DIÁRIO OFICIAL DA UNIÃO

Publicado em: 16/06/2021 | Edição: 111 | Seção: 1 | Página: 185

Órgão: Ministério da Economia/Instituto Nacional de Metrologia, Qualidade e Tecnologia

PORTARIA INMETRO Nº 264, DE 15 DE JUNHO DE 2021

Altera a Portaria Inmetro nº 559 de 15 de dezembro de 2016, que aprova o Regulamento Técnico Metrológico de bombas medidoras de combustíveis líquidos utilizados nas medições de volume e seu Anexo.

O PRESIDENTE DO INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA - INMETRO, no exercício da competência que lhe foi outorgada pelos artigos 4º, § 2º, da Lei nº 5.966, de 11 de dezembro de 1973, e 3º, incisos II e III, da Lei nº 9.933, de 20 de dezembro de 1999, combinado com o disposto nos artigos 18, inciso V, do Anexo I ao Decreto nº 6.275, de 28 de novembro de 2007, e 105, inciso V, do Anexo à Portaria nº 2, de 4 de janeiro de 2017, do então Ministério da Indústria, Comércio Exterior e Serviços, publicada no Diário Oficial da União de 05 de janeiro de 2017, seção 1, página 41, e item 4, alínea "a" da Resolução nº 8, de 22 de dezembro de 2016, do Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro). Considerando a necessidade de esclarecer e aprimorar alguns requisitos da Portaria Inmetro nº 559, de 15 de dezembro de 2016, publicado no Diário Oficial da União de 16 de dezembro de 2016, seção 1, página 49, referentes à segurança de software e hardware; Considerando que o Inmetro se tornou uma Autoridade Certificadora de Primeiro Nível na Infraestrutura de Chaves Públicas Brasileiras (ICP-Brasil), e o que consta no processo SEI nº 0052600.000241/2021-26, resolve:

Art. 1º As bombas medidoras de combustíveis líquidos aprovadas conforme o regulamento técnico metrológico estabelecido pela Portaria Inmetro nº 23, de 25 de fevereiro de 1985 poderão ser submetidas a verificação inicial até 30 de junho de 2022.

Parágrafo Único Durante mesmo prazo poderão ser realizadas modificações de modelo de bombas medidoras de combustíveis líquidos mencionadas no caput.

Art. 2º O artigo 8º da Portaria Inmetro nº 559, de 15 de dezembro de 2016, alterado pela Portaria 516, de 13 de dezembro de 2019, passa a vigorar com a seguinte redação:

"Art. 8º A partir de 1º de julho de 2022, as bombas medidoras de combustíveis líquidos em uso, aprovadas pela Portaria Inmetro nº 023/1985, com qualquer ano de fabricação e autuadas pelo Inmetro por fraude, não poderão permanecer em uso, devendo ser substituídas por bombas medidoras de combustíveis líquidos aprovadas em conformidade com este RTM." (NR)

Art. 3º O artigo 11 da Portaria Inmetro nº 559, de 15 de dezembro de 2016, alterado pela Portaria 516, de 13 de dezembro de 2019, passa a vigorar com a seguinte redação:

"Art. 11 Ficam revogadas, a partir de 1º de julho de 2022:

I - Portaria Inmetro nº 23, de 25 de fevereiro de 1985, publicada no Diário Oficial da União em 07 de março de 1985, Seção 01, páginas 3891 a 3894.

II - Portaria Inmetro nº 174, de 07 de agosto de 1991, publicada no Diário Oficial da União em 14 de agosto de 1991, Seção 01, páginas 16399 a 16400.

III - Portaria Inmetro nº 52, de 13 de fevereiro de 2004, publicada no Diário Oficial da União em 16 de fevereiro de 2004, Seção 01, página 58." (NR)

Art 4º Fica revogado o subitem 6.1.1.1 do Regulamento Técnico Metrológico aprovado pela Portaria Inmetro nº 559, de 15 de dezembro de 2016.

Art. 5º O subitem 7.1 do Regulamento Técnico Metrológico aprovado pela Portaria Inmetro nº 559, de 15 de dezembro de 2016 passa a vigorar acrescido dos seguintes requisitos:

(...)

7.1.7 Em local de fácil visualização, no dispositivo transdutor:

a) código de produto;

b) número de série.

7.1.8 Em local de fácil visualização, no dispositivo controlador:

a) código do produto;

b) número de série." (...) NR

Art. 6º O subitem 10.3.1.6 do Regulamento Técnico Metrológico aprovado pela Portaria Inmetro nº 559, de 15 de dezembro de 2016 passa a vigorar acrescido do seguinte requisito:

(...)

10.3.1.6.1 Usando a chave pública dos dispositivos transdutores envolvidos no abastecimento, validar os respectivos certificados digitais ICP-Brasil tipo OM-BR. (...) NR

Art. 7º O subitem 10.4.1.4 do Regulamento Técnico Metrológico aprovado pela Portaria Inmetro nº 559, de 15 de dezembro de 2016 passa a vigorar acrescido do seguinte requisito:

(...)

10.4.1.4.1 Usando a chave pública dos dispositivos transdutores envolvidos no abastecimento, validar os respectivos certificados digitais ICP-Brasil tipo OM-BR. (...) NR

Art. 8º O ANEXO B - Requisitos de segurança de software e hardware Portaria Inmetro nº 559, de 15 de dezembro de 2016, passa a vigorar na forma do ANEXO da presente portaria.

Art. 9º Esta Portaria entrará em vigor na data de sua publicação no Diário Oficial da União.

MARCOS HELENO GUERSON DE OLIVEIRA JUNIOR

ANEXO - REQUISITOS DE SEGURANÇA DE SOFTWARE E HARDWARE

1. OBJETIVO E CAMPO DE APLICAÇÃO

1.1 Este Anexo estabelece os requisitos técnicos mínimos de segurança de software e hardware a que devem atender as bombas medidoras computadoras de preços eletrônicas de combustíveis líquidos controladas por software, doravante denominadas instrumentos, na avaliação de modelo, verificação inicial, verificações subsequentes e inspeções/supervisão metrológica.

1.2 Este Anexo não se aplica à bombas medidoras não computadoras de preços nem à bombas medidoras mecânicas.

1.3 Este Anexo objetiva garantir adequado nível de confiança no volume de combustível medido por meio dos instrumentos, assegurando confiança nas medições e impedindo ou evidenciando a ocorrência de fraudes metrológicas.

1.4 Todas as evidências para o cumprimento dos requisitos técnicos de software e hardware estabelecidos no presente anexo devem ser providas pelo requerente do processo de avaliação de modelo.

2. TERMINOLOGIA

2.1 Assinatura digital: Resultado proveniente de processo algorítmico, que assegura autenticidade, integridade, não-repúdio, e autoria de uma medição ou arquivo digital.

2.2 Autenticidade: garantia da identidade declarada/alegada de um usuário, processo ou dispositivo.

2.3 Carga de software: processo de transferência de software para os dispositivos de hardware do instrumento por intermédio de qualquer meio técnico apropriado.

2.4 Dispositivo controlador: dispositivo responsável por controlar os outros dispositivos da bomba medidora e processar a informação metrológica.

2.5 Dispositivo indicador: dispositivo que apresenta os resultados das medições.

2.6 Dispositivo controlador-indicador: dispositivo que reúne as funcionalidades dos dispositivos controlador e indicador.

2.7 Dispositivo medidor: componente de uma bomba medidora que transforma o fluxo ou o volume do líquido medido em sinais, de qualquer natureza, que são transmitidos para o dispositivo transdutor.

2.8 Dispositivo transdutor: dispositivo que transforma os sinais de informação gerados pelo dispositivo medidor em um sinal de saída que representa a massa ou o volume de combustível a ser medido sob a forma de dados digitais, a serem transmitidos ao dispositivo controlador por meio do protocolo de comunicação.

2.9 Identificador do abastecimento do dispositivo controlador: número inteiro, iniciando em zero e monotonamente crescente, que identifica univocamente cada abastecimento realizado pela bomba medidora.

2.10 Identificador do abastecimento do dispositivo transdutor: número inteiro, iniciando em zero e monotonamente crescente, que identifica univocamente o abastecimento realizado por um dado transdutor.

2.11 Identificador unívoco do transdutor: conjunto alfanumérico único que identifica o modelo e o número de série do transdutor.

2.12 Integridade: garantia de que os dados, software, ou parâmetros não foram submetidos à alterações, intencionais ou não intencionais, durante o uso, reparo, manutenção, transferência ou armazenamento.

2.13 Interface de comunicação: qualquer tipo de interface (ótica, rádio, eletrônica etc.) que habilite a transferência de informações entre dispositivos do instrumento de medição, ou com dispositivos externos.

2.14 Interface de separação: conjunto de componentes de software e/ou hardware que define a separação entre módulos de software e/ou hardware legalmente relevantes e não legalmente relevantes, por meio da qual comandos ou dados são trocados entre as partes legalmente relevantes e não legalmente relevantes.

2.15 Interface de usuário: interface que permite a troca de informações entre um usuário ou operador e o instrumento ou seus componentes de software e hardware.

2.16 Interface de verificação metrológica: interface que permite e troca de informações legalmente relevantes entre um agente metrológico e o instrumento ou seus componentes de software e hardware.

2.17 Meio inseguro de comunicação: meio que compartilha tráfego de dados com outras aplicações e não provê requisitos de autenticidade e integridade.

2.18 Nome do dispositivo Bluetooth: sequência de caracteres que corresponde ao identificador da interface de comunicação serial sem fio padrão Bluetooth utilizada como interface de verificação metrológica.

2.19 Partes legalmente relevantes: partes do software/hardware/dados do instrumento diretamente envolvidas ou que de alguma forma interferem nas características metrológicas regulamentadas pela metrologia legal.

2.20 Registro de alterações/auditoria: conjunto de dados contendo o registro de quaisquer eventos e/ou alterações no instrumento que sejam legalmente relevantes e passíveis de influenciar suas características metrológicas.

2.21 Registro de Alteração de Parâmetros Metrológicos Relevantes: registro de auditoria que armazena os eventos relacionados às alterações de parâmetros metrológicos relevantes no instrumento.

2.22 Registro de Interrupções de Funcionamento do Instrumento: registro de auditoria que armazena os eventos relacionados às interrupções no funcionamento do instrumento ou de algum de seus dispositivos.

2.23 Registro de Eventos de Manutenção: registro de auditoria que armazena os eventos relacionados às operações de manutenção no instrumento.

2.24 Registro de Cargas de Software Legalmente Relevante: registro de auditoria que armazena os eventos relacionados às operações de carga de software legalmente relevante no instrumento.

2.25 Requisitos gerais de software: requisitos que tratam de aspectos técnicos referentes às tecnologias de uso geral em instrumentos de medição controlados por software.

2.26 Requisitos específicos de software: requisitos que tratam de aspectos técnicos referentes às tecnologias específicas utilizadas no instrumento ou à inclusão de funcionalidades complementares.

2.27 Separação de software: separação do software de um instrumento nas partes legalmente relevante e não legalmente relevante, que se comunicam por meio de uma interface de software.

2.28 Verificação de integridade: procedimento que estabelece se um arquivo, software ou firmware corresponde a um arquivo, software ou firmware previamente conhecido.

2.29 Versão de software: sequência de caracteres que identifica univocamente um módulo de software e suas alterações.

3. REQUISITOS GERAIS DE SOFTWARE E HARDWARE

3.1 O software e o hardware considerados legalmente relevantes devem satisfazer à totalidade dos requisitos gerais.

3.2 Versão do software legalmente relevante

3.2.1 O software legalmente relevante do instrumento e/ou de suas partes deve possuir uma versão que o identifique univocamente.

3.2.2 A versão deve ser apresentada por comando executado a partir das interfaces de usuário e de verificação metrológica.

3.2.3 Qualquer alteração no software do instrumento e/ou de suas partes e que seja definida como legalmente relevante deve implicar na geração de uma nova versão de software que o identifique univocamente.

3.3 Proteção de Software e Hardware

3.3.1 O software e o hardware do instrumento devem ser projetados e construídos de tal forma que a possibilidade de seu uso impróprio ou fraudulento, quer seja intencional, não intencional ou acidental, sejam mínimas.

3.3.2 As proteções do software compreendem métodos de selagem que utilizem meios físicos, eletrônicos ou criptográficos e devem garantir que intervenções ou alterações não autorizadas no software e no hardware do instrumento sejam evitadas e, caso aconteçam, sejam evidenciadas.

3.3.3 Partes legalmente relevantes do instrumento: quer sejam de software ou de hardware, não podem ser inadmissivelmente influenciadas por outras partes do instrumento de medição.

3.3.4 O software os parâmetros legalmente relevantes devem ser protegidos contra modificações inadmissíveis ou não autorizadas, carga de software não autorizada e modificações causadas pela troca indevida de unidades de memória.

3.3.5 Em complementação à selagem mecânica, outros meios técnicos devem ser utilizados para proteger partes do instrumento que possuam sistema operacional embarcado, interfaces de comunicação ou opção de carga de software.

3.3.6 Somente funções claramente documentadas podem ser ativadas pelas interfaces de usuário, de verificação metrológica e de comunicação, que devem ser concebidas de forma a impedir o uso fraudulento ou impróprio do instrumento.

3.3.7 Os parâmetros que definem características metrológicas do instrumento devem ser armazenados de forma segura, protegidos contra intrusão e modificações indevidas, podendo ser alterados somente mediante procedimento documentado pelo fabricante.

3.3.8 O evento a que se refere o item 3.3.7 (alteração de parâmetros relevantes) deve implicar no rompimento de lacres físicos, bem como no armazenamento desta ação em um registro de auditoria implementado em memória não volátil (Registro de Alteração de Parâmetros Metrológicos Relevantes).

3.3.9 O registro do evento a que se refere o item 3.3.8 deve conter os seguintes dados: identificação do nível de acesso do responsável pela alteração, data e hora da alteração, tipo do parâmetro alterado, e os valores anterior e posterior à alteração.

3.3.10 Os registros de auditoria a que se refere o item 3.3.8 devem ser armazenados em fila circular em memória não volátil.

3.3.11 Cada evento armazenado no registro de auditoria a que se refere o item 3.3.8 deve estar associado a um identificador (índice do registro) que observe a ordem cronológica dos eventos causadores do registro.

3.3.12 O prazo mínimo do armazenamento a que se refere o item 3.3.8 é de 5 (cinco) anos.

3.3.13 No caso de preenchimento total da memória a que se refere o item 3.3.8 antes do prazo a que se refere o item 3.3.12, o instrumento deve sinalizar sua ocorrência no dispositivo indicador e impedir sua utilização até a substituição do dispositivo que abrigue a memória utilizada para armazenamento do registro de auditoria.

3.3.14 Os registros de auditoria a que se refere o item 3.3.8 devem ser disponibilizados para leitura por intermédio da interface de verificação metrológica, conforme definido na Norma NIT-Sinst-020.

3.3.15 Deve-se garantir que os componentes que armazenam registros de auditoria, dados e parâmetros legalmente relevantes sejam física e logicamente invioláveis.

3.3.16 Deve-se garantir que o dispositivo transdutor do instrumento seja inviolável, não sendo permitido o acesso físico, ou lógico indevido, ao seu interior.

3.4 Detecção de falhas

3.4.1 O instrumento deve possuir funções de detecção de falhas, a critério do fabricante, mediante implementações de software e/ou hardware

3.4.2 No caso de ocorrência de falhas, o software envolvido na detecção deve reagir de modo apropriado e conforme descrito no manual operacional do instrumento.

3.4.3 O instrumento deve interromper seu funcionamento caso:

a) seja constatada diferença na indicação de volume de combustível, acima do especificado pelo fabricante, entre a soma das medições realizadas por cada dispositivo transdutor utilizado no abastecimento e o valor registrado pelo dispositivo controlador;

b) sejam detectadas tentativas de acesso não autorizadas no instrumento, tanto por meios físicos como por meios lógicos.

3.4.4 Em caso de interrupção do funcionamento do instrumento devido a algum dos motivos elencados no item 3.4.3, uma mensagem de erro deve ser exibida no dispositivo indicador até que seja realizada uma operação de manutenção pelo responsável autorizado pelo órgão metrológico.

3.4.5 O evento a que se refere o item 3.4.3 (interrupção de funcionamento do instrumento) deve ser armazenado em um registro de auditoria implementado em memória não volátil (Registro de Interrupções de Funcionamento do Instrumento), da mesma forma como definido nos itens 3.3.10 a 3.3.15.

3.4.6 O registro do evento a que se refere o item 3.4.5 deve conter os seguintes dados:

a) identificação do tipo de evento que gerou a interrupção no funcionamento do instrumento;

b) o no identificador do dispositivo associado à falha identificada;

c) data e hora da interrupção.

3.4.7 O evento a que se refere o item 3.4.4 (operação de manutenção do instrumento) deve ser armazenado em um registro de auditoria implementado em memória não volátil (Registro de Eventos de Manutenção), da mesma forma como definido nos itens 3.3.10 a 3.3.15.

3.4.8 O registro do evento a que se refere o item 3.4.7 deve conter os seguintes dados:

a) identificação do nível de acesso do responsável pela manutenção do instrumento;

b) o resultado da operação de manutenção, a identificação do dispositivo ou parte da bomba medidora que foi alvo da operação de manutenção;

c) data e hora da operação.

3.5 Comunicação entre dispositivos de hardware da bomba medidora

3.5.1 A comunicação entre dispositivo transdutor, dispositivo controlador e dispositivo indicador deve ser realizada através de protocolo de comunicação definido pelo fabricante sendo facultado, adicionalmente ao protocolo, o uso de outros modos de comunicação.

3.5.2 O dispositivo transdutor deve armazenar internamente um certificado digital ICP-Brasil tipo OM-BR. que permita referenciá-lo sem ambiguidade.

3.5.3 Cada dispositivo transdutor deve ser capaz de gerar um par de chaves criptográficas de forma segura, exportar sua chave pública, gerar requisição de certificado digital assinado com a chave privada, receber e exportar o certificado digital de objeto metrológico ICP Brasil tipo OM-BR.

3.5.3.1 Cada dispositivo transdutor deve assinar digitalmente o pacote de dados especificado no item 3.5.14.

3.5.3.2 Cada dispositivo transdutor deve exportar o certificado digital através de protocolo de comunicação definido pelo fabricante.

3.5.3.3 Deve ser disponibilizado um método para extração do certificado digital contido em cada dispositivo transdutor, bem como as ferramentas de hardware e software necessárias para realização dessa operação.

3.5.4 Dispositivos transdutores devem possuir certificados digitais padrão ICP-Brasil e identificadores unívocos diferentes.

3.5.5 A chave privada gerada por cada dispositivo transdutor deve ser armazenada de modo inviolável e inextricável do meio físico e lógico, assim como não pode ser exportada em hipótese alguma.

3.5.6 Os identificadores unívocos de cada dispositivo transdutor e as chaves públicas contidas nos respectivos certificados OM-BR devem ser armazenados no dispositivo controlador e no dispositivo indicador.

3.5.7 Antes de cada abastecimento, deve ser verificado se os identificadores unívocos e as chaves públicas de cada dispositivo transdutor estão armazenados no dispositivo indicador.

3.5.8 Em caso de falha na verificação referida no item 3.5.7, o dispositivo transdutor cuja verificação não for positiva deve ter seu funcionamento impedido até que seja realizada operação de manutenção pelo responsável autorizado pelo órgão metrológico.

3.5.9 O evento a que se refere o item 3.5.8 (interrupção de funcionamento do dispositivo transdutor) deve ser armazenado no mesmo registro de auditoria a que se refere o item 3.4.5 (Registro de Interrupções de Funcionamento do Instrumento).

3.5.10 O registro do evento a que se refere o item 3.5.9 deve conter os seguintes dados:

a) identificação do tipo de evento que gerou a interrupção no funcionamento do instrumento;

b) o no identificador do dispositivo associado à falha identificada;

c) data e hora da interrupção.

3.5.11 O evento a que se refere o item 3.5.8 (operação de manutenção do instrumento) deve ser armazenado no mesmo registro a que se refere o item 3.4.7 (Registro de Eventos de Manutenção).

3.5.12 O registro do evento a que se refere o item 3.5.11 deve conter os seguintes dados:

a) identificação do nível de acesso do responsável pela manutenção do instrumento;

b) o resultado da operação de manutenção, a identificação do dispositivo ou parte da bomba medidora que foi alvo da operação de manutenção;

c) data e hora da operação.

3.5.13 Ao final da operação de abastecimento ou no caso de o fornecimento do combustível for interrompido por um período de tempo superior a 60 segundos, o dispositivo transdutor deve transmitir ao dispositivo indicador as informações de totalização da medição em um pacote de dados assinado digitalmente com a chave privada a que se refere o subitem 3.5.3.

3.5.14 O pacote de dados citado no item 3.5.13 deve conter as seguintes informações:

a) o identificador do abastecimento fornecido pelo dispositivo controlador;

b) a identificação unívoca do dispositivo transdutor;

c) a identificação unívoca do dispositivo controlador;

d) o identificador do abastecimento do dispositivo transdutor;

e) constante de calibração do dispositivo transdutor;

f) volume medido pelo dispositivo transdutor;

g) volume total da transação fornecido pelo dispositivo controlador;

h) valor monetário total da transação fornecido pelo dispositivo controlador;

i) preço por litro do combustível fornecido pelo dispositivo controlador;

j) data e hora do abastecimento fornecidas pelo dispositivo controlador.

3.5.15 Cada dispositivo transdutor deve realizar internamente:

a) transformação dos sinais de informação gerados pelo dispositivo medidor em um sinal de saída que representa a massa ou o volume de combustível a ser mensurado;

b) a geração dos pacotes de dados a que se refere o item 3.5.14;

c) a assinatura digital do pacote de dados a que se refere o item 3.5.14.

3.5.16 Ao final do abastecimento, o dispositivo indicador deve, no mínimo, apresentar as informações:

a) volume total da transação fornecido pelo dispositivo controlador a que se refere o item 3.5.14g;

b) valor monetário total da transação fornecido pelo dispositivo controlador a que se refere o item 3.5.14h;

c) preço por litro do combustível fornecido pelo dispositivo controlador a que se refere o item 3.5.14i.

3.5.17 Imediatamente após o recebimento do pacote de dados assinado a que se refere o item 3.5.13, sua assinatura digital deve ser verificada pelo dispositivo indicador, que deve sinalizar se o resultado da operação de verificação for positivo.

3.5.18 Se o resultado da verificação da assinatura digital a que se refere o item 3.5.17 for negativo, o funcionamento do dispositivo transdutor correspondente ao abastecimento deve ser impedido até que seja verificado e liberado pelo responsável técnico autorizado pelo órgão metrológico, e uma mensagem de erro deve ser apresentada no painel indicador.

3.5.19 O evento a que se refere o item 3.5.18 (interrupção de funcionamento do dispositivo transdutor) deve ser armazenado no mesmo registro de auditoria a que se refere o item 3.4.5 (Registro de Interrupções de Funcionamento do Instrumento).

3.5.20 O registro do evento a que se refere o item 3.5.19 deve conter os seguintes dados:

a) identificação do tipo de evento que gerou a interrupção no funcionamento do instrumento;

b) no do dispositivo transdutor associado à falha identificada;

c) data e hora da interrupção.

3.5.21 O evento a que se refere o item 3.5.18 (operação de manutenção do instrumento) deve ser armazenado no mesmo registro de auditoria a que se refere o item 3.4.7 (Registro de Eventos de Manutenção).

3.5.22 O registro do evento a que se refere o item 3.5.21 deve conter os seguintes dados:

a) identificação do nível de acesso do responsável pela manutenção do instrumento;

b) o resultado da operação de manutenção;

c) o código de identificação do dispositivo ou parte da bomba medidora que foi alvo da operação de manutenção;

d) data e hora da operação.

3.5.23 No caso de o instrumento utilizar um dispositivo controlador-indicador, este deve realizar a verificação da assinatura digital do pacote de dados a que se refere o item 3.5.13, e sinalizar se o resultado da operação de verificação for positivo.

3.5.24 Se o resultado da verificação da assinatura digital referida no item 3.5.23 for negativo, o funcionamento do dispositivo transdutor cuja verificação não foi positiva deve ser impedido até que seja realizada operação de manutenção pelo responsável autorizado pelo órgão metrológico, e uma mensagem de erro deve ser apresentada no dispositivo indicador.

3.5.25 Os eventos a que se refere o item 3.5.24 (interrupção de funcionamento do dispositivo transdutor e operação de manutenção do instrumento) devem ser armazenados nos registros de auditoria, da mesma forma como descrito nos itens 3.5.19 a 3.5.22.

3.5.26 Diferenças de arredondamento entre os resultados apresentados no dispositivo indicador e os resultados de medições provenientes do dispositivo transdutor não podem ser superiores aos erros máximos admissíveis para o instrumento.

3.5.26.1 As diferenças de arredondamento a que se refere este item devem ser avaliadas no dispositivo indicador.

3.5.26.2 As regras e operações utilizadas para arredondamento devem estar conforme definido nos itens 6.2.3.7 e 6.2.3.7.1 deste Regulamento Técnico Metrológico (Requisitos Técnicos).

3.5.27 O dispositivo indicador deve verificar se, para o pacote de dados recebido a que se refere o item 3.5.14, o valor denominado como "volume medido pelo dispositivo transdutor" (3.5.14.f) está conforme definido no item 3.5.26, quando comparado com o valor denominado como "volume total da transação" (3.5.14.g).

3.5.28 Se o resultado da verificação a que se refere o item 3.5.27 for negativo, o funcionamento do dispositivo transdutor envolvido na transação deve ser impedido até que seja realizada operação de manutenção pelo responsável autorizado pelo órgão metrológico, e uma mensagem de erro deve ser exibida.

3.5.29 O evento a que se refere o item 3.5.28 (interrupção de funcionamento do dispositivo transdutor) deve ser armazenado no mesmo registro de auditoria a que se refere o item 3.4.5 (Registro de Interrupções de Funcionamento do Instrumento).

3.5.30 O registro dos eventos a que se refere o item 3.5.29 devem conter as seguintes informações:

a) identificação do nível de acesso do responsável pela manutenção do instrumento;

b) o resultado da operação de manutenção

c) o código de identificação do dispositivo ou parte da bomba medidora que foi alvo da operação de manutenção;

d) data e hora da operação.

3.5.31 Não pode haver conexões de equipamentos auxiliares, não constantes na Portaria de Aprovação de Modelo, diretamente nas placas eletrônicas do dispositivo transdutor, controlador ou indicador.

3.5.32 As interfaces de comunicação do instrumento com equipamentos auxiliares externos devem ser protegidas contra tentativas de acessos não autorizados ou indevidos ao instrumento.

3.5.33 Os comandos dos protocolos de interface de comunicação com equipamentos auxiliares externos não devem alterar parâmetros, dados e software legalmente relevantes de forma diferente daquela declarada pelo fabricante.

3.6 Verificação de integridade de software

3.6.1 Deve ser disponibilizada uma interface de verificação metrológica no instrumento que será utilizada para:

a) acesso ao Registro de Alteração de Parâmetros Metrológicos Relevantes;

b) acesso ao Registro de Interrupções de Funcionamento do Instrumento;

c) acesso ao Registro de Eventos de Manutenção;

d) acesso ao Registro de Cargas de Software Legalmente Relevante;

e) acesso ao pacote de dados gerado e assinado digitalmente por cada dispositivo transdutor utilizado no último abastecimento, juntamente com o sua respectiva chave pública contida no certificado digital OM-BR.

f) execução do procedimento de verificação de integridade do software dos dispositivos transdutores e indicadores.

3.6.2 Para o instrumento bombas medidoras de combustíveis líquidos, a interface de verificação metrológica a que se refere o item 3.6.1 corresponde a uma interface de comunicação serial de dados padrão Bluetooth.

3.6.3 As especificações da interface de verificação metrológica, o respectivo protocolo de comunicação e o procedimento de verificação de integridade do software legalmente relevante são descritas na Norma NIT Sinst-020.

3.6.4 O nome do dispositivo Bluetooth utilizado para emparelhamento com dispositivos externos deve estar afixado em área visível sobre a superfície do instrumento, conforme descrito no item 7 deste Regulamento Técnico Metrológico (Inscrições Obrigatórias).

3.6.5 A operação de emparelhamento da interface Bluetooth com dispositivos externos deve ser possível em qualquer momento a partir do início de cada operação de abastecimento.

3.6.6 A identificação visual do nome do dispositivo Bluetooth a que se refere o item 3.6.4 deverá ser atualizada sempre que for necessária a substituição e/ou reconfiguração do dispositivo Bluetooth instalado na bomba medidora.

3.7 Documentação requerida para os requisitos gerais

3.7.1 As partes ou componentes do sistema de medição que realizem funções legalmente relevantes devem ser claramente identificadas, definidas e documentadas.

3.7.2 O requerente deve fornecer a documentação relacionada a seguir.

3.7.2.1 Descrição funcional do instrumento.

3.7.2.2 Manual operacional do instrumento.

3.7.2.3 Especificação do hardware contendo:

a) descrição completa do hardware contemplando arquitetura em módulos;

b) diagramas de blocos funcionais de cada módulo;

c) diagrama esquemático das placas e componentes;

d) especificação das interfaces de comunicação existentes incluindo seus tipos e protocolos de comunicação utilizados;

e) especificação de segurança do hardware criptográfico que armazena as chaves criptográficas e o processo de requisição e armazenamento do certificado digital ICP-Brasil

3.7.2.4 Descrição funcional da interface de usuário do instrumento, incluindo menus, diálogos e funções existentes que tenham efeitos em dados, parâmetros e software legalmente relevantes.

3.7.2.5 Lista de todas as funções que podem ser ativadas através da interface de usuário e que tenham efeitos em dados, parâmetros e software legalmente relevantes, com as correspondentes ações passíveis de serem desencadeadas no instrumento.

3.7.2.6 Descrição de como a versão de software é construída, como é organizada, e como pode ser visualizada.

3.7.2.7 Descrição das medidas de proteção contra uso fraudulento e intrusão inadmissível ou não autorizada, incluindo planos de selagem e meios eletrônicos e criptográficos.

3.7.2.8 Descrição das medidas de proteção contra carga ou modificações não autorizadas de software.

3.7.2.9 Descrição do procedimento de registro de alteração de parâmetros que definem características legalmente relevantes do instrumento e do formato dos dados armazenados.

3.7.2.10 Descrição das medidas de proteção contra alterações indevidas dos parâmetros que definem características legalmente relevantes do instrumento.

3.7.2.11 Descrição do meio técnico que garante inviolabilidade do dispositivo transdutor conforme item 3.3.16.

3.7.2.12 Lista de falhas detectáveis, descrição do algoritmo ou método de detecção, descrição da reação do instrumento à detecção de cada falha, conforme item 3.4.

3.7.2.13 Descrição do protocolo de comunicação entre o dispositivo transdutor e o dispositivo controlador, conforme item 3.5.1.

3.7.2.14 Descrição do meio que assegura a inviolabilidade das chaves criptográficas a que se referem os itens 3.5.3 e 3.5.5.

3.7.2.15 Descrição do procedimento de registro dos eventos de interrupção de funcionamento e de operações de manutenção do instrumento, e o formato dos dados armazenados.

3.7.2.16 Descrição do formato do pacote de dados assinado, conforme item 3.5.14.

3.7.2.17 Descrição do procedimento de extração dos certificados digitais armazenados nos dispositivos transdutores do instrumento, e também do modo de operação das ferramentas de hardware e software fornecidas para essa operação.

3.7.2.18 Especificação do algoritmo de assinatura digital utilizado, conforme item 3.5.3.

3.7.2.19 Acesso irrestrito ao código-fonte completo e comentado do software legalmente relevante dos dispositivos transdutor e indicador. Acesso ao código fonte dá-se no local de avaliação de modelo.

3.7.2.20 Descrição do procedimento de vinculação entre o dispositivo transdutor e os dispositivos indicadores, incluindo o registro da identificação unívoca do dispositivo transdutor e sua respectiva chave pública contida no certificado digital OM-BR.

3.8 Software e Hardware para avaliação de modelo

3.8.1 O requerente deve fornecer o software e hardware necessários para que os requisitos deste Anexo possam ser avaliados, incluindo: dispositivo transdutor, dispositivo controlador, dispositivo indicador, outros dispositivos, cabos de conexão, interfaces de hardware (de usuário, de comunicação, de verificação metrológica) e ferramentas de software e hardware necessárias para funcionamento e avaliação do instrumento.

3.9 Ensaios funcionais de requisitos gerais de software

3.9.1 A critério do Inmetro, os ensaios funcionais descritos na última versão da norma NIT-Sinst-022 podem ser realizados para evidenciar o cumprimento dos requisitos gerais de segurança de software e hardware.

4 REQUISITOS ESPECÍFICOS DE SOFTWARE E HARDWARE

4.1 O software e o hardware legalmente relevantes que empregarem as funcionalidades tecnológicas específicas a seguir devem satisfazer os requisitos técnicos correspondentes, adiante elencados.

4.2 Separação de software e/ou hardware

4.2.1 Todos os módulos de software e hardware do dispositivo transdutor e dispositivo indicador, que realizem funções legalmente relevantes, formam as partes legalmente relevantes do instrumento.

4.2.2 São consideradas partes legalmente relevantes do dispositivo transdutor os elementos de software e hardware que atuem desde o momento da aquisição de dados, geração da informação de volume medido, processamento desta informação até o momento da assinatura digital e, no dispositivo indicador, os elementos de software e hardware que atuem desde o recebimento da informação do abastecimento, conferência da assinatura digital até a publicação da informação de medição.

4.2.3 Partes legalmente relevantes do hardware e/ou do software do instrumento não podem ser inadmissivelmente influenciadas por comandos recebidos por meio de interfaces de comunicação ou de partes não legalmente relevantes do instrumento.

4.2.4 Deve haver uma correspondência unívoca e não ambígua entre cada comando emitido via interface (de usuário, de verificação metrológica, de comunicação ou de separação) e cada função iniciada no software legalmente relevante ou alterações de dados realizadas na parte legalmente relevante.

4.2.5 Se a separação de software e/ou hardware não for possível ou for desnecessária, o software e/ou o hardware dos dispositivos transdutores e indicadores, como um todo, será considerado legalmente relevante.

4.2.6 Todas as comunicações entre as partes legalmente relevantes e não legalmente relevantes devem ser realizadas exclusivamente por intermédio de uma interface de separação de software e/ou de hardware definida especificamente para este fim.

4.2.7 A partes legalmente relevantes do instrumento, incluindo a interface de separação, devem ser clara e completamente identificadas e documentadas.

4.2.8 O requerente deve declarar a completude dos comandos referido no item 4.2.7.

4.2.9 O resultado de medição não deve ser comprometido por atrasos ou bloqueios ocorridos pela realização de tarefas não legalmente relevantes.

4.3 Armazenamento e transmissão de dados em meio inseguro

4.3.1 No caso de transmissão de dados legalmente relevantes através de meio inseguro de comunicação ou armazenamento de dados para uso legalmente relevante futuro, estes devem ter sua autenticidade e integridade garantidas.

4.3.2 A autenticidade e integridade devem ser garantidas através da assinatura digital do pacote de dados a que se refere o item 3.5.14.

4.3.3 A assinatura digital do pacote de dados a que se refere o item 3.5.14 deve ser verificada pelo software e/ou hardware responsável por sua publicação ou processamento.

4.3.4 Se, no processo descrito em 4.3.3, alguma irregularidade for detectada, os dados devem ser descartados.

4.3.5 Componentes de software e/ou hardware que preparam dados legalmente relevantes para armazenamento ou transmissão, ou que realizam a verificação dos dados após leitura ou recepção, pertencem à parte legalmente relevante.

4.3.6 Chaves criptográficas privadas empregadas devem ser mantidas secretas e seguras internamente ao instrumento.

4.4 Carga de software legalmente relevante

4.4.1 Somente pode ser carregado no instrumento software submetido pelo requerente ao Inmetro e aprovado no processo de avaliação de modelo.

4.4.2 O instrumento não pode realizar medições durante o processo de carga de software legalmente relevante.

4.4.3 Ao final do procedimento de carga e instalação de novo software, o ambiente de proteção deve retornar ao mesmo nível de segurança declarado no processo de avaliação de modelo.

4.4.4 Devem ser empregados meios técnicos para garantir a autenticidade e integridade do software a ser carregado.

4.4.5 Se a autenticidade ou integridade do novo software não puderem ser verificadas, o instrumento deve descartá-lo e utilizar a versão anterior, ou tornar-se inoperante.

4.4.6 A carga e a tentativa de carga de software devem implicar no rompimento de lacres físicos, bem como no registro desta ação em um registro de auditoria implementado em memória não volátil (Registro de Cargas de Software Legalmente Relevante), da mesma forma como definido nos itens 3.3.10 a 3.3.15.

4.4.7 O registro dos eventos a que se refere o item 4.4.6 (carga ou tentativa de carga de software) deve conter os seguintes dados:

a) identificação do nível de acesso do responsável pela carga;

b) data e hora da carga, sucesso ou insucesso da carga, e;

c) as versões anterior e posterior à carga.

4.5 Carga de software não legalmente relevante

4.5.1 A carga de software não legalmente relevante pode ser realizada sem necessidade de sua aprovação pelo Inmetro

4.6 Arquiteturas que utilizam múltiplos dispositivos transdutores (N >1) para um mesmo abastecimento.

4.6.1 Ao final de cada abastecimento, cada dispositivo transdutor utilizado no abastecimento deve transmitir ao dispositivo indicador sua respectiva informação de totalização da medição por meio de pacotes de dados assinados digitalmente com a chave privada a que se refere o subitem 3.5.3.

4.6.2 Caso o fornecimento do combustível seja interrompido por um período de tempo superior a 60 segundos, cada dispositivo transdutor utilizado no abastecimento deve transmitir ao dispositivo indicador sua respectiva informação de totalização da medição por meio de pacotes de dados assinados digitalmente com a chave privada a que se refere o subitem 3.5.3.

4.6.3 Imediatamente após o recebimento dos pacotes de dados a que se refere o item 3.5.14, o dispositivo indicador deve verificar se cada um dos pacotes de dados recebidos tem como origem dispositivos transdutores distintos entre si.

4.6.4 Se o resultado da verificação a que se refere o item 4.6.3 for negativo, o funcionamento dos dispositivos transdutores envolvidos na transação deve ser impedido até que seja realizada operação de manutenção pelo responsável autorizado pelo órgão metrológico, e uma mensagem de erro deve ser exibida.

4.6.5 Imediatamente após o recebimento dos pacotes de dados a que se refere o item 3.5.14, o dispositivo indicador deve verificar se as informações constantes do pacote de dados denominadas como "identificador do abastecimento" (3.5.14.a), "volume total da transação" (3.5.14.g), "valor monetário total da transação" (3.5.14.h), "preço por litro" (3.5.14.i) e "data e hora" (3.5.14.j) são idênticas para todos os pacotes recebidos.

4.6.6 Se o resultado da verificação a que se refere o item 4.6.5 for negativo, o funcionamento dos dispositivos transdutores envolvidos na transação deve ser impedido até que seja realizada operação de manutenção pelo responsável autorizado pelo órgão metrológico, e uma mensagem de erro deve ser exibida.

4.6.7 Imediatamente após o recebimento dos pacotes de dados assinados a que se refere o item 3.5.13, a assinatura digital dos dispositivos transdutores envolvidos no abastecimento deve ser verificada pelo dispositivo indicador, que deve sinalizar se o resultado da operação de verificação foi positivo para todos os dispositivos envolvidos.

4.6.8 Se o resultado da verificação da assinatura digital a que se refere o item 4.6.7 for negativo para algum dos dispositivos transdutores envolvidos no abastecimento, o funcionamento deste dispositivo deve ser impedido até que seja verificado e liberado pelo responsável técnico autorizado pelo órgão metrológico, e uma mensagem de erro deve ser apresentada no dispositivo indicador.

4.6.9 O evento a que se refere o item 4.6.8 (interrupção de funcionamento do dispositivo transdutor) deve ser armazenado no mesmo registro de auditoria a que se refere o item 3.4.5 (Registro de Interrupções de Funcionamento do Instrumento).

4.6.10 O registro do evento a que se refere o item 4.6.9 deve conter os seguintes dados:

a) identificação do tipo de evento que gerou a interrupção no funcionamento do instrumento;

b) o no do dispositivo transdutor associado à falha identificada,

c) data e hora da interrupção.

4.6.11 Diferenças de arredondamento entre os resultados apresentados no dispositivo indicador e os resultados de medições provenientes da composição de medições de múltiplos transdutores não podem ser superiores aos erros máximos admissíveis para o instrumento.

4.6.11.1 As diferenças de arredondamento a que se refere este item devem ser avaliadas no dispositivo indicador.

4.6.11.2 As regras e operações utilizadas para arredondamento devem estar conforme definido nos itens 6.2.3.7 e 6.2.3.7.1 deste Regulamento Técnico Metrológico (Requisitos Técnicos).

4.6.12 O dispositivo indicador deve verificar se, para todos os pacotes de dados recebidos a que se refere o item 3.5.14, o resultado da soma de todos os valores denominados como "volume medido pelo dispositivo transdutor" (3.5.14.f) está conforme definido no item 4.6.11, quando comparado com o valor constante dos pacotes de dados denominado como "volume total da transação" (3.5.14.g).

4.6.13 Se o resultado da verificação a que se refere o item 4.6.12 for negativo, o funcionamento dos dispositivos transdutores envolvidos na transação deve ser impedido até que seja realizada operação de manutenção pelo responsável autorizado pelo órgão metrológico, e uma mensagem de erro deve ser exibida.

4.6.14 Os eventos a que se referem os itens 4.6.4, 4.6.6 e 4.6.13 (operação de manutenção do instrumento) devem ser armazenados no mesmo registro de auditoria a que se refere o item 3.4.7 (Registro de Eventos de Manutenção).

4.6.15 O registro dos eventos a que se refere o item 4.6.14 devem conter as seguintes informações:

a) identificação do nível de acesso do responsável pela manutenção do instrumento;

b) o resultado da operação de manutenção;

c) o código de identificação do dispositivo ou parte da bomba medidora que foi alvo da operação de manutenção;

d) data e hora da operação.

4.7 Documentação requerida para os requisitos específicos

4.7.1 Documentação requerida para separação de software e/ou hardware

4.7.1.1 Projeto da separação de software e/ou hardware; descrição e identificação dos módulos de software (programas, sub-rotinas, bibliotecas) e hardware (placas eletrônicas, componentes, transdutores) que realizem funções legalmente relevantes ou que contenham dados legalmente relevantes.

4.7.1.2 Descrição da interface de separação entre as partes legalmente relevantes e não legalmente relevantes.

4.7.1.3 Acesso irrestrito ao código-fonte do software legalmente relevante, incluindo a interface de separação.

4.7.1.4 Relação completa, descrição e funcionalidades dos comandos de interface de separação.

4.7.1.5 Declaração de completude dos comandos de interface de separação.

4.7.2 Documentação requerida para armazenamento e transmissão de dados legalmente relevantes

4.7.2.1 Descrição dos métodos que garantem autenticidade e integridade na transmissão ou armazenamento de dados.

4.7.2.2 Especificação do algoritmo de assinatura digital utilizado.

4.7.2.3 Descrição do meio e protocolo de transmissão e/ou armazenamento.

4.7.2.4 Código-fonte do software que prepara os dados para transmissão/ armazenamento e recepção/leitura.

4.7.2.5 Descrição das medidas que garantem a segurança das chaves criptográficas utilizadas.

4.7.3 Documentação requerida para carga de software legalmente relevante

4.7.3.1 Descrição do procedimento de carga de software legalmente relevante.

4.7.3.2 Descrição dos meios pelos quais se garante autenticidade e integridade do software a ser carregado.

4.7.3.3 Descrição do procedimento de registro das atualizações de software e o formato dos dados armazenados.

4.8 Ensaios funcionais de requisitos específicos de software e/ou hardware

4.8.1 A critério do Inmetro, os ensaios funcionais descritos na Norma Inmetro Técnica NIT-Sinst-022 podem ser realizados para evidenciar o cumprimento dos requisitos gerais de segurança de software e hardware.

5 ORGANIZAÇÃO E POSSE DA DOCUMENTAÇÃO E CÓDIGO FONTE

5.1 O requerente é o fiel depositário da documentação, incluindo o código fonte.

5.2 A documentação deve atender os seguintes requisitos:

a) O conteúdo do pacote de documentação a ser entregue deve ser organizado conforme descrito na NIT-Sinst-003;

b) O pacote de documentação deve ser compactado e armazenado de forma segura, ficando de posse do fabricante de forma permanente e disponível para acesso sob demanda do Inmetro;

c) Deve ser fornecido um resumo criptográfico, hash, desse arquivo compactado utilizando algoritmo criptográfico seguro;

d) Deve ser fornecido um hash para cada binário oriundo da compilação do código fonte legalmente relevante;

e) Deve ser estabelecido um procedimento seguro que permita demonstrar periodicamente ao Inmetro que está em posse do pacote de entrega, isto é, provar que possui a pré-imagem do hash à que se refere o item 5.2 alínea b) e demais documentos inclusos no pacote disponibilizado durante o processo de aprovação de modelo.

5.3 Os hashes a que se referem o item 5.2 (pacote de entrega e de cada um dos binários) devem ser declarados na portaria de aprovação de modelo.

6 DISPOSIÇÕES GERAIS

6.1 Manutenção e reparo

6.1.1 Ao dispositivo transdutor não é permitida manutenção e em caso de defeito deve ser devolvido ao fabricante e substituído por outro original.

6.2 Avaliação de Modelo

6.2.1 Todas as versões do software legalmente relevante do instrumento devem ser avaliadas e aprovadas pelo Inmetro previamente à sua carga no instrumento.

6.2.2 Em casos omissos, o Inmetro se reserva o direito de definir quais componentes de software e hardware são legalmente relevantes.

6.3 Segurança do processo de emissão de certificado digital para a bomba de combustível

6.3.1 É responsabilidade do fabricante sob supervisão do INMETRO garantir ambiente seguro e controlado para emissão de certificado digital padrão ICP-Brasil

6.3.2 O certificado digital e os algoritmos criptográficos utilizados no processo de assinatura digital mencionado neste RTM são definidos conforme regulamentos da ICP-Brasil e do Instituto Nacional de Tecnologia da Informação (ITI).

6.4 Verificações iniciais, subsequentes e inspeções

6.4.1 Nas verificações iniciais e subsequentes, o instrumento deve ter a integridade de seu software legalmente relevante verificada e os valores atuais dos parâmetros legalmente relevantes devem ser registrados.

6.4.2 Nas verificações, inicial, subsequentes e inspeções metrológicas, ou a qualquer momento, o instrumento que apresente mau funcionamento da interface de verificação metrológica deve ser interditado até que seja inspecionado, corrigido e liberado pelo responsável autorizado pelo órgão metrológico.