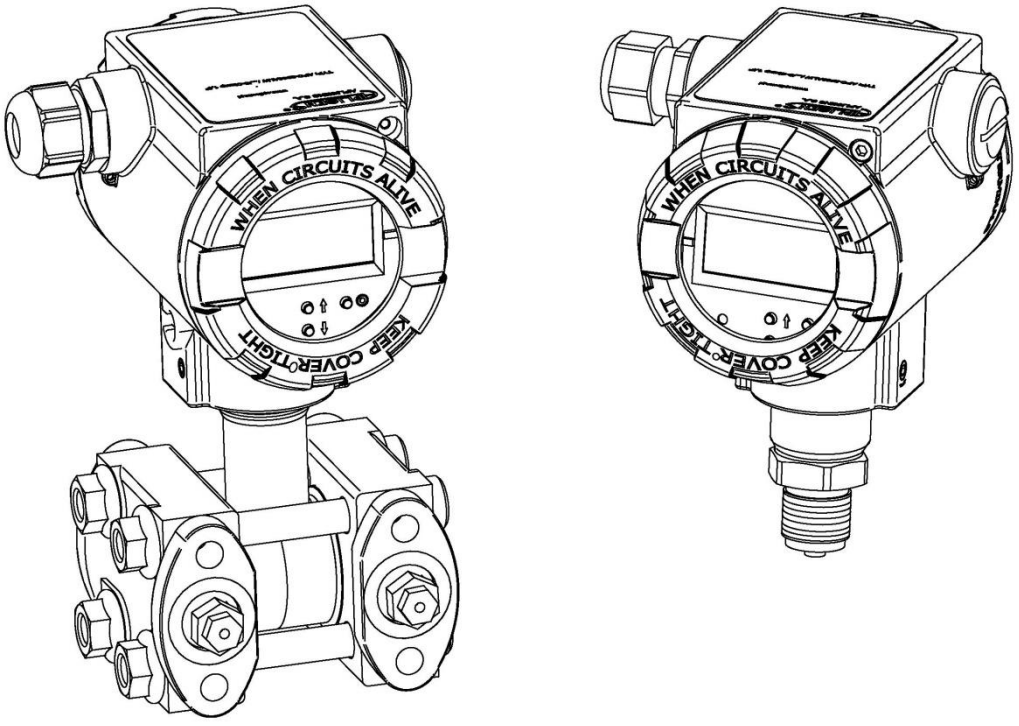
MANUAL DE SEGURANÇA SIL

TRANSMISSORES DE PRESSÃO E DE PRESSÃO DIFERENCIAL

APC-2000ALW Safety
APR-2000ALW Safety

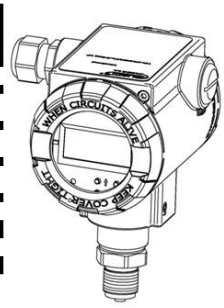


APLISENS S.A., 03-192 Varsóvia, R. Morelowa 7
Tel. +48 22 814 07 77; fax +48 22 814 07 78
www.aplisens.com, e-mail: export@aplisens.com

CÓDIGO DO PRODUTO – ver: secção **5.2. do Manual de Instruções**.
Um código QR ou número de identificação permite a identificação do transmissor e o acesso rápido à documentação no website do fabricante: instruções de funcionamento, instruções de segurança SIL, instruções do dispositivo de construção à prova de explosão, informações técnicas, declaração de conformidade e cópias de certificados.

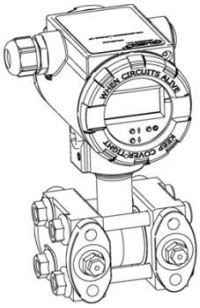
APC-2000ALW Safety (Inmetro Brasil)

ID: 0001 0004 0002 0000 0000 0007 0001 36
https://www.aplisens.pl/ID/000100040002000000000007000136



APR-2000ALW Safety (Inmetro Brasil)

ID: 0002 0004 0002 0000 0000 0007 0001 33
https://www.aplisens.pl/ID/000200040002000000000007000133



Designações utilizadas

Símbolo	Descrição
	Aviso de que as informações contidas na documentação devem ser rigorosamente aplicadas para garantir a segurança e a plena funcionalidade do dispositivo.

REQUISITOS BÁSICOS DE SEGURANÇA FUNCIONAL

O fabricante não será responsável pelos danos resultantes de uma instalação incorrecta do dispositivo, da não manutenção do mesmo em condições técnicas adequadas, ou da utilização do dispositivo para outros fins não previstos.

A instalação deve ser realizada por pessoal qualificado, autorizado a instalar equipamento eléctrico e aparelhos de controlo e medição. É da responsabilidade do instalador realizar a instalação de acordo com este manual e com os regulamentos e normas de segurança e CEM aplicáveis ao tipo de instalação.

Configurar o sistema E/E/PE de segurança de acordo com a sua função. Uma configuração incorreta pode resultar num funcionamento defeituoso, provocando danos no sistema E/E/PE relacionados com a segurança ou um acidente.

Num sistema com instrumentos de controlo e medição, existe um perigo para o pessoal do meio pressurizado no caso de fugas. Durante a instalação, utilização e inspecção do transmissor, devem ser considerados todos os requisitos de segurança e protecção.

Se for detetado um funcionamento defeituoso do sistema E/E/PE relacionado com a segurança, este deve ser desligado da instalação e devolvido ao fabricante para reparação.

A fim de minimizar a possibilidade de mau funcionamento e riscos associados para o pessoal, evitar instalar o equipamento em condições particularmente adversas onde existam os seguintes perigos:

- possibilidade de choques mecânicos, choques excessivos e vibrações;
- flutuações excessivas de temperatura;
- condensação de vapor, pó, gelo.

Os transmissores da série APC(R)-2000ALW Safety para funcionamento em circuito de segurança funcional devem ser configurados para um sinal de saída de 4...20 mA. O protocolo HART ou os botões locais que alteram as definições do dispositivo podem ser utilizados para diagnóstico, bem como para configurar o produto no posto de trabalho. Após a configuração e colocação em funcionamento do sistema de segurança funcional, só deve ser utilizado o sinal de saída de corrente analógico.

As alterações efectuadas na fabricação dos produtos podem preceder a actualização da documentação em papel do utilizador. As instruções de funcionamento actuais podem ser encontradas no website do fabricante em www.aplisens.com.

ÍNDICE

SIL DECLARATION OF CONFORMITY

Document number DZ.APC.APR.ALW.SIL.ID.REV4

Manufacturer: **APLISENS S.A.,**
Morelowa 7 St., 03-192 Warsaw

Declare with full responsibility that:

pressure transmitters
APC-2000ALW Safety ID: 0001 0004 0002 XXXX XXXX XXXX XXXX XX[1)]

differential pressure transmitters
APR-2000ALW Safety ID: 0002 0004 0002 XXXX XXXX XXXX XXXX XX[1)]
[1)] X in the ID code is manufacturer's indication not related to the certificate

meet the requirements of standards:

PN-EN 61508:2010 Part 1÷7
PN-EN 61511-1:2017 + PN-EN 61511-1:2017/A1:2018-03
PN-EN 62061:2008 + PN-EN 62061:2008/A1:2013-06 + PN-EN 62061:2008/A2:2016-01

Products	λ_{total} FIT	λ_{NE} FIT	λ_{SD} FIT	λ_{SU} FIT	λ_{DD} FIT	λ_{DU} FIT	SFF %	DC %	MTBF
APC-2000ALW Safety	905,321	265,723	0	138,208	451,857	49,533	92,256	90,121	1,105x10^6 h 126 Yrs
APR-2000ALW Safcty	919,621	265,723	0	138,208	453,387	62,303	90,472	87,919	1,087x10^6 h 124 Yrs

HFT=0, Route 1_H	SIL 2
HFT=1, Route 1_H	SIL 3
Systematic Capability, Route 1_S	SC 3 (SIL 3 Capable)
Subsystem	Type B

The products can be used in safety-related systems that meet the requirements up to and including SIL 3. SIL verification of a security-related system is the responsibility of the system integrator.

Certificate No. 939/CW/001 was issued by UDT-CERT, Office of Technical Inspection, Szczęśliwicka 34 St., 02-353 Warsaw 06.06.2019.

Warsaw, 27.08.2019

Daniel Samczak
Functional Safety Coordinator

Morelowa 7 St., Warsaw 03-192
phone +48 22 814-07-77 fax +48 22 814-07-78
e-mail: export@aplisens.com
www.aplisens.com

Urząd Dozoru Technicznego
UDT-CERT

CERTIFICATE

No. 939/CW/001

Office of Technical Inspection
Product Certification Body UDT-CERT

certifies that

pressure transmitters
APC-2000ALW Safety ID 0001 0004 0002 XXXX XXXX XXXX XXXX XX[1)]
differential pressure transmitters
APR-2000ALW Safety ID: 0002 0004 0002 XXXX XXXX XXXX XXXX XX[1)]

[1)] X manufacturer's designation in the ID code, not related to the certificate

manufactured by

APLISENS S.A.
ul. Morelowa 7
03-192 Warszawa

satisfy the requirements of the standards

PN-EN 61508:2010 parts 1 ÷ 7
PN-EN 61511-1:2017 + PN-EN 61511-1:2017/A1:2018-03
PN-EN 62061:2008 + PN-EN 62061:2008/A1:2013-06 + PN-EN 62061:2008/A2:2016-01

for safety integrity level

up to and including SIL 3, with a tolerance of hardware faults HFT = 1 according to Route 1_H
up to and including SIL 2, with a tolerance of hardware faults HFT = 0 according to Route 1_H

and satisfy the requirements of systematic integrity

up to and including SC3 according to Route 1_S

Products	λ_{total} FIT	λ_{NE} FIT	λ_{SD} FIT	λ_{SU} FIT	λ_{DD} FIT	λ_{DU} FIT	SFF %
APC-2000ALW Safety	905,321	265,723	0	138,208	451,857	49,533	92,256
APR-2000ALW Safety	919,621	265,723	0	138,208	453,387	62,303	90,472

The products can be used in safety-related systems that meet the requirements up to and including SIL3. SIL verification of a security-related system is the responsibility of the system integrator.

The conditions for issue and validity of the Certificate are specified in the Annex.

Date of issue: **06.06.2019**

SIL CERTIFICATION

Director of Certification and Conformity Assessment Department

Jacek Niemczyk

UDT-CERT, 02-353 WARSZAWA, ul. SZCZĘŚLIWICKA 34

3. DEFINIÇÕES E ABREVIATURAS

SIL – nível de integridade de segurança. Trata-se de um nível discreto, 1 de 4 possíveis, correspondente a uma gama de valores de integridade de segurança, em que o nível de integridade de segurança 4 é o nível mais elevado e o nível de integridade de segurança 1 é o nível mais baixo.

SFF – quota de danos seguros. Percentagem de falhas/danos seguros que não podem causar uma falha do sistema. Quanto maior for o valor, menor é a probabilidade de uma falha perigosa do sistema.

DC – cobertura de diagnóstico. Medida da capacidade do sistema para detetar falhas perigosas. O rácio entre a taxa de falhas perigosas detetadas e a taxa de todas as falhas perigosas no sistema.

PFH – probabilidade de danos perigosos por hora.

PFD_{avg} – probabilidade média de falha da função de segurança no modo de chamada pouco frequente.

MTBF – tempo médio entre danos. Descreve o tempo de funcionamento entre dois danos consecutivas de subconjuntos. A própria indicação MTBF refere-se à fiabilidade do dispositivo.

HFT – tolerância de defeitos do equipamento. A capacidade do dispositivo para continuar a desempenhar a função de segurança requerida, apesar da ocorrência de danos.

MTTR – tempo médio de recuperação. Tempo médio entre a ocorrência do dano e a conclusão da reparação. O MTTR inclui o tempo necessário para detetar um dano, iniciar a ação corretiva e concluí-la totalmente.

MRT – tempo total de reparação previsto (não inclui o tempo para detetar danos).

FMEDA – análise detalhada dos vários modos de falha e capacidades de diagnóstico do dispositivo (Failure Modes Effects and Diagnostics Analysis).

ALARM_L – condição de alarme de diagnóstico em que a corrente I_ALARM_L é inferior a 3,600 mA.

FIT – danos ao longo do tempo. Valor definido como um fator de dano (**λ**) por mil milhões de horas.

λ – fator de intensidade do danos. Determina o número de danos do sistema por unidade de tempo.

λ_{SD} – índice de intensidade de danos seguros detetáveis.

λ_{SU} – índice de gravidade de danos seguros não detetáveis.

λ_{DD} – índice de classe de gravidade de danos para danos perigosos e detetáveis.

λ_{DU} – índice de gravidade de danos para danos perigosos não detetáveis.

λ_{NE} – índice de intensidade de danos sem efeito.

λ_{total} – índice de intensidade de danos (soma de todos os componentes do índice de intensidade do dano).

4. INFORMAÇÕES GERAIS

A função de segurança dos transmissores **APC-2000ALW Safety** e **APR-2000ALW Safety** consiste em medir pressões e pressões diferenciais de gases, vapores e líquidos com precisão e exatidão assumidas. Esta medição controla proporcionalmente a corrente no circuito de corrente de 2 fios de 4...20 mA e é, em alternativa, apresentada em unidades padronizadas no ecrã LCD local.

Os transmissores da série **APC(R)-2000ALW Safety** nas versões standard, intrinsecamente segura Exi e à prova de fogo Exd são utilizados para medições em sistemas que asseguram o nível de integridade de segurança **SIL2** de acordo com a norma **PN-EN 61508:2010**.

4.1. Parâmetros técnicos

Fonte de alimentação		**Temperatura ambiente**	**Alarmes**	
Versão de padrão	11,5 ÷ 36 V DC	-25 ÷ 85°C	diagnóstico interno	baixo (LO) < 3,6 mA
Versão Exi	11,5 ÷ 30 V DC	-25 ÷ 80°C	crítico	baixo (LO) << 3,6 mA
Versão Exd	11,5 ÷ 36 V DC	-25 ÷ 75°C		

* No caso das versões intrinsecamente seguras, devido a possíveis limitações da norma para atmosferas explosivas, a temperatura máxima de funcionamento para as classes T4, T5, T6 pode diferir dos assumidos.

Para outros parâmetros técnicos, consultar o **Manual de Instruções**.

5. DESCRIÇÃO DOS REQUISITOS E RESTRIÇÕES DE SEGURANÇA

Nas seguintes condições de funcionamento, a função de segurança não é garantida:

- durante a configuração;
- quando o HART® multi drop está ativo;
- na transmissão de valores de medição através do protocolo HART;
- durante a simulação;
- durante os teste de resistência;
- quando o bloqueador de registo está desativado.

Um transmissor configurado para funcionar num circuito de segurança funcional, uma vez efetuadas as definições necessárias relativas à sua identificação, metrologia e modos de alarme, **deve** ter um bloqueio de registo de dados configurado para o transmissor através do protocolo HART, efetuado por meio de um comunicador ou Raport 2.

HART® é uma marca registada do FieldComm Group.

A margem segura aceitável de erro de medição adotada na análise FMEDA é: **1%**.
Tempo de realização de um ciclo completo de diagnóstico: **1 minuto**.
Vida útil: **50 anos**, determinados pelo desgaste dos componentes.
A vida útil não se aplica às ligações ao processo (partes molhadas).

5.1. Alarmes

Os transmissores da série APC(R)-2000ALW Safety possuem um sistema de alarme acionado pela deteção de condições perigosas através de diagnósticos internos.

O referido diagnóstico detetará os estados perigosos tais como:

- tensão de alimentação do transmissor insuficiente;
- falha da ponte de medição da pressão que consiste num curto-circuito, numa abertura ou numa alteração do valor de uma das piezoresistências da ponte;
- defeitos na ponte de medição da pressão que consistem em curto-circuitos ou abertura das ligações da ponte;
- falhas que impliquem um curto-circuito ou uma abertura de qualquer uma das ligações entre a ponte de medição de pressão e o conversor ADC;

- danos nas referências raciométricas ou o seu desvio acima do normal;
- danos nos componentes ou nas ligações entre eles no percurso de medição ADC, memória de coeficientes relacionados com a linearização / compensação da cabeça, alimentação elétrica na zona de medição do sensor de pressão;
- danos nos componentes ou nas ligações entre eles no percurso de processamento D/A e U/I;
- estados de sobrecarga de pressão da estrutura de medição;
- danos no percurso de transmissão do sinal de medição digital através da barreira galvânica;
- danos em partes funcionais individuais da CPU, como RAM, FLASH, registos, bloco de suporte de hardware para cálculos de ponto flutuante, periféricos de I/O;
- danos na integridade da execução do programa da CPU;
- ultrapassagem da diferença permitida entre a corrente definida (processo) e a corrente medida no circuito de 4...20 mA;
- ultrapassagem dos limites de temperatura: ponte de medição de pressão, conversor ADC, CPU;
- ultrapassagem da temperatura mínima ou máxima de funcionamento (temperatura ambiente);
- ultrapassagem dos limites de alimentação nos circuitos do transmissor.

Se um ataque cibernético causar a ultrapassagem do número limite de tentativas de acesso não autorizado para alterar a palavra-passe ou alterar a segurança da gravação, é acionado um alarme no transmissor. O acesso à função de desativação é protegido por uma palavra-passe de 32 bits (4,3 mil milhões de combinações). Após 20 tentativas de acesso não autorizado, é ativado um alarme que durará até à redefinição do software ou do hardware do transmissor.

Alguns diagnósticos têm limiares de disparo que eliminam os eventos estocásticos a favor de eventos correlacionados. Isto aplica-se, em particular, aos possíveis efeitos das interferências eletromagnéticas na transmissão digital nas áreas do protocolo SPI e na área dos amplificadores de sinal de isolamento galvânico.

Não serão detetados pelo diagnóstico do transmissor:

- fugas no sistema de pressão da ligação ao processo;
- fuga de óleo do sensor de pressão / pressão diferencial ou dos separadores causada por perfuração da membrana do sensor;
- efeito da penetração das moléculas de hidrogénio no espaço do sensor ou nos separadores, resultando num erro de medição;
- vibrações ou choques acima do normal, a não ser que isso provoque a destruição dos componentes internos ou das ligações elétricas.

Devido à natureza da fonte de alimentação e da interface elétrica do transmissor, é utilizado um nível de corrente de alarme para assinalar condições de alarme.
No modo de alarme de diagnóstico, o transmissor deve emitir a corrente nominal de: **I_ALARM_L = 3,600 mA – E**, em que E é o erro seguro admissível do pressuposto FMEDA de 1%, equivalente a ±160 µA DC na corrente do circuito. Finalmente, o valor da corrente nominal definido no modo ALARME_L deve ser de 3,440 mA.
O diagnóstico do transmissor não envolve um modo de alarme de corrente acima da gama de 20,500 mA. Do ponto de vista do PLC, uma corrente acima do valor de 20,600 mA deve ser considerada como um FAIL_SAFE e um dano seguro diagnosticável.

Os alarmes de diagnóstico são permanentemente ativados e não estão sujeitos a qualquer configuração.

Em caso de alarmes críticos, o controlo é imediatamente transferido para o circuito infinito, acionando o circuito de vigilância independente WDT_SIL com discriminador de tempo. O circuito WDT_SIL desligará a eletrónica principal do transmissor da fonte de alimentação no espaço de 2 segundos, fazendo com que o circuito de corrente desça abaixo de 0,3 mA. Este estado mantém-se até que a fonte de alimentação seja completamente desligada do transmissor e este seja novamente ligado.

As causas dos alarmes críticos são:

- erro de cálculos matemáticos de vírgula flutuante;
- deteção de erros de RAM;
- deteção de erros na memória FLASH;
- deteção de erros de registo da CPU;
- inconsistência das 8 medições consecutivas da corrente do circuito de corrente com o valor de corrente definido;
- perturbação do autómato do programa que resulte numa saída fora da janela de tempo da atualização WDT_SIL.

Os estados de diagnóstico de alarme (exceto os críticos) são legíveis através da comunicação **HART**. O comando **HART CMD_48** (Read Additional Transmitter Status) permite uma identificação mais precisa da causa do alarme.

Para além dos diagnósticos legíveis por HART, os estados de diagnóstico são indicados no ecrã LCD local. Os alarmes de diagnóstico nos blocos de função individuais são somados logicamente num estado de erro acumulado, que pode ser apresentado em forma numérica no ecrã LCD local.

5.2. Restrições

As restrições à utilização de transmissores da série APC(R)-2000ALW Safety em sistemas de segurança funcional incluem o seguinte:

- o transmissor de medição **deve** ser adaptado à aplicação, tendo em conta as caraterísticas do meio de processo e o ambiente de funcionamento;
- as gamas de funcionamento permitidas especificadas nas Informações Técnicas (en: Technical Information) do transmissor não devem ser **excedidas**;
- um transmissor defeituoso deve ser substituído **logo** que se verifique que está avariado.

5.3. Comentários sobre a cibersegurança

Os sistemas de controlo industrial, que até agora funcionavam como sistemas isolados, baseiam-se atualmente em plataformas abertas, têm pontos de contacto com a rede TIC da empresa e utilizam a conetividade implementada através da Internet pública ou, mais frequentemente, de redes fracamente protegidas. Tendo em conta a cibersegurança, uma vez efetuadas as definições necessárias do transmissor relacionadas com os seus modos de identificação, metrologia e alarme, o transmissor deve ter os bloqueios ativados:

- registo remoto de dados (HART) ou alterações de definições;
- alterações das definições locais utilizando os botões MENU locais.

Após a configuração e colocação em funcionamento do sistema de segurança funcional, só deve ser utilizado o sinal de saída de corrente analógico. A responsabilidade pela cibersegurança cabe ao operador do sistema, que deve garantir uma ligação segura entre o sistema E/E/PE relacionado com a segurança e a rede da empresa. O operador deve estabelecer e manter todos os meios adequados de autenticação, cifragem e instalação de software adequado para proteger o sistema de automatização, que deve servir contra quaisquer violações da segurança, acesso não autorizado, adulteração, pirataria informática e roubo de dados.

A Aplisens S.A. e as suas subsidiárias não serão responsáveis por quaisquer danos e/ou perdas relacionadas com tais violações de segurança como acesso não autorizado, adulteração, pirataria informática, fuga e/ou roubo de dados ou informações.

6. TESTES DAS FUNÇÕES DE SEGURANÇA

6.1. Proof Test

Recomenda-se a realização de testes da função de segurança (Proof Test) que permitem detetar 100% dos possíveis erros perigosos não diagnosticáveis dos transmissores.

O fabricante recomenda que os testes periódicos de T[Proof] se realizem uma vez por ano.

O teste da função de segurança é efetuado através do software **RAPORT 2** da APLISENS S.A. com o plug-in **SIL PROOF TEST**.

Lista das etapas do teste da função de segurança (Proof Test):

1. Configurar o PLC que está a funcionar no circuito de segurança para ignorar as medições e os alarmes do transmissor utilizado no teste.
2. Verificar o estado das coberturas mecânicas do transmissor (falta de afrouxamentos e fugas) e substituir as juntas e os bucins endurecidos ou danificados, responsáveis pela estanquidade da carcaça.
3. Verificar o estado das ligações elétricas (certeza das ligações dos fios aos terminais de ligação).
4. Verificar o estado da linha de ligação (substituir o cabo se o isolamento estiver desgastado). Verificar visualmente o estado da cabeça de medição; no caso de depósitos na membrana da cabeça de medição, remover os depósitos quimicamente, dissolvendo-os num agente não destrutivo da membrana. A membrana de medição não deve ser limpa mecanicamente. Se houver sinais de corrosão na extremidade da cabeça ou na membrana, contactar o fabricante para substituir a cabeça ou utilizar outros materiais mais resistentes para a cabeça nesta aplicação.
5. Executar o software **Raport 2** da APLISENS S.A. num PC com WINDOWS®. Ligar ao computador um modem HART/USB da APLISENS S.A. ou outro modem que funcione no padrão BELL 202. Ligar a fonte de alimentação, o modem e o amperímetro ao circuito de corrente que alimenta o transmissor a testar, de acordo com o diagrama da **Figura 1.** Prestar atenção para remover a jumper para o teste, que depois de este ser concluído deve ser reinstalada. Alimentar o transmissor com 16,50 V DC medidos nos terminais da fonte de alimentação.

   Efetuar a identificação do transmissor e, em seguida, abrir o separador "**SIL Proof Test**". Remover a proteção de registo no transmissor no software, utilizando o comando HART. Para tal, no separador "**SIL Proof Test**" no menu, selecionar "**Write lock**" (Bloqueio de registo). O assistente de operação será ativado. Seguir as instruções do assistente que, nos passos seguintes, perguntará pelas intenções do operador e executará as ações necessárias.

   WINDOWS® é uma marca registada da propriedade da Microsoft Corporation.

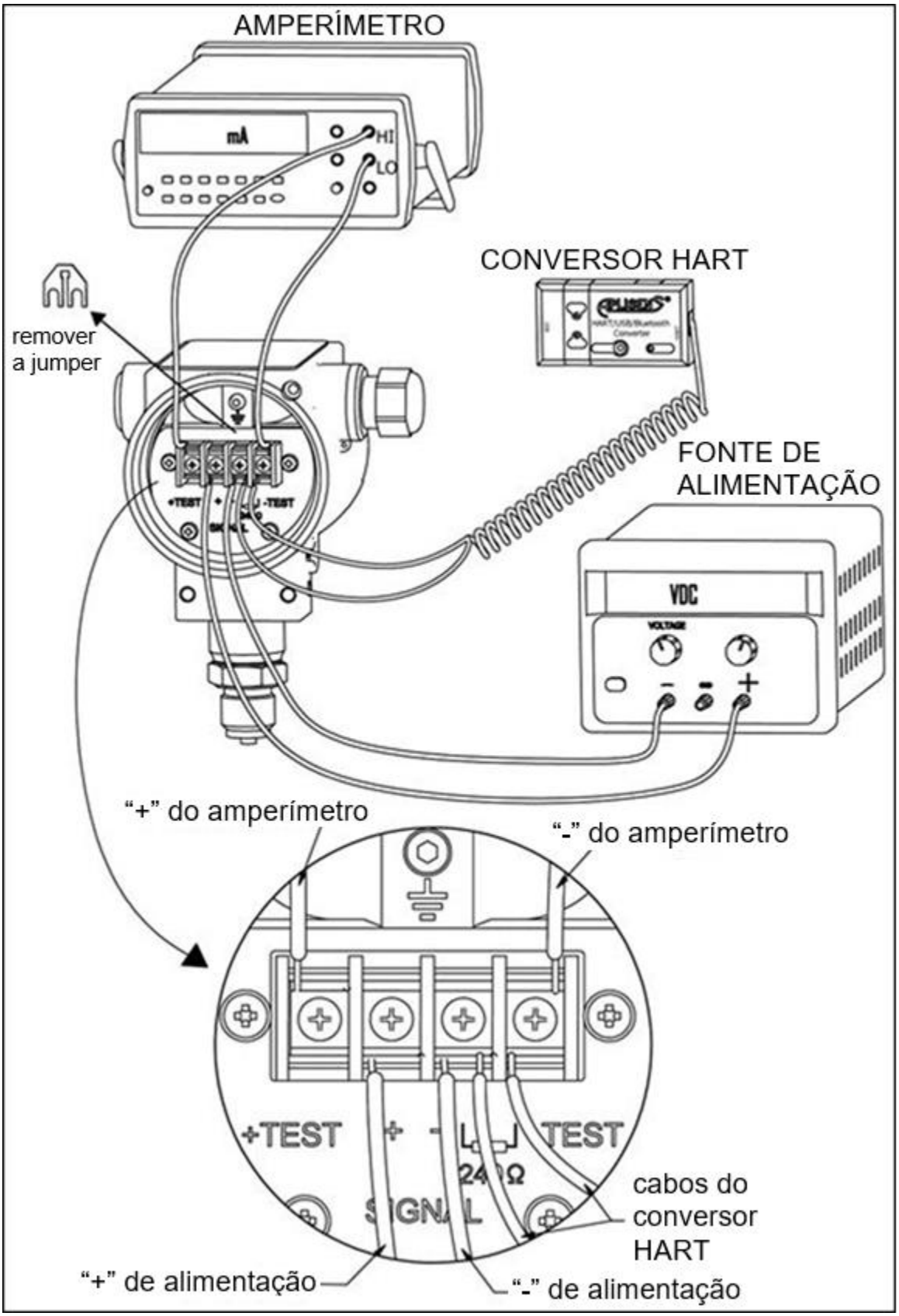


Figura 1. Sistema de ligação do transmissor a um circuito de corrente para um teste de prova

6. Efetuar testes na saída analógica do circuito de corrente. Para tal, no separador "**SIL Proof Test**" no menu, selecionar a opção "**Analog output test**" (Teste de saída analógica). O assistente de teste será ativado. Seguir as instruções do assistente que, nos passos seguintes, efetuará os testes do conversor DAC, testes do conversor U/I e testes do percurso de controlo do circuito de corrente. O assistente irá recomendar sucessivamente:

6.1. Alimentar o transmissor com 16,50 V DC medidos nos terminais da fonte de alimentação. Utilizando o comando HART, a saída de corrente do transmissor será definida para a corrente de 20,660 mA correspondente à corrente máxima de segurança do transmissor. Utilizando um miliamperímetro DC de referência com a classe de ≤ 0,025 e a resistência interna de ≤ 10 Ω incorporada no circuito de corrente, ler a corrente que circula na linha. Este teste, para além de verificar o valor da corrente de alarme, deteta possíveis problemas relacionados com a tensão mínima de alimentação do transmissor, que podem surgir devido a quedas de tensão através da resistência da linha de alimentação ou da resistência da fonte de alimentação.

6.2. Com a saída de corrente definida para 20,660 mA, o assistente de teste lê o parâmetro PVIret. O desvio admissível do parâmetro PVIret é de ±0,032 mA.

6.3. Utilizando o comando HART, a saída de corrente do transmissor será definida para a corrente de 3,280 mA correspondente à corrente de alarme LO (menos o erro admissível de 1%, ou seja, 0,16 mA). Utilizando um miliamperímetro DC de referência com a classe de ≤ 0,025 incorporado no circuito de corrente, ler a corrente que circula na linha. Este teste deteta possíveis problemas relacionados com a corrente de inatividade excessiva consumida pelo transmissor (por exemplo, devido a danos nos componentes).

Se o valor de corrente medido no teste **6.1**, **6.2** ou **6.3** se desviar, respetivamente, dos valores esperados (tendo em conta o desvio admissível das instruções de funcionamento), deve ser efetuado o procedimento de calibração da saída analógica da corrente — para 4 mA e 20 mA. O procedimento de calibração deve ser efetuado utilizando um miliamperímetro de referência DC com a classe de ≤ 0,025 e a resistência interna de ≤ 10 Ω. Após a calibração, é necessário efetuar novamente os passos referidos no **ponto 6** do teste.

Se, apesar da calibração, o valor da corrente medida em **6.1**, **6.2** ou **6.3** se desviar do valor esperado (tendo em conta o desvio admissível das instruções de funcionamento), **o teste não será concluído com sucesso e o transmissor terá de ser devolvido ao fabricante para reparação**.

7. Efetuar uma verificação da função de medição da pressão / pressão diferencial. Para tal, no separador "SIL Proof Test", selecionar a opção "**Pressure / differential pressure measurement test**" (Teste de medição de pressão / pressão diferencial). O assistente de teste será ativado. O assistente efetuará testes de pressão nos passos seguintes, devendo ser seguidas as suas instruções:

7.1. Alimentar o transmissor com 16,50 V DC medidos nos terminais da fonte de alimentação. Utilizando um transmissor de pressão com a classe ≤ 0,03, fornecer uma pressão de referência ao transmissor com um valor correspondente a 4 mA (0% da gama de pressão definida) e, utilizando um miliamperímetro com a classe ≤ 0,025 e a resistência interna ≤ 10 Ω, medir a corrente que circula no circuito de corrente.

7.2. Utilizando um transmissor de pressão com a classe ≤ 0,03, fornecer uma pressão de referência ao transmissor com um valor correspondente a 12 mA (50% da gama de pressão definida) e, utilizando um miliamperímetro com a classe ≤ 0,025 e a resistência interna ≤ 10 Ω, medir a corrente que circula no circuito de corrente.

7.3. Utilizando um transmissor de pressão com a classe ≤ 0,03, fornecer uma pressão de referência ao transmissor com um valor correspondente a 20 mA (100% da gama de pressão definida) e, utilizando um miliamperímetro com a classe ≤ 0,025 e a resistência interna ≤ 10 Ω, medir a corrente que circula no circuito de corrente.

Se os valores de corrente medidos se desviarem do valor esperado, que deve estar dentro do intervalo de ±0,012 mA (tendo em conta o desvio permitido resultante das instruções de funcionamento), deve ser efetuado um procedimento de calibração da pressão no transmissor para os valores de pressão de referência definidos, correspondentes ao início e ao fim do intervalo definido (ou básico). Neste caso, após a calibração, o teste deve ser repetido a partir do **ponto 7**.

Se, com o procedimento de calibração corretamente executado, o transmissor continuar a dar um valor de corrente que se desvie do valor esperado (tendo em conta o desvio admissível resultante das instruções de funcionamento), **o transmissor deve ser devolvido imediatamente ao fabricante para reparação.**

8. Alimentar o transmissor com 16,50 V DC medidos nos terminais da fonte de alimentação. Efetuar o controlo de medição da temperatura na estrutura do sensor de pressão, no conversor ADC e no microcontrolador principal. Para o efeito, uma vez estabilizadas as condições térmicas num ambiente de 15 - 25°C, a temperatura da carcaça do transmissor deve ser medida utilizando um termómetro eletrónico de referência de, pelo menos, classe "B". Por "condições térmicas estabilizadas" entende-se que a temperatura da carcaça do transmissor e do sensor de pressão nele integrado é relativamente homogénea. No menu do separador "**SIL Proof Test**", selecionar a opção "**Temperature tests**" (Testes de temperatura). O assistente de teste será ativado. Seguir as instruções do assistente, que efetuará os testes de temperatura nos passos seguintes. O software lê a segunda, terceira e quarta variáveis de processo (SV, TV, FV). As mesmas correspondem sucessivamente à temperatura do sensor de pressão (SV), à temperatura do microcontrolador principal (TV) e à temperatura do conversor ADC (FV).

Se, com o procedimento de teste corretamente executado, os valores de temperatura SV, TV, FV se desviarem da temperatura medida pelo termómetro eletrónico de referência em mais de 5°C, **o transmissor deve ser devolvido imediatamente ao fabricante para reparação.**

9. Alimentar o transmissor com 16,50 V DC medidos nos terminais da fonte de alimentação. Efetuar um controlo funcional dos módulos de alarme. No menu do separador "**SIL Proof Test**", selecionar a opção "**Alarm modules test**" (Teste dos módulos de alarme). O assistente de teste será ativado. Seguir as instruções do assistente, que efetuará os testes do módulo de alarme primário e de reserva nos passos seguintes.

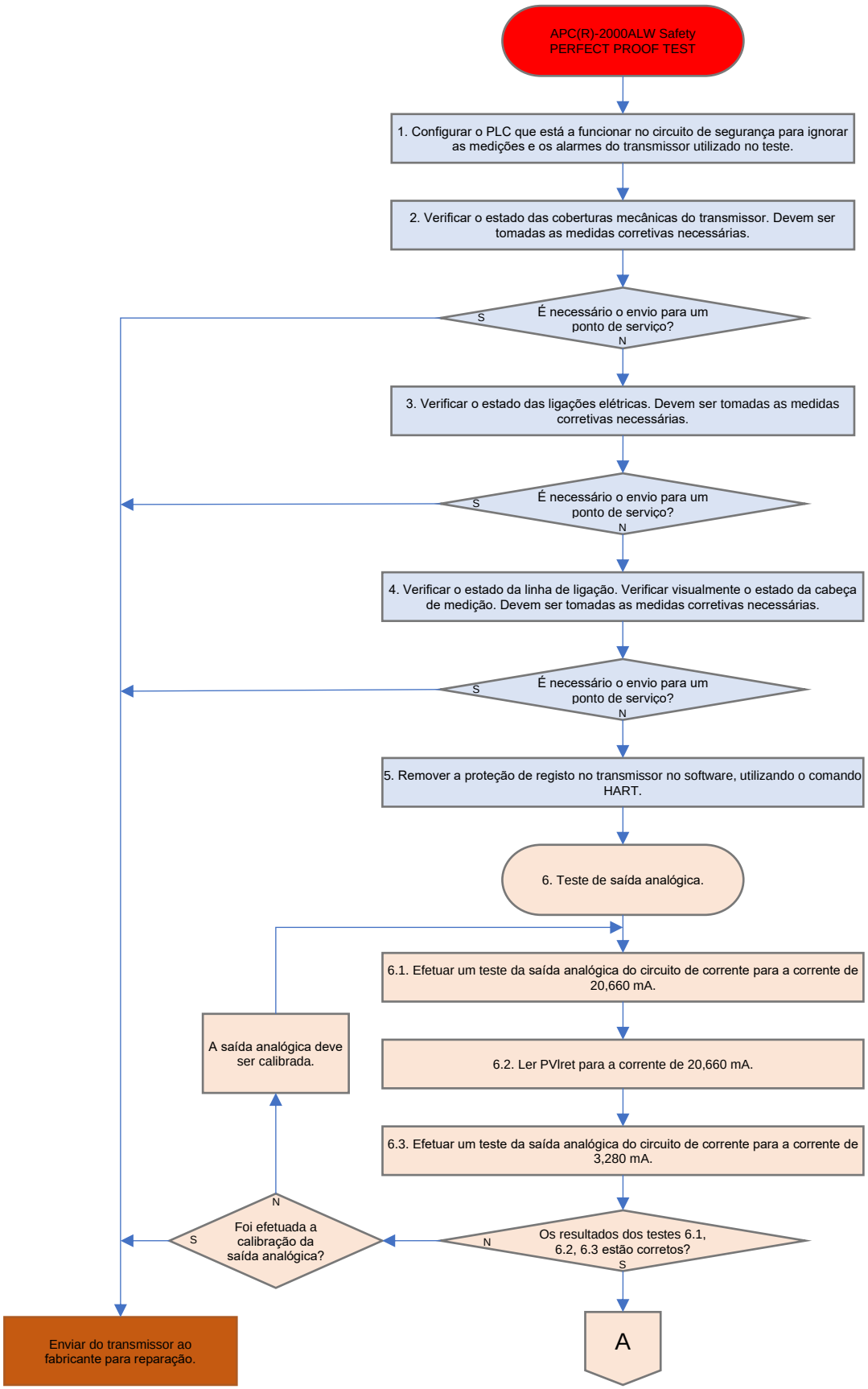
Se, com o procedimento de teste corretamente executado, o transmissor não se comportar como descrito no assistente de teste, **deve ser imediatamente devolvido ao fabricante para reparação.**

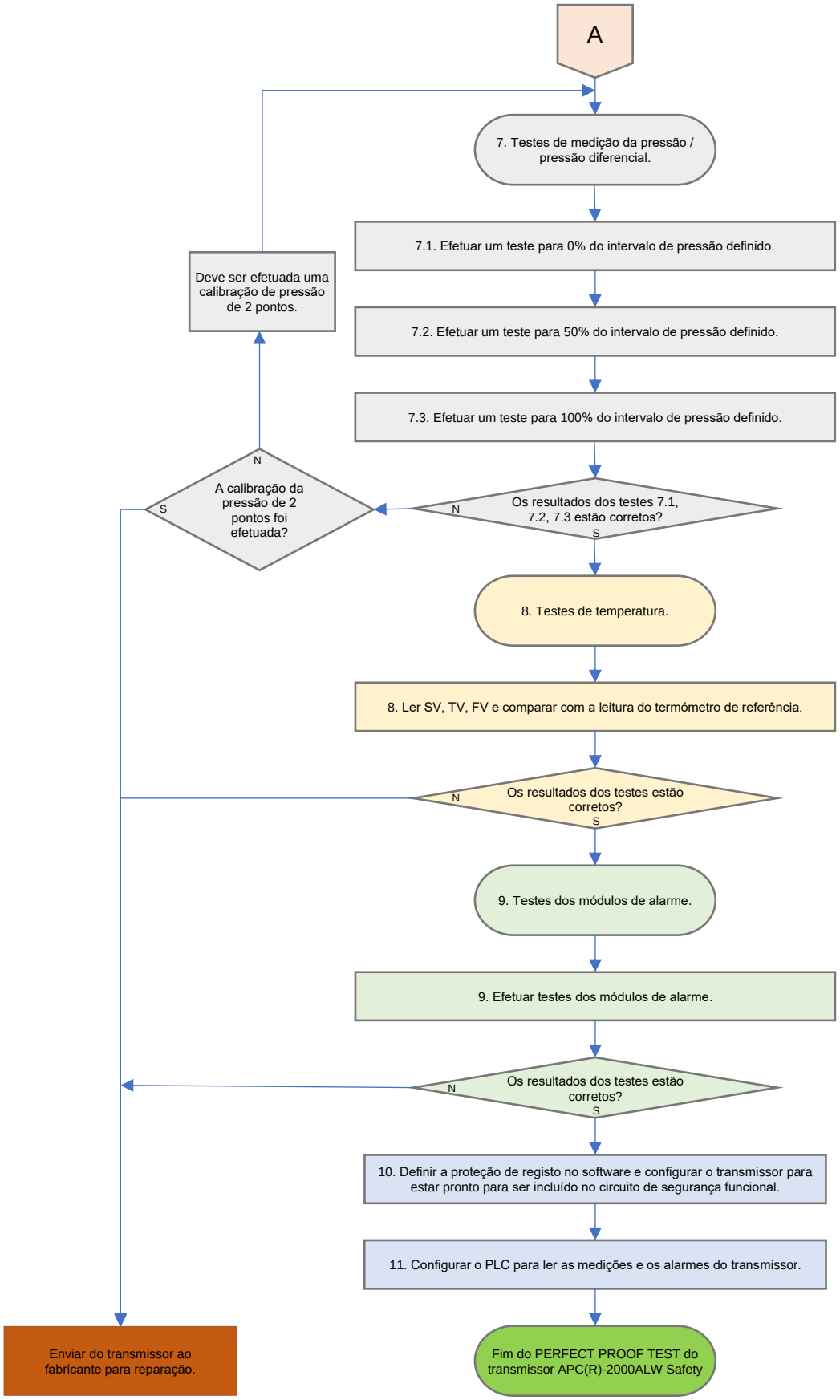
10. Definir a proteção de registo no transmissor no software, utilizando o comando **HART** (software Raport 2 da APLISENS S.A.). Para tal, no separador "**SIL Proof Test**", selecionar "**Write lock**" (Bloqueio de registo). O assistente de operação será ativado. Seguir as instruções do assistente que, nos passos seguintes, perguntará pelas intenções do operador e executará as ações necessárias. Quando os testes forem concluídos corretamente, o assistente de teste irá gerar um relatório de teste e definir o transmissor para estar pronto para incorporação no circuito de segurança funcional.

11. Configurar o PLC do circuito de segurança para ler as medições e os alarmes do transmissor utilizado no teste. Documentar e arquivar os resultados dos testes.

O **anexo 1** do Manual de Segurança inclui uma lista de verificação das atividades a realizar para o teste de prova (Proof Test).

6.2. Fluxograma do Teste de prova (Proof Test)




A
7. Testes de medição da pressão / pressão diferencial.
7.1. Efetuar um teste para 0% do intervalo de pressão definido.
7.2. Efetuar um teste para 50% do intervalo de pressão definido.
7.3. Efetuar um teste para 100% do intervalo de pressão definido.
Os resultados dos testes 7.1, 7.2, 7.3 estão corretos?
N
S
A calibração da pressão de 2 pontos foi efetuada?
N
S
Deve ser efetuada uma calibração de pressão de 2 pontos.
8. Testes de temperatura.
8. Ler SV, TV, FV e comparar com a leitura do termómetro de referência.
Os resultados dos testes estão corretos?
N
S
9. Testes dos módulos de alarme.
9. Efetuar testes dos módulos de alarme.
Os resultados dos testes estão corretos?
N
S
10. Definir a proteção de registo no software e configurar o transmissor para estar pronto para ser incluído no circuito de segurança funcional.
11. Configurar o PLC para ler as medições e os alarmes do transmissor.
Fim do PERFECT PROOF TEST do transmissor APC(R)-2000ALW Safety
Enviar do transmissor ao fabricante para reparação.

7. REPARAÇÃO

Não são permitidas reparações ou outras interferências nos circuitos eletrónicos do transmissor. A avaliação do dano e eventual reparação só pode ser efetuada pelo departamento de assistência técnica da APLISENS S.A. As funções de segurança não podem ser garantidas se as reparações forem efetuadas por outra pessoa.

8. DADOS DE FIABILIDADE

Transmissor	λ_{total} FIT	λ_{NE} FIT	λ_{SD} FIT	λ_{SU} FIT	λ_{DD} FIT	λ_{DU} FIT	SFF %	DC %	MTBF
APC-2000ALW Safety	905,321	265,723	0	138,208	451,857	49,533	92,256	90,121	$1{,}105\times10^{6}$ h 126,094 Yrs
APR-2000ALW Safety	919,621	265,723	0	138,208	453,387	62,303	90,472	87,919	$1{,}087\times10^{6}$ h 124,133 Yrs

Transmissor	T[Proof] = 1 ano	T[Proof] = 2 anos	T[Proof] = 5 anos	T[Proof] = 10 anos
APC-2000ALW Safety	$PFD_{avg} = 2{,}17\times10^{-4}$	$PFD_{avg} = 4{,}34\times10^{-4}$	$PFD_{avg} = 1{,}08\times10^{-3}$	$PFD_{avg} = 2{,}17\times10^{-3}$
APR-2000ALW Safety	$PFD_{avg} = 2{,}73\times10^{-4}$	$PFD_{avg} = 5{,}46\times10^{-4}$	$PFD_{avg} = 1{,}36\times10^{-3}$	$PFD_{avg} = 2{,}73\times10^{-3}$

Systematic Capability	SC 3 (SIL 3 Capable)
Random Capability	Type B Element SIL2@HFT=0; SIL3@HFT=1; Route 1_H

PFH = λ_{DU}
MTTR = MRT = 8h
O fabricante recomenda que os testes periódicos de T[Proof] dos pordutos acima referidos se realizem uma vez por ano.

9. REGISTO DE ALTERAÇÕES

Número de alteração	Edição de um documento	Descrição das alterações
-	01.A.001/2023.05	Primeira versão do documento em português. Desenvolvido pelo departamento DBFD.

ANEXO 1. Lista de controlo das ações a efetuar no âmbito dum teste de prova **(Proof Test)**

Data de início do teste: _____

Pessoa responsável pelo teste: _____

1. Configurar o PLC que está a funcionar no circuito de segurança para ignorar as medições e os alarmes do transmissor utilizado no teste.

realizado? **S/N** **[ ]**

2. Verificar o estado das coberturas mecânicas do transmissor (falta de afrouxamentos e fugas) e substituir as juntas e os bucins endurecidos ou danificados, responsáveis pela estanquidade da carcaça.

realizado? **S/N** **[ ]**

3. Verificar o estado das ligações elétricas (certeza das ligações dos fios aos terminais de ligação).

realizado? **S/N** **[ ]**

4. Verificar o estado da linha de ligação (substituir o cabo se o isolamento estiver desgastado).

realizado? **S/N** **[ ]**

Verificar visualmente o estado da cabeça de medição. No caso de depósitos na membrana da cabeça de medição, remover os depósitos quimicamente, dissolvendo-os num agente não destrutivo da membrana.

realizado? **S/N** **[ ]**

5. Remover a proteção de registo no transmissor no software, utilizando o comando HART.

realizado? **S/N** **[ ]**

NOTA:

6. Efetuar testes na saída analógica do circuito de corrente.

6.1. Efetuar um teste da saída analógica do circuito de corrente para a corrente de 20,660 mA.

realizado? **S/N** **[ ]**

6.2. Ler PVlret para a corrente de 20,660 mA.

realizado? **S/N** **[ ]**

6.3. Efetuar um teste da saída analógica do circuito de corrente para a corrente de 3,280 mA.

realizado? **S/N** **[ ]**

Os resultados dos testes estão corretos? **S/N** **[ ]**

Foi efetuada uma calibração? **S/N** **[ ]**

NOTA:

---

7. Efetuar testes de medição de pressão / pressão diferencial.

7.1. Efetuar um teste para 0% do intervalo de pressão definido.

realizado? **S/N** **[ ]**

7.2. Efetuar o teste para 50% do intervalo de pressão definido.

realizado? **S/N** **[ ]**

7.3. Efetuar o teste para 100% do intervalo de pressão definido.

realizado? **S/N** **[ ]**

Os resultados dos testes estão corretos? **S/N** **[ ]**

Foi efetuada uma calibração? **S/N** **[ ]**

NOTA:

8. Efetuar testes de temperatura através da leitura de SV, TV, FV e comparar com a leitura de um termómetro de referência.

realizado? **S/N** **[ ]**

NOTA:

---

9. Efetuar testes dos módulos de alarme (os testes incluem também os alarmes desencadeados por ciberataques).

realizado? **S/N** **[ ]**

NOTA:

---

10. Verificar se a definição da unidade de pressão está correta.

realizado? **S/N** **[ ]**

Verificar se a definição do tipo de caraterística de conversão está correta.

realizado? **S/N** **[ ]**

Verificar se a definição de início e fim do intervalo de pressão definido está correta.

realizado? **S/N** **[ ]**

Verificar se a definição da constante de tempo está correta.

realizado? **S/N** **[ ]**

Verificar o endereço pool do instrumento (deve ser igual a zero – funcionamento analógico).

realizado? **S/N** **[ ]**

Verificar a configuração da saída analógica – modo de funcionamento e corrente de alarme “L”.

realizado? **S/N** **[ ]**

Definir a proteção de registo no software no transmissor.

realizado? **S/N** **[ ]**

NOTA:

---

11. Configurar o PLC para ler as medições e os alarmes do transmissor, incluindo-o no circuito de segurança funcional.

realizado? **S/N** **[ ]**

NOTA:

Data da conclusão do teste e assinatura da pessoa responsável pelo teste:

....

Data Assignatura