mil alterações.

6.5. TESTE E DESVIO

6.5.1. Teste

- Os testes funcionais do SIS têm o objetivo de garantir a integridade das funções de segurança. Os testes funcionais devem incluir o SIS por completo (sensores, executores de Lógica, elementos finais e alarmes associados) e devem basear-se em objetivos claros e bem definidos, responsabilidades e procedimentos escritos;
- O SIS deve ser projetado para acomodar testes periódicos on-line de todos os seus componentes (Sensores para medição de processo, Executor de Lógica, e Elementos Finais) sem interromper o processo;
- O teste on-line dos vários componentes do SIS pode ser realizado em momentos diferentes.

6.5.2. Desvio

- Contornar as entradas do SIS temporariamente inibe a função de segurança. Existem 3 tipos de contornos comumente necessários: Partida, Teste Periódico ou Manutenção/Reparo;
- Os contornos para Partida, quando requeridos, são usados pela equipe de operação para iniciar o processo;
- Os contornos de Teste são usados pelas equipes de operação e de manutenção para testar periodicamente os componentes do SIS: (Sensores, Executores de Lógica e Elementos Finais);
- Os contornos de Manutenção são usados pela equipe de manutenção para realizar manutenção ou reparos em componentes de hardware ou software SIS que estejam fora-de-serviço;
- Todos os contornos devem ser protegidos por senha e devem ter registro de data/hora e usuário;
- A duração do contorno deve estar em conformidade com N-2595. O programa aplicativo do Executor da Lógica deve controlar o tempo de duração do contorno;
- São aplicáveis os seguintes requisitos para os diferentes tipos de contornos do SIS:

- Contorno de Partida: Os contornos de Partida normalmente são usados como condições de trip especificas que precisam ser estabelecidas antes do início do processo:
    a) Os contornos de Partida devem ser projetados para ignorar quaisquer entradas ou saídas do SIS que já estejam presentes antes e durante a partida da unidade de processo, e que caso contrário, impediriam a partida. Normalmente, estas são trips do tipo “Low-Low” de variáveis de processo;
    b) Os contornos de partida devem ser projetados como parte da lógica SIS e não devem consistir em um “force” em determinada entrada (ou seja, onde a lógica SIS é forçada temporariamente para um estado desejado por ação humana deliberada usando o programador do Executor da Lógica);
    c) Os contornos individuais de Partida devem ser ativados usando a IHM do SDCD;
    d) Os contornos de Partida devem sempre ser fornecidos com alarmes e mensagens adequados para avisar os operadores quando os mesmos devem armar as funções de segurança SIS usando a IHM do SDCD;
    e) Os comandos de contorno de Partida devem ser desativados através de funções automáticas, evitando o uso do comando manual para este fim. A filosofia de desativação automática (ou seja, condição de processo e/ou tempo) é definida pela documentação de projeto básico;
    f) O operador deve receber um alarme de aviso antes que o contorno seja desativado, para que este tenha a oportunidade de manter o contorno e estender o temporizador de partida.
- Contorno de Teste / Manutenção: Os contornos para Teste/Manutenção podem ser tipicamente usados para ignorar as condições de trip, para permitir o teste do SIS:
    a) Os contornos de Teste devem ser projetados para ignorar quaisquer entradas do SIS, para fins de teste funcional e calibração do SIS;
    b) Os contornos de Teste devem ser projetados como parte da lógica do SIS e não devem consistir em um “force” em determinada entrada (ou seja, onde a lógica SIS é forçada temporariamente para um estado desejado por ação humana deliberada usando o programador do Executor da Lógica);

c) Os contornos de Testes individuais específicos devem ser ativados usando a IHM do SDCD desde que a chave de contorno de Teste geral da unidade, localizada no Gabinete do Executor da Lógica, tenha sido habilitada;
d) Todos os contornos de Teste devem ser registrados como eventos pelo Servidor do Sequenciador de Eventos e devem identificar os instantes de início e fim do contorno de Teste;
e) As entradas do SIS que foram contornadas para fins de Teste devem ser projetadas com alarmes e mensagens apropriados para alertar os operadores de condições perigosas indesejáveis que podem ocorrer durante o teste das entradas do SIS. As indicações de pré-trip e trip do SIS devem permanecer ativas durante o teste;
f) Contorno de Teste não deve ser desativado automaticamente;
g) Cada O gabinete do Executor da Lógica deve ter uma chave para fins de contorno de Manutenção;
h) Um comando de contorno do SDCD para o Executor da Lógica via Modbus TCP só deverá ser permitido se a chave no gabinete do Executor da Lógica estiver na posição de habilitada.

- Chaves para desvio de intertravamento, em alternativa ao exposto na N-2595 (configuradas na Estação de Engenharia do Executor de Lógica do SIS), podem ser configuradas nas Consoles de Operação do SDCD, desde que a liberação para desvios de proteção ocorra através de acionamento de HS (chave elétrica física) instalada no Console Cego do CIC e interligada por fiação ao Executor de Lógica do SIS. Esta HS somente poderá ser atuada através de chave mecânica do tipo fechadura. Somente com a HS ligada (fecha contato seco interligado à entrada discreta do Executor de Lógica do SIS) fica liberado para Executor de Lógica do SIS receber os sinais das Chaves de Desvio configuradas no SDCD (para desviar proteções ou para remover o desvio de proteções). Para aumentar a segurança, a comunicação digital Executor de Lógica do SIS x SDCD deverá ser realizada através de duas vias distintas, uma para transmissão e outra para recebimento de informações.

7. PROJETO DO PAINEL SIS (1248-SIS-21)

Com base nas definições apresentadas no item 6, realizar a construção do novo Painel de SIS em substituição ao atual painel de relés.

O 1248-SIS-21 será instalado em sala de painéis na Cafor Norte, conforme indicado no item 3.2.

As características construtivas básicas do painel são:

- Dimensões: 800 mm (largura) x 800 mm (profundidade) x 2000 mm (altura) + 100 mm (soleira). Deve ser do tipo “back to back”;
- Os armários deverão ser identificados com plaquetas. O painel do SIS deve possuir identificação diferenciada dos demais. Sugerem-se pinturas parciais do painel na cor alaranjado segurança;
- A construção deverá ser em chapa de aço carbono SAE-1010 / 1020;
- Estrutura do tipo auto-portante; chapas em aço carbono espessura #12;
- Fechamentos superior, laterais em chapa de aço carbono #14;
- Base soleira, em aço carbono espessura #12, cor preto (Munsell) N1,0;
- Porta frontal e traseira com fecho do tipo cremona escamoteável com chave, com ângulo de abertura de 120°;
- Placas de montagem, em aço carbono espessura #12 na cor laranja Munsell 2,5 YR 6/14;
- Acabamento externo, cor cinza Munssell 6,5;
- Grau de proteção IP55;
- Olhais de içamento;
- Acabamento com pintura eletrostática em pó poliéster - Anticorrosiva;
- Entrada e saída dos cabos pela parte inferior, segregados por tipo de sinal, através de flange de cabos;
- Porta documentos;
- Limitador de abertura de porta;
- Cordoalha de aterramento entre porta e painel;
- Terminal de aterramento para cabo de 35 mm²;
- A acomodação dos cabos internos ao painel será feita através de calhas plásticas tipo semiaberta da hellermann ou equivalente, nas dimensões indicadas nos desenhos Anexo.
- As borneiras de terminação devem ser montados em trilhos DIN e/ou Base Plate do fornecedor;
- Os terminais devem ser identificados permanentemente de acordo com o sistema de numeração aprovado pela Petrobras.
- Possuir iluminação interna e tomada de serviço em 127 Vca. Iluminação elétrica com acendimento automático a partir da abertura da porta;
- O painel deve apresentar abertura frontal com visor de acrílico, permitindo a visualização do Executor de Lógica e demais componentes de automação;

- Sistema de ventilação forçada com monitoramento de falha. Possuir venezianas de ventilação e dispositivos de filtragem de ar na parte superior;
- Cada módulo de I/O do Executor da Lógica, com correspondente cabo e borneira frontal, deve ser codificado e identificado de acordo com os diagramas de malhas, de modo a facilitar os procedimentos de montagem, teste e manutenção;
- Todos os canais de entradas analógicas, entradas digitais, saídas analógicas e saídas digitais fornecidos deverão estar conectados às respectivas borneiras frontais, mesmo que não estejam em uso.

7.1. MÓDULOS DE ALIMENTAÇÃO

No interior do PN, deve ser montados sistemas de alimentação com fontes redundantes, conforme descritivo abaixo:

- 2 CONJUNTOS com 2 Fontes 125Vcc / 24 Vcc redundantes para alimentação dos hardware principal do painel (relés, cartões, módulos, switches e etc);
- Módulo diodo redundante;
- A fonte deve ser do tipo chaveada;
- As fontes de alimentação deverão possuir circuito próprio de detecção de falha interna ou oscilação de tensão de saída, com respectivo contato de alarme (1 SPDT mínimo);
- O sistema deve resistir a falhas de energia de até 20 ms sem interrupção da operação;
- A saída da fonte deve ser protegida contra sobretensão, subtensão e surtos, e deve desconectar-se automaticamente caso algum desses eventos ocorra;
- Pelo menos os seguintes elementos devem estar presentes e devidamente identificados no painel frontal:
    - Fusível de proteção de entrada;
    - LED indicador de energia;
    - LED que indica a saída de tensão para outros módulos.
- A falha (curto) em quaisquer um dos carões do CLP não deverá afetar a boa operação dos outros cartões do CLP;
- Todos os circuitos de alimentações elétricas devem ser protegidos por disjuntores termomagnéticos e devem ser dimensionados pelo fornecedor dos painéis;
- Elementos do SIS redundantes (por exemplo, iniciadores, módulos de I/O, elementos finais, por exemplo solenoides) devem ser instalados em chassis separados e devem ser alimentados a partir de diferentes circuitos de energia.

7.2. MÓDULOS DE COMUNICAÇÃO

- O Executor de Lógica deve comunicar-se com o SDCD ABB 1248-ACN-25, localizado na Cafor Norte, através de protocolo Modbus TCP/IP e Modbus RTU, modo redundante. Através desta comunicação, será feito o monitoramento do Executor de Lógica, através do CIC;
- O executor da lógica deve comunicar-se com a rede de automação de manutenção REFAP, através de rede Ethernet, protocolo Modbus TCP/IP, modo simplex.

A interligação dos módulos de comunicação ao SDCD é de escopo REFAP. Fornecedor deve indicar o tipo de porta a ser disponibilizada para tal comunicação. Também deve informar quais as características recomendadas para cabos que fazem esse link, de forma a garantir interoperabilidade do SIS com camadas de automação superiores.

7.3. MÓDULOS DE I/O

Segue abaixo estimativa de I/O (físico) necessários:

- *EA (Entrada Analógica) -> 25 pontos;*
- *ED (Entrada Discreta) -> 127 pontos;*
- *SA (Saída Analógica) -> 4 pontos;*
- *SD (Saída Discreta) -> 103 pontos.*

Para isso, o seguinte está sendo estimado e sugerido quanto a densidades e quantidades, em relação a quantidade de cartões de I/O:

- Três (3) módulos de Entradas Analógica com densidade de trinta e duas (32) entradas analógicas por módulo;
- Um (1) módulo de Saída Analógica com densidade de dezesseis (16) saídas analógicas por módulo;
- Quatro (4) módulos de Entradas Discretas com densidade de trinta e duas (32) entradas discretas por módulo;
- Quatro (4) módulos de Saída Discreta com densidade de trinta e duas (32) saídas por módulo.

No interior do PN, deve ser montados módulos de I/O e demais hardwares de interligação, conforme descritivo abaixo:

- Borneiras de terminação localizadas na parte Traseira do Painel independentes e protegidas por fusíveis (bornes fusíveis) para cada tipo de sinal (Entradas Analógicas, Entradas Digitais, Saídas Analógicas, Saídas Digitais, etc.);

- Cabos para conexão entre módulos de I/O e as borneiras de terminação. As bitolas de cabos devem ser adequadas / consonantes com as recomendações do fabricante do CLP;
- Os módulos de I/O devem ser conectados ao backplane através de um conector de duas partes de alta integridade. O identificador de tipo de módulo deve ser codificado no módulo de I/O e reconhecido automaticamente pelo sistema operacional do Executor da Lógica;
- O Executor de Lógica deve ser capaz de comunicar-se com, pelo menos, 3 (três) backplanes de módulos de I/O com densidades de slots de I/O idênticas. Ou seja, a solução do Executor de Lógica em relação aos I/Os deve ser expansível (ao menos para 250 pontos de I/O analógicos e discretos);
- A inserção de um módulo de I/O errado em um slot de I/O deve ser prevenida por dispositivos de codificação física;
- Onde as entradas possuem dois ou mais sensores independentes para fins de redundância, os diagnósticos de entrada devem ser incluídos no programa aplicativo. Os sinais de sensores redundantes devem ser atribuídos a módulos de I/O distintos. Como requisito mínimo, quando vários sensores forem usados, uma falha de uma entrada de campo não deve desativar qualquer outra entrada, e o reparo on-line deve ser possível;
- Deve ser fornecido isolamento ótico, com tensão de isolamento de no mínimo de 1.000 Vcc, entre cada canal de entrada / saída e o processador;
- Os módulos devem estar providos de LEDs para indicação de estado;
- Cada canal de I/O deve ser protegido com fusível individual, o qual deve fornecer indicação de fusível rompido.

7.3.1. Módulo de entrada analógica

- Cartão com Aplicação HART incorporado por canal;
- O range dos sinais de entrada deve ser 1-5 Vcc @ 1MΩ ou 4-20 mA @ 250 ohms;
- Os módulos vão se comunicar com instrumentos com comunicação a dois (2) e (4) fios;
- Compatível com HART - versão 5,6 e 7;
- Exatidão: melhor do que +/- 0.15% do span;
- “Led” para indicar o estado das entradas;
- Os módulos devem apresentar isolamento galvânico, isolamento por acoplador ótico entre os sinais de entrada e os circuitos internos e proteções contra surtos de tensão e elevação de corrente.

7.3.2. Módulo de saída analógica

- Cartão com Aplicação HART incorporado por canal;
- O range dos sinais de entrada deve ser 1-5 Vcc @ 1MΩ ou 4-20 mA @ 250 ohms;
- Os módulos vão se comunicar com instrumentos com comunicação a dois fios;
- Compatível com HART - versão 5,6 e 7;
- Exatidão: melhor do que +/- 0.15% do span;
- “Led” para indicar o estado das entradas;
- Os módulos devem apresentar isolamento galvânico, isolamento por acoplador ótico entre os sinais de entrada e os circuitos internos e proteções contra surtos de tensão e elevação de corrente.

7.3.3. Módulo de entrada digital

- Entrada DC: 24 Vcc (isolado);
- Devem operar satisfatoriamente com ± 10 % de variação da tensão nominal de alimentação;
- Devem apresentar isolamento por acoplador ótico entre os sinais de entrada e os circuitos lógicos internos (isolamento mínimo de 1500V);
- “Led” para indicar o estado das entradas;
- Os módulos devem apresentar isolamento galvânico, isolamento por acoplador ótico entre os sinais de entrada e os circuitos internos e proteções contra surtos de tensão e elevação de corrente.

7.3.4. Módulo de saída digital

- Saída DC: 24 Vcc (isolado / eletronicamente protegido);
- Todas as saídas digitais devem ser capazes de detectar e alarmar circuitos abertos ou em curto-circuito;
- Se algum sinal de saída do tipo energiza para trip for especificado, deverá ser providenciada capacidade de monitoramento de linha (supervisão);
- “Led” para indicar o estado das entradas;
- Os módulos devem apresentar isolamento galvânico, isolamento por acoplador ótico entre os sinais de entrada e os circuitos internos e proteções contra surtos de tensão e elevação de corrente.

7.3.5. Fiação

- Toda a fiação interna dos gabinetes deve ser encaminhada em calhas de PVC com tampas, convenientemente distribuídas e dimensionadas, considerando, em todos os casos, capacidade de reserva e espaço;
- Todos os cabos e fiação associados ao SIS devem ter uma seção transversal mínima que suporte uma carga elétrica extra de 20%;
- Para a conexão correta da fiação interna devem ser usados conectores tipo garfo, pino ou olho para conectar todos os fios aos terminais, conforme necessário;
- Apenas dois condutores podem ser conectados por terminal, um de cada lado. No caso de serem necessários mais condutores conectados em paralelo, será utilizada uma ponte fixa;
- Todos os cabos, fios e blocos de terminais devem ser identificados de forma fixa, permanente e indelével;
- As fiações CA (127 Vca, 60 Hz.) e CC (24 Vcc, 125 Vcc) devem ser adequadamente identificadas e separadas para evitar tensões induzidas na fiação de CC;
- Para a fiação de sistemas em 127(Vca) utilizar:
  - FASE: Preto - bitola compatível com carga a ser alimentada;
  - NEUTRO: Azul Claro - bitola compatível com carga a ser alimentada;
  - TERRA (PE): Verde - bitola compatível com carga a ser alimentada;
- Para a fiação de sistemas de alimentação Vcc, utilizar:
  - POSITIVO(+): Vermelho - bitola compatível com carga a ser alimentada;
  - NEGATIVO(-): Azul - bitola compatível com carga a ser alimentada;
- Os cabos de fibra óptica serão do tipo:
  - Fibra monomodo, 9/125 µm, 0 – 32.5Km, 16 dB link budget a 1300 nm, A =0 .4 dB/km, 3 dB reserva, D = 3.5ps/(nm x Km);
- Para os fios usados nos diversos gabinetes, considerar:
  - Fio com condutores de cobre estanhados, Classe 5, PVC (Policloreto de Vinila), -40°C a 70°C, 300V/500V (até 1 mm2) // 450V/750V (1,5 mm2 e acima);
- Para os cabos de rede ethernet, considerar cabo CAT6 com conectores RJ-45;

7.3.6. Borneiras

- As borneiras devem ser do tipo de compressão com conexões de braçadeira tubulares e feitos de material não higroscópico;
- As borneiras devem ser montados em trilhos DIN e instaladas em colunas;
- Deve ser garantido um espaçamento mínimo de 100 mm para conexão às borneiras;

- Todos os terminais devem ser do tipo de aperto indireto, com peças metálicas de baixa resistência elétrica e protegidos contra a corrosão, com um isolamento mínimo de 500 V em material termofixo ou termoplástico de alta qualidade;
- Apenas dois condutores podem ser conectados por terminal, um de cada lado. Se houver necessidade de mais condutores conectados em paralelo, uma ponte fixa deve ser usada;
- Os terminais devem ser identificados permanentemente de acordo com o sistema de numeração aprovado pela Petrobras;
- Diferenciação por cores bornes comum e terra;
- Todos os terminais de 127 Vca e 125 Vcc devem ser identificados com etiquetas de advertência adequadas;
- Todas as partes condutoras de terminais expostas com tensões acima de 50 volts devem ser identificadas e possuir tampas de proteção;
- Aplicar bornes do tipo parafuso, dimensionados e identificados, conforme especificidades.

7.3.7. Proteção Elétrica e Aterramento

O painel deve possuir as seguintes características, quanto ao aterramento:

- Barra de aterramento (PE), de cobre com parafusos para conexões estruturais do painel (porta, placa de montagem, etc);
- O ponto de aterramento para os instrumentos e cabos deve ser exclusivo e a conexão deste ponto às barras de aterramento deve ser feita por cabos isolados e independentes para cada barra de acordo com o N-1882;
- As barras de aterramento de aterramento de segurança (PE) e aterramento eletrônico deverão ser segregados. Bem como, as barras de terra eletrônico e segurança intrínseca devem ser isoladas da carcaça do painel;
- As portas articuladas devem ser ligadas ao gabinete principal com tiras de aterramento flexíveis;
- Todos os circuitos de alimentações elétricas devem ser protegidos por disjuntores termomagnéticos e devem ser dimensionados pelo fornecedor dos painéis.

8. TESTE DE ACEITAÇÃO DE FÁBRICA (TAF)

O hardware do Executor da Lógica do SIS e o programa aplicativo devem ser inspecionados e testados na fábrica, ou em instalações de teste, para garantir que foram construídos e configurados conforme o projeto, antes do envio e entrega na unidade.

Nesta etapa, o fornecedor deve realizar simulação antecipada da aplicação em fábrica, com o objetivo de simular os cenários de intertravamento num cenário mais realista possível. Assim, minimizar problemas / incompatibilidades de lógica na etapa de comissionamento.

O objeto do TAF do SIS é garantir e confirmar o seguinte:

- Todos os itens fornecidos, ou seja, hardware, software do sistema operacional, documentação, mídia etc., estão presentes e são aceitáveis;
- O funcionamento correto do SIS de acordo com a especificação funcional, incluindo todas as interfaces para outros equipamentos e subsistemas;
- O sistema irá operar com carregamento simulado durante o período de testes com a disponibilidade prevista no projeto ou melhor;
- O sistema deve ser capaz de tolerar a falha de módulos e subsistemas individuais e ser recuperado para a função completa após o reparo e a reintegração de tais itens.

Os procedimentos propostos do TAF devem ser enviados à Petrobras no mínimo 60 dias antes da data prevista para o início do TAF.

O TAF deve incluir o teste e a aceitação de hardware e software proprietário do sistema. Todo o software proprietário do sistema deve estar completo e residir no Executor da Lógica antes do início do TAF. Toda documentação e listas devem estar livres de mark-ups e comentários.

Todo o equipamento deve ser energizado e permanecer energizado durante o período de testes. Isso inclui qualquer equipamento energizado externamente. As saídas devem ser conectadas a um dispositivo tão semelhante quanto possível ao elemento de campo final (por exemplo, bobina de relé, bobina de válvula de solenoide, etc.) ou equipamento de teste para simular com precisão as condições de operação.

Todos os sinais de entrada cabeados do sistema devem ser testados aplicando um sinal simulado nos respectivos terminais das borneiras de rearranjo e observando o efeito na Estação de Engenharia. As saídas também devem ser manipuladas e o resultado medido novamente a partir dos respectivos terminais das borneiras de rearranjo. Os intertravamentos de segurança devem ser testados um a um.

A versão do programa aplicativo usada deve incluir exemplos de cada tipo de Bloco de Função Personalizado para ser usado no SIS, e testes abrangentes desses Blocos de Função Personalizados devem ser realizados.

TAF deve se convocado com 30 dias de antecedência e apresentar nessa convocação um cronograma das atividades / resumo de testes a executar.

A Petrobras reservará o direito de testemunhar o TAF inteiro como um observador não participante. O procedimento do TAF deve ser assinado pelos participantes, bem como pelos observadores. Uma cópia dos procedimentos do TAF assinados e impressões relacionadas deve ser fornecida à Petrobras na conclusão bem-sucedida do TAF.

A critério da PETROBRAS, a inspeção pode ser feita de modo “presencial” ou “remoto”. Quando em modo “presencial”, o fornecedor deve conceder aos inspetores designados pela PETROBRAS acesso irrestrito às instalações de teste e aos equipamentos. Quando em modo “remoto”, a inspeção deve ser realizada através do sistema Microsoft Teams, ou sistema equivalente de reunião virtual, desde que não implique em necessidade de aquisição de licença e seja homologado pela PETROBRAS. O fornecedor deve dispor, no mínimo, de dois dispositivos com câmera e microfone para utilização simultânea durante a inspeção, e infraestrutura de internet banda larga na área de testes, de modo a garantir a qualidade de comunicação.

O fornecedor deve dispor de mão-de-obra qualificada e infraestrutura adequada para realização de todos os testes previstos, incluindo ferramentas, instrumentos e etc. Toda a comunicação durante as inspeções deve ser feita em português. Caso o TAF seja realizado no exterior, o fornecedor deverá disponibilizar tradutor ou, a critério da PETROBRAS, a comunicação poderá ser realizada em inglês.

Antes de cada ensaio, o fornecedor deve apresentar a lista de instrumentos a serem utilizados e os respectivos certificados de calibração válidos, com rastreabilidade INMETRO. (ou equivalente, caso realizado no exterior).

Caso os equipamentos não atinjam os critérios de aceitação preconizados, a PETROBRAS poderá optar entre permitir a repetição dos testes (mediante justificativa técnica e ação corretiva por parte do fornecedor) ou cancelar do processo de compra unilateralmente, ambos sem ônus para a PETROBRAS.

À PETROBRAS se reserva o direito de dispensar parcial ou totalmente a inspeção, sem prejuízo da obrigação de o fornecedor executar e apresentar os relatórios dos testes previstos com os mesmos critérios de qualidade. Somente serão aprovados os testes testemunhados pelos inspetores designados, ou sem inspetor quando previamente autorizados pela PETROBRAS.

- TAF do hardware:
  - Testes dos Módulos;
  - Rotinas de diagnóstico;
  - Testes de download de software do módulo redundante;
  - Falha de energia e teste de recuperação de módulos redundantes;
  - Falha de energia e teste de recuperação de módulos individuais;
  - Teste de substituição “a quente” (on-line);
  - Teste do sistema de bateria;
  - Teste de partida da alimentação elétrica de emergência;
  - Testes de isolamento da fiação e terminações dos painéis;
  - Verificações de alimentação, fusíveis e aterramento;
  - Teste de continuidade de terra do sistema de segurança;
  - Teste de continuidade de terra dos instrumentos;
  - Teste da redundância da fonte de alimentação;
  - Teste de proteção de sobrecorrente;
  - Teste de proteção de sobretensão de alimentação;
  - Teste de EMC, de emissão e susceptibilidade;
- Testes das I/Os - Todas as I/Os devem ser testadas e todas as respostas da lógica devem ser observadas usando a Estação de Engenharia existente. Os testes de I/O devem garantir que:
  - Todas as I/Os estão corretamente endereçadas e conectadas aos terminais designados das borneiras frontais e de rearranjo;
  - Todas as I/Os são fornecidas com alimentação do circuito de campo a partir das fontes de alimentação do SIS;
  - Todas as entradas respondem corretamente ao circuito aberto e ao circuito fechado nos terminais do campo; Todas as Entradas Analógicas (incluindo contatos monitorados) respondem corretamente em toda a faixa de entrada de sinal (0 - 20 mA) e limites de comutação de contato monitorados (entre o circuito aberto, contato aberto, contato fechado e curto circuito).
  - Todas as saídas monitoradas fornecem resposta de alarme correspondente ao circuito aberto nos terminais do campo;
  - Todas as saídas digitais podem ser forçadas a ligar/desligar a partir da Estação de Engenharia.

Os critérios de aprovação/falha devem considerar um desempenho 100% correto, caso contrário o item defeituoso deve ser consertado ou substituído, sem ônus à Petrobras. Na identificação de uma falha de teste, a Petrobras terá autoridade para interromper todos os testes até que tenham sido implementadas soluções satisfatórias. O reinício do teste será feito após aprovação da Petrobras.

Após a conclusão bem-sucedida do TAF, toda a documentação e desenhos devem ser atualizados para refletir as correções feitas durante o teste.

9. SERVIÇOS DE CONFIGURAÇÃO E CAMPO

Configuração, testes e comissionamento do Executor de Lógica e demais componentes do gabinete onde encontra-se, permitindo o pleno funcionamento do Executor de Lógica;

Elaboração, desenvolvimento, programação, testes e comissionamento da receita a ser operada pelo Executor de Lógica (Funções Instrumentadas de Segurança, intertravamentos, alarmes, watchdogs, monitoramentos etc.), atendendo os documentos de referência e normas desta Especificação Técnica;

10. TESTE DE INTEGRAÇÃO DOS SISTEMAS

Os Testes de Integração dos Sistemas devem ser realizados em campo com todos os sistemas já montados no site de instalação final.

Todas as I/O de todos os sistemas devem ser simuladas através do equipamento de teste para simular com precisão as condições de operação. Devem ser fornecidos os procedimentos de teste, equipamento de teste e pessoal devidamente qualificado para realizar os testes do SIS, incluindo o monitoramento de displays relevantes do SDCD. Todos os erros de configuração no SDCD identificados pelos testes do SIS, ou por outras equipes de teste, devem ser corrigidos.

- Testes Gerais do SIS:
  - Os Testes de Integração dos Sistemas devem ser realizados no SIS completo, conectado ao sistema SDCD completo, além do sistema Fogo e Gás e outros dispositivos, com todas as interconexões equivalentes à configuração final instalada.
- Interfaces para outros sistemas / sub-sistemas:
  - Todas as interfaces de comunicação entre o SIS e o SDCD devem ser devidamente testadas, ou seja, Estações de Engenharia e de Manutenção, Servidor do Sequenciador de Eventos e Servidor do Sistema de Gerenciamento de Ativos, etc;
  - O teste de integração do SIS será conduzido em conjunto com os testes do SDCD com o qual ele deve se conectar, para verificar o funcionamento correto de todas as interfaces;

- Devem ser produzidos procedimentos de teste de integração do SIS, que incluirão critérios de aprovação/falha aprovados pela Petrobras.

- Teste do Software do Sistema de Segurança:
  - Esses testes devem ser integrados com o teste de configuração do SDCD a fim de confirmar que todos os eventos que ocorrem nas entradas do SIS produzem a resposta necessária nas saídas do SIS e as respostas esperadas na tela de operação e de alarmes no SDCD.
  - Os Testes de Integração dos Sistemas também devem confirmar a operação correta de todas as ações do operador que afetam o SIS.
  - Esses testes devem confirmar que a combinação do hardware do SIS, do Programa Aplicativo do Sistema de Segurança e da configuração do SDCD responde de forma a cumprir os requisitos definidos na Especificação de Requisitos de Segurança.
- Teste de Operabilidade - Tempo de Resposta do Sistema:
  - Nas condições acima mencionadas, os tempos de resposta, para as condições simuladas de 50% e 100% de carregamento do sistema, devem ser testados para todos os comandos operacionais comuns do SDCD, e registrados os tempos de resposta em folhas de teste para comparação com as especificações funcionais.
- Testes de gerenciamento de alarmes:
  - Nas condições acima mencionadas, e nas condições simuladas de 50% e 100% de carregamento do sistema, testar o desempenho do processamento de alarmes do sistema SDCD, simulando sobrecargas em etapas de 25%, 50%, 75% e 100% de alarmes configurados e monitorar e registrar a resposta SDCD para comparação com as especificações funcionais.
  - Esses testes devem garantir que, nas condições do pior caso, todas as informações de alarme e status do SIS sejam capturadas de forma confiável pelo SDCD.

Após a conclusão bem-sucedida dos Testes de Integração dos Sistemas, toda a documentação e desenhos devem ser atualizados para refletir as correções feitas durante o teste.

11. TESTE DE ACEITAÇÃO DE CAMPO (TAC)

O objetivo é testar funcionalmente no campo todo o hardware do SIS (Iniciadores, Executor da Lógica e Elementos Finais) e o programa aplicativo associado para garantir a conformidade com a N-2595. O TAC deve ser completado de forma satisfatória e

devidamente documentado perante as condições de desvio operacional para as quais o SIS foi projetado.

Deve ser preparado um procedimento de Teste de Aceitação de Campo (TAC) descrevendo como este deve ser conduzido que deverá ser submetido para a aprovação da Petrobras.

O entregável desta etapa de execução é a execução real do TAC pelo procedimento do TAC. Além disso, um TAC bem-sucedido deve resolver quaisquer discrepâncias entre os resultados esperados dos procedimentos de teste e os resultados dos testes finais reais, e entregar um conjunto completo de listas de verificação assinadas. Um TAC concluído com sucesso indica que o SIS está pronto para operação.

O TAC deve incluir, mas não ser limitado, a confirmação do seguinte:

- A funcionalidade do fornecimento de energia do SIS;
- Os sensores, a lógica, os cálculos e os elementos finais devem estar em conformidade com o SRS. Devem ser feitas a verificação e teste de funcionalidade de 100% da lógica, conforme as tabelas de causa e efeito e diagramas lógicos. Isso inclui a verificação da funcionalidade de todas as operações de pré-parada, de sequência de parada, alarme, reinício, teste e bypass, bem como a precisão de qualquer cálculo, como discrepâncias do sinal do transmissor;
- Os sistemas de desligamento manual funcionam corretamente;
- Funcionalidade de todas as interfaces do Executor da Lógica (Iniciadores, Elementos Finais, SDCD, Estações Engenharia, de Manutenção e demais Comunicações), conforme SRS;
- O intervalo entre testes (totais ou parciais) está documentado em procedimentos de manutenção consistentes com os requisitos do SRS;
- A documentação do SIS para garantir que seja consistente com a instalação e os procedimentos operacionais reais;

Antes da energização do sistema, o fornecedor deve supervisionar a instalação física e interconexões realizadas pela PETROBRAS.

É exigido operação assistida do fornecedor após a partida do sistema em operação normal por no mínimo 5 dias. Neste período o profissional designado para a operação assistida e a empresa contratada deverão prestar toda assistência em caso de ocorrência de alguma anormalidade.

12. VALIDAÇÃO DE SEGURANÇA PRÉ-PARTIDA

A Validação de Segurança Pré-Partida é uma avaliação de segurança final necessária para novas instalações e para instalações modificadas, quando a modificação é significativa o suficiente para exigir um procedimento de Gerenciamento de Mudança. A Validação de Segurança Pré-Partida é a última verificação de que todos os projetos, instalações, procedimentos e treinamento do projeto do SIS são adequados e completos antes do início da partida da unidade de processo. A Validação de Segurança Pré-Partida define um marco de quando o SIS será entregue às operações da Petrobras.

A Validação de Segurança Pré-Partida deve ser realizada antes da entrega do SIS às operações da Petrobras. Esta validação deve ser liderada pela Petrobras com participação ativa dos responsáveis pelo projeto de detalhamento, projeto de construção, projeto de montagem e do fornecedor do Executor da Lógica.

O entregável para esta fase é um relatório de validação de segurança Pré-Partida assinado por pessoal designado pela Petrobras em Operações, Manutenção e Engenharia de Instalações. Isso assegura que todos os desenhos, procedimentos, treinamento e instalações do SIS estejam completos.

13. DESENHOS E DOCUMENTAÇÃO

A documentação de projeto a ser entregue pelo fornecedor deve ser conforme, RM-1248-80-PDF-0006 e documentação exigida na N-2595.

Toda a documentação deverá ser perfeitamente identificada e numerada, de acordo com o padrão do fornecedor e conter as informações da respectiva Requisição de Material emitida para este fornecimento.

Toda documentação do fornecimento, incluindo as propostas para fornecimento e toda a correspondência posterior à assinatura do contrato de fornecimento, incluindo descrições técnicas, desenhos, manuais, relatórios, etc., deverão ser necessariamente escritos em língua portuguesa, a menos que autorizado por escrito pela REFAP. No caso de relatórios de ensaios realizados em laboratórios fora do país (caso forem necessários), os mesmos poderão ser escritos em inglês.

O contratado deverá seguir a norma N-381 informando os casos onde esta norma não poderá ser aplicada.

Toda a simbologia, escalas e sistemas de unidades a serem adotados deverão seguir os padrões dos originais existentes.

O contratado poderá utilizar aplicativos para a elaboração dos desenhos em sistema 3D (três dimensões) desde que o produto final seja uma planta em arquivo com terminação DWG para leitura em AUTO-CAD.

Os desenhos revisados deverão apresentar legenda indicativa da revisão indicando claramente o número da revisão, número do contrato, nome da firma, data da revisão, etc. , conforme padrão já existente nos originais.

Ao final do comissionamento dos Painéis, estando eles operacionais, o fornecedor deve enviar a documentação “as-builtada”.

14. SOBRESSALENTES

Deve ser fornecido um kit de peças sobressalentes recomendadas junto com a entrega do painel para o comissionamento e partida de operação, no mínimo considerando os seguintes itens:

- Módulo de processador;
- Módulos de comunicação;
- Módulos de I/O + Terminal Blocks;
- Módulos de fonte de alimentação;
- Cabos para conexão entre equipamentos;
- Elementos de proteção dos circuitos como: disjuntores, bornes seccionadores, isoladores ópticos, fusíveis e etc;
- Elementos de rede (conversores, switches, etc.);
- Pacote de fusíveis de proteção de cartões, se aplicável

Considerar:

·1 (uma) unidade por modelo (part number) para peças com até 3 unidades utilizadas na montagem do painel;

·2 (duas) unidades por modelo (part number) para peças com 4 à 9 unidades utilizadas na montagem do painel;

·2 (duas) unidades mais 10% (dez por cento) do total de peças de um determinado modelo (part number) utilizados na montagem do painel quando o total de peças utilizados ultrapassar 9 unidades;

Deve ser fornecida uma lista de todas as peças sobressalentes do Executor da Lógica do SIS recomendadas para suporte de operação e manutenção por dois (2) anos.

O fornecedor do Executor da Lógica deve garantir a disponibilidade de todas as peças do Executor da Lógica do SIS e serviços de suporte por dez (10) anos a partir da data de comissionamento. Isso deve incluir peças sobressalentes, serviços de reparação e manutenção, atualizações de software e modificações do sistema

O fornecedor deverá incluir em sua proposta uma “Lista de Peças Sobressalentes para Partida” e uma “Lista de Peças Sobressalentes para dois anos de operação”, incluindo o preço dos componentes. Este item é obrigatório na Proposta Técnica;

O custo desses sobressalentes iniciais deve estar incluso no valor do equipamento.

A lista de sobressalentes deve indicar todos os dispositivos mais relevantes / passíveis de falha. Elencar na lista - descritivo e código “*part number*” do fabricante, para facilitar futuras aquisições e manutenções.

15. GARANTIA

Todo o hardware e software fornecido devem ser garantidos contra defeitos.

Sob esta garantia, o fabricante do Executor da Lógica deve substituir todo o hardware e subsistemas que possuem dualidade devido a dispositivos defeituosos, mão-de-obra, engenharia ou programação durante o período de garantia. O fabricante do Executor da Lógica deve, se exigido pela Petrobras, fornecer o serviço de um técnico experiente para realizar e supervisionar as reparações e substituições necessárias.

Sob esta garantia, o fabricante do Executor da Lógica deve substituir ou corrigir qualquer software fornecido, o que seja considerado defeituoso. Deve ser disponibilizado pessoal qualificado para substituir, corrigir e verificar o sistema.

Na eventual ocorrência de defeitos por qualquer motivo, o fornecedor se obrigará a executar todas as alterações necessárias, reparos e substituições sem ônus para o comprador, inclusive sem ônus de transporte e estadia de pessoal técnico especializado.

16. REQUISITOS DE QUALIDADE INDUSTRIAL

Os equipamentos a serem fornecidos deverão ser novos, ser completos e testados, prontos para serem instalados e utilizados sob regime de operação contínua.

Todos os componentes devem possuir qualidade industrial e com dimensionamento adequado, ou seja, não são admitidos equipamentos cujo projeto submeta os componentes a operação em condições muito próximas a seus limites.

Deverão ser fornecidos com placas de identificação fixadas em local visível e de fácil acesso.

Não serão aceitos equipamentos e componentes que se encontrem em fase de desenvolvimento ou sem consolidação de uso, nem, tampouco, aqueles que já tenham sido descontinuados da linha de produção normal do fabricante.

O fabricante deve informar em sua proposta técnica o período de suporte de peças previsto para os itens ofertados.

O projeto ou know-how devem ter sido empregado em aplicações industriais semelhantes, a ser evidenciado pelo fornecedor na fase de propostas através de documentação.

Todos os equipamentos fornecidos no pacote, devem estar na lista de fornecedores cadastrados / aceitos pela PETROBRAS.

O fornecedor deve comprovar a disponibilidade de fornecimento de sobressalentes originais e de assistência técnica autorizada no Brasil. Equipamentos sem estes requisitos não são aceitos.

17. TRANSPORTE DOS EQUIPAMENTOS

O proponente deverá prever toda a embalagem necessária para o sistema, documentação, materiais auxiliares, sobressalentes, ferramentas, etc. Considerar a identificação “FRÁGIL” quando necessário.

O proponente deverá informar a data de disponibilidade do equipamento com no mínimo 05 (cinco) dias úteis de antecedência.

18. SERVIÇOS NAS INSTALAÇÕES DA REFAP

18.1. MOBILIZAÇÕES

Os serviços nas instalações da REFAP devem ser realizados em datas a serem acordadas entre o cliente e o fornecedor, podendo ocorrer dentro de um período de até 1 (um) ano após o recebimento dos equipamentos na REFAP.

O fornecedor deve planejar os serviços de modo a cumprir todas as tarefas necessárias para o correto comissionamento do sistema, contemplando o tempo de espera para procedimentos de credenciamento de pessoal, para liberação dos serviços e etc.

O fornecedor deve designar profissional tecnicamente qualificado para realização dos serviços, devidamente autorizado nos termos da NR-10 e em atendimento às normas de Segurança e Saúde Ocupacional da PETROBRAS.

O fornecedor é responsável por todas as despesas relativas à realização dos serviços nas instalações da REFAP, incluindo deslocamento de pessoal, hospedagem, diárias, EPIs, ferramentas, instrumentos, etc.

18.2. TREINAMENTO

Devem ser ministrados os seguintes treinamentos, nas dependências da REFAP:

- Treinamento de Operação
  - Conteúdo mínimo: Princípio de funcionamento, procedimentos de partida e parada, manobras, parâmetros de operação e proteção, descrição dos alarmes;
  - Carga horária mínima: 3 (três) turmas de 4 (quatro) horas cada.
- Treinamento de Manutenção
  - Conteúdo mínimo: Idem ao treinamento de operação, acrescido de procedimentos de manutenção preventiva e corretiva, diagnóstico de defeitos e falhas, substituição de componentes, utilização do software, ajuste de parâmetros;
  - Priorizar segregação de treinamentos de manutenção em hardware e software;
  - Carga horária mínima: 3 (três) turma de 8 (oito) horas.
- Treinamento na Aplicação de configuração do programa da caldeira D-321
  - Conteúdo mínimo: Apresentar à equipe de automação todas as rotinas de programação, considerando: blocos aplicados, rotinas especiais em linguagem estruturada, ajuste de parâmetros;
  - Carga horária mínima: 1 (uma) turma de 16 (dezesseis) horas.

Deve ser prevista a participação de até 10 pessoas em cada turma.

As datas e horários do treinamento deverão ser previamente acordados entre PETROBRAS e o fornecedor. A PETROBRAS disponibilizará a sala de aula para a realização dos treinamentos.

19. ANEXOS

Sem Anexos