SUMÁRIO

1 OBJETIVO

Esta norma estabelece os conceitos básicos que permitirão aos técnicos envolvidos, na perícia, identificar as Placas de Circuito Impresso (PCI) que compõem o instrumento e descrever o procedimento de perícia em PCI´s de bombas medidoras de combustíveis. O procedimento de perícia é descrito em detalhes indicando os passos necessários na apreensão, registro e identificação de fraudes do material apreendido em campo.

2 CAMPO DE APLICAÇÃO

Esta Norma se aplica à Dimel/Disme e aos órgãos da Rede Brasileira de Metrologia Legal e Qualidade – Inmetro - RBMLQ-I.

3 RESPONSABILIDADE

A responsabilidade pela elaboração, revisão, aprovação, publicação ou cancelamento desta norma é da Dimel/Disme.

4 DOCUMENTOS DE REFERÊNCIA

Portaria MTE nº 598, de 07 de dezembro de 2004	Altera a Norma Regulamentadora nº 10, que trata de Instalações e Serviços em Eletricidade, aprovada pela Portaria nº 3.214, de 1978.
NR 10	Segurança em Instalações e Serviços em Eletricidade
VERÁSTEGUI, Thomaz Milton Navarro	Simulação Eletrodinâmica da Propagação de Modos entre Planos de Referência em Placas de Circuito Impresso – UFPR, 2007.
MANTECON, Vitor Sued	Instalações elétricas em atmosferas explosivas – UFRGS.

(continua)

DORO, Marcos Marinovic	Sistemática para implantação da garantia da qualidade em empresas montadoras de placas de circuito impresso (Dissertação) – UFSC, 2004.
Portaria Inmetro nº 150, de 29 de março de 2016.	Vocabulário Internacional de Termos de Metrologia Legal (VIML)
Portaria Inmetro/Dimel nº 133/2007	Autoriza a adaptação do sistema de gerenciamento, marca CARDDY, modelo BESS-01, em bombas medidoras de combustíveis líquidos eletrônicas. (Portaria Revogada)

5 DOCUMENTOS COMPLEMENTARES

NIT-Seflu-005	Verificação e inspeção de bomba medidora para combustíveis líquidos
FOR-Dimel-288	Laudo de perícia metrológica em bombas medidoras de combustíveis

6 SIGLAS

As siglas das UP/UO do Inmetro podem ser acessadas em: http://www.inmetro.gov.br/inmetro/pdf/regimento-interno.pdf.

AC	*Alternating Current* (Corrente Alternada)
ABNT	Associação Brasileira de Normas Técnicas
BMC	Bombas Medidoras de Combustíveis
CI	Circuito Integrado
CPU	*Central Processing Unit* (Unidade Central de Processamento)
DC	*Direct Current* (Corrente Contínua)
EIA	*Electronics Industry Association* (Associação da Indústria Eletrônica)
EEPROM ou E^2PROM	*Electrically-Erasable Programmable Read-Only Memory* (Memória não volátil, apagável eletricamente, somente de leitura)
EPROM	*Erasable Programmable Read-Only Memory* (Memória não volátil, apagável, somente de leitura)
ESD	*Electric Static Discharge* (Descarga de eletricidade estática)
Exi	Equipamento de Segurança Intrínseca
I/O	*Input / Output* (Entrada / Saída)
IS	Intrinsicamente Seguro
NR	Norma Regulamentadora
PAM	Portaria de Aprovação de Modelo
PCI	Placa de Circuito Impresso
Q2	Posição de Transistor
RAM	*Random Access Memory* (Memória volátil de acesso randômico)
RBMLQ-I	Rede Brasileira de Metrologia Legal e Qualidade - Inmetro
RF	Rádio Frequência
RS	*Recommended Standard* (Padrão recomendado)
SMD	*Surface-Mount Device* (Componente de montagem em superfície)
UFPR	Universidade Federal do Paraná
UFRGS	Universidade Federal do Rio Grande do Sul
UFSC	Universidade Federal de Santa Catarina

7 TERMOS E DEFINIÇÕES

7.1 Perícia

Para a presente norma, define-se como a análise técnica ou o exame comparativo que tem por fim examinar e certificar/demonstrar as condições em que se encontram as placas eletrônicas/PCI's ou acessórios da bomba medidora de combustíveis líquidos, determinando se apresentam características metrológicas de acordo com as exigências regulamentares aplicáveis.

7.2 *Pulser*

Dispositivo transdutor que transforma a vazão de combustível medida pelo bloco medidor de combustível líquido em pulsos elétricos.

7.3 Microcontrolador

Pode ser definido com um computador em um único *chip*, no mesmo *chip* estão integrados uma CPU e circuitos auxiliares (periféricos) como memória de dados, circuito de *clock*, interface de comunicação serial, temporizadores/contadores, portas de I/O, etc. Esses diferentes recursos embutidos em um microcontrolador variam em função do modelo e do fabricante. O microcontrolador é um dos principais componentes usados para fraude(s) de bombas medidoras de combustíveis citada(s) na presente norma.

7.4 Microprocessador

Componente que incorpora as funções de uma unidade central de computador (CPU) em um único circuito integrado. É um dispositivo multifuncional programável que aceita dados digitais como entrada, processa estes dados de acordo com as instruções armazenadas em sua memória, e fornece resultados como saída, operando com números e símbolos representados no sistema binário.

7.5 Rede RS-485

É um padrão de comunicação serial, também denominado EIA-485 por ser desenvolvido pela EIA (*Electronics Industry Association*), que também desenvolvem os padrões de comunicação serial: RS-232(EIA-232) e RS-422(EIA-422). O padrão RS-485 é baseado na transmissão diferencial de dados, através de um par trançado de fios, que é ideal para transmissão em altas velocidades, longas distâncias e em ambientes propícios a interferência eletromagnética. Ele permite a comunicação entre vários elementos participantes em uma mesma rede de dados.

7.6 Placa de rádio frequência

PCI que possui características especiais para a transmissão e recepção de dados por ondas de rádio, sem a necessidade de uso de fios para estabelecer a comunicação.

8 IDENTIFICAÇÃO DE UMA PCI

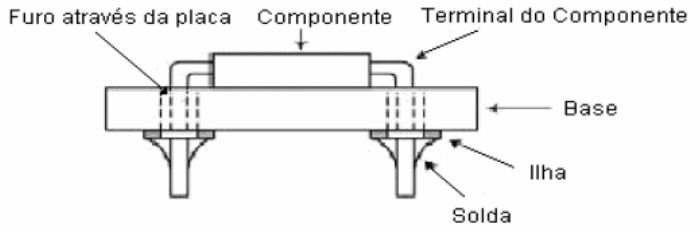
8.1 Características

8.1.1 Uma placa de circuito impresso – PCI pode ser definida como um suporte isolante de componentes eletrônicos, arranjados de tal forma a facilitar a ligação elétrica destes componentes através de trilhas impressas (fios planos) que correspondam a um projeto eletrônico (circuito) previamente desenvolvido para realizar uma ou mais funções, como por exemplo, uma placa de circuito impresso para um sintonizador de rádio.

8.2 Construção

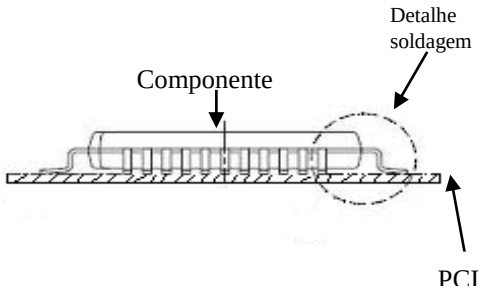
8.2.1 As placas de circuito impresso podem utilizar em sua montagem, basicamente dois tipos de componentes: componentes convencionais, também denominados *thru-hole*, que são montados com seus terminais inseridos em furos metalizados na PCI (Figura 1), ou os componentes de montagem em superfície – SMD – (*Surface -Mount Device*) cujos terminais são soldados na superfície da placa (Figura 2).

Figura 1 – PCI Comum



Fonte: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSJIiINeLuL9SCKL6emrpTYu6DOJJ8fdBWbUpy0omBARVfFeXOa

Figura 2 – PCI SMD



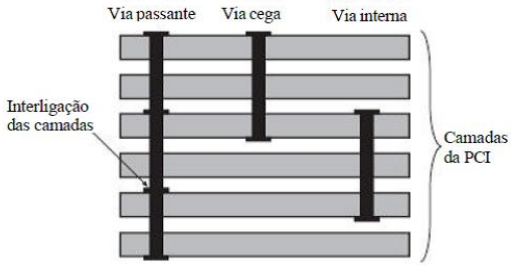
Fonte: http://www.emc.ufsc.br/controle/arquivos/estagio/relatorio/relatorio_2395_1161_1.pdf

8.2.2 As PCI's podem ser identificadas fisicamente quanto ao lado (face) que se deseja fazer referência. No lado da solda são realizadas as soldas dos componentes com suas respectivas ilhas. No lado dos componentes é possível observar os componentes da placa, sejam eles SMD ou convencionais. Tal informação é importante quando se deseja identificar claramente em documentos um componente ou conexão elétrica na PCI.

8.2.3 A evolução tecnológica foi capaz de produzir placas com duas ou mais camadas de trilhas condutoras, que nada mais são do que os "fios" que interligam um componente a outro (Figura 3). Esta

tecnologia visa facilitar a miniaturização de circuitos e aumentar sua velocidade de resposta entre outros benefícios.

Figura 3 – PCI Multicamadas



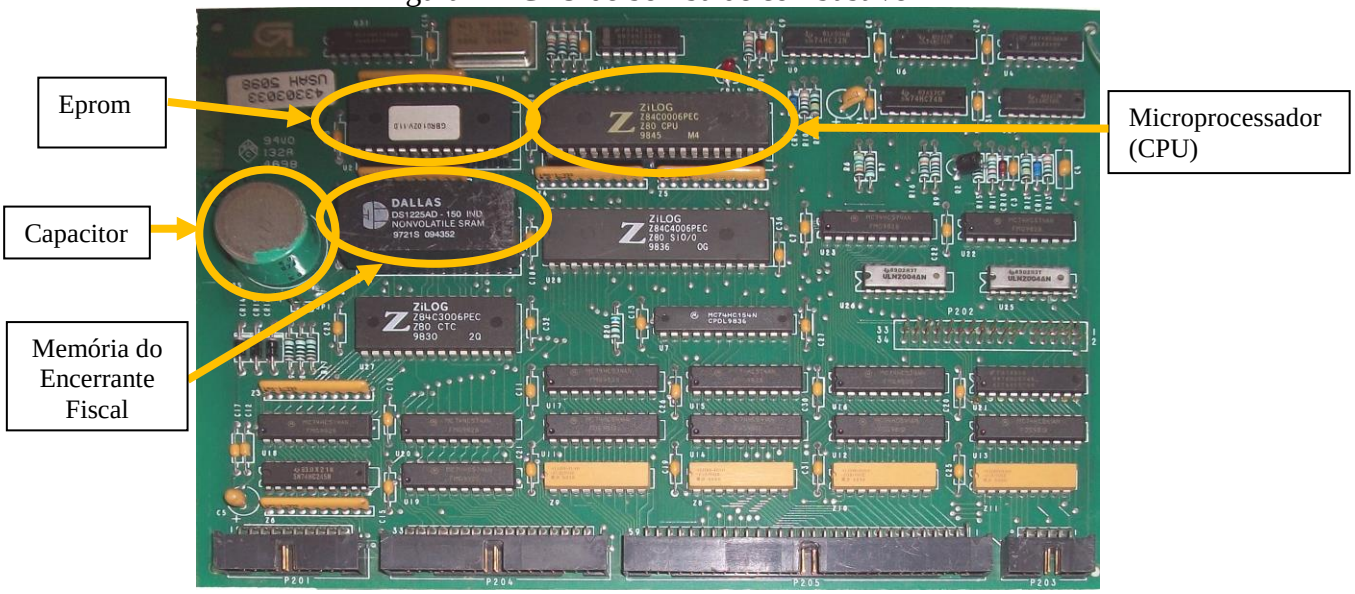
Fonte: http://www.emc.ufsc.br/controle/arquivos/estagio/relatorio/relatorio_2395_1161_1.pdf

8.3 Aplicações

8.3.1 As PCI's em BMC – Bombas Medidoras de Combustíveis são identificadas quanto à utilização prática para qual foram projetadas, podendo ser divididas em campos de aplicação genéricos:

a) CPU – *Central Processing Unit* (Unidade de central de processamento) é um tipo de placa onde estão reunidos componentes denominados processadores, onde são realizadas instruções de um programa de computador para executar o controle do instrumento, o cálculo da medida a partir da informação dos seus transdutores e preparação dos dados para apresentação. Normalmente placas CPU também apresentam componentes para armazenamento de informações, tais como memórias voláteis e/ou não voláteis denominados RAM e EEPROM, respectivamente. Estas memórias são utilizadas pela CPU para armazenar resultados das entradas e saídas do processamento, como também podem armazenar o programa que será executado pelo processador. As placas CPU permitem ainda a implementação, opcional, de sistemas de automação do posto de gasolina. A automação consiste no estabelecimento de um canal de comunicação entre as bombas de um posto e um computador central. Com a automação é possível ao gerente do posto controlar o uso das bombas, as quantidades de combustível vendidas, a produtividade de seus funcionários, entre outras coisas. E por sua natureza de controle e processamento, as placas de CPU podem ser alvo de mudanças intencionais com a finalidade de fraudes metrológicas. A Figura 4 apresenta uma placa CPU e seus principais componentes;

Figura 4 – CPU de bomba de combustível



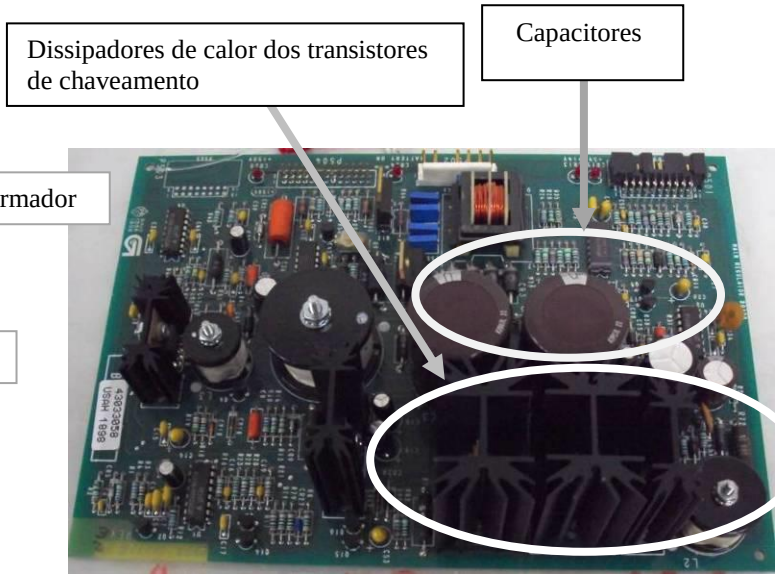
Fonte: Disme/Sinst

b) fonte – Placa de circuito impresso que está presente em quase todos os equipamentos ou que está integrada a outra placa sob a forma de um subcircuito adjacente. A placa da fonte, ou simplesmente a fonte, é a responsável pelo suprimento de energia às demais partes de um equipamento com níveis de tensão e correntes compatíveis a cada parte. Comumente são providas de transformadores e capacitores eletrolíticos de alta capacidade, (Figuras 5 e 6). Os transformadores são responsáveis em prover o acoplamento entre níveis de tensão da rede onde o equipamento está ligado e os demais circuitos internos do equipamento sob ela alimentados. Os capacitores presentes nas fontes de alimentação, normalmente são capazes de armazenar cargas elevadas e perigosas por longos períodos de tempo e recomenda-se descarrega-los através de uma carga resistiva antes de manusear as PCI. Quando possível, recomenda-se desconectar a fonte dos demais circuitos para evitar acidentes/danos;

Figura 5 - Fonte AC

Fonte: Disme/Sinst

Figura 6 - Fonte DC regulada



Fonte: Disme/Sinst

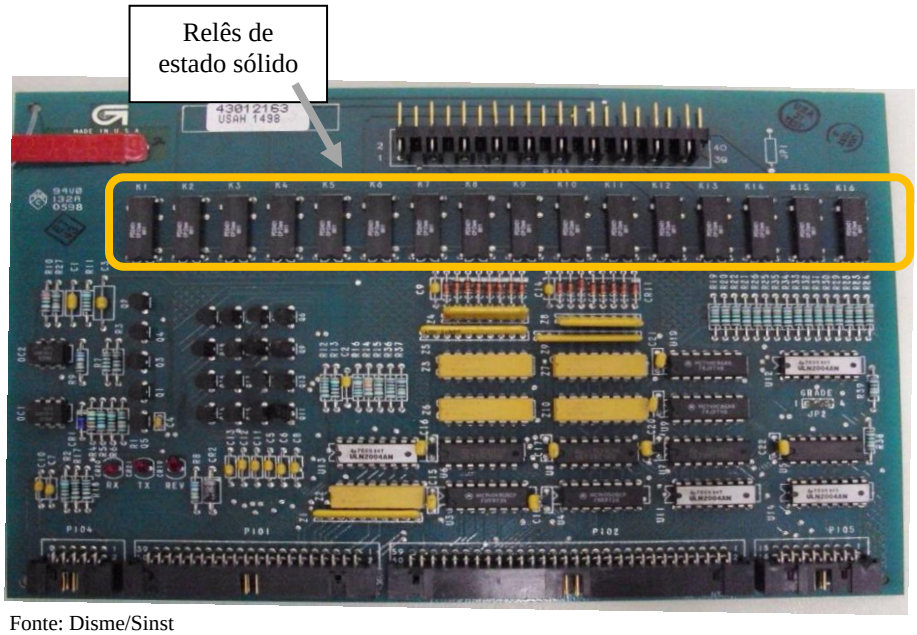
c) teclado – Interface presente na maioria dos equipamentos que necessitam realizar tarefas onde o operador digita informações através de botões ou membranas sensíveis ao toque como, por exemplo, no micro-ondas. Estas placas normalmente são passivas e não possuem grande relevância ao restante do circuito, podendo ser desconectadas ou substituídas sem grande prejuízo ao funcionamento principal dos demais circuitos (Figura 7);

Figura 7 - Teclado

Fonte: Disme/Sinst

d) interfaces de controle (ou hidráulica) – Nesta PCI, são acondicionados componentes acionadores de grandes cargas, como por exemplo, motores e válvulas solenóides que controlam vazão de líquidos, gases ou motores de bombas. Podem também acionar contactoras eletromecânicas para acionamento de cargas trifásicas através de um pulso monofásico. Outra característica comum é sua interligação a placa CPU, por onde receberá seus comandos. Pela sua natureza de controle de processos físicos, estas placas são alvo de intervenções intencionais para fraudes metrológicas como a inclusão de componentes estranhos as especificações originais ou a troca de componentes passivos por componentes "inteligentes" (Figura 8);

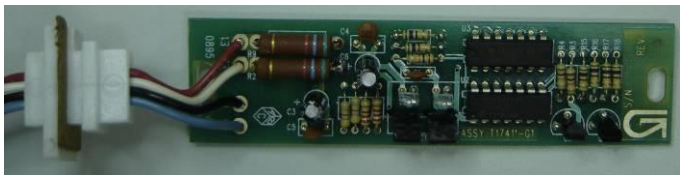
Figura 8 – Interface Hidráulica



Fonte: Disme/Sinst

e) sensores e transdutores – Algumas placas de circuito impresso podem estar associadas a funções de interligação a sensores diversos, como termômetros, sensores de posição, foto receptores, etc. A função destas PCI's é prover um acoplamento (medição ou identificação) entre um determinado fenômeno físico e demais circuitos onde esta informação será tratada. Pela sua natureza de entrada de informações é muito comum ser alvo de alterações intencionais para a realização de fraudes metrológicas, onde a grandeza medida está sendo influenciada ou alterada por componentes estranhos às especificações originais; Na Figura 9 é apresentado um tipo muito comum de PCI encontrada no interior do *pulser* e na Figura 10 sua caixa de proteção utilizada também para fixação na bomba de combustível; e

Figura 9 – PCI do *Pulser*



Fonte: Disme/Sinst

Figura 10 – Caixa do *Pulser*

Fonte: Disme/Sinst

f) barreiras de segurança – Algumas PCI's promovem nível de segurança requerido para áreas classificadas, como no caso dos postos de combustíveis. Estas placas são projetadas de forma a garantir que não seja possível formar energia de ignição suficiente para inflamar a atmosfera explosiva em que determinado circuito esteja operando. Estas áreas são denominadas pela ABNT como Zonas 1 e 0. Tais equipamentos (barreiras) recebem a denominação **Exi** – Intrinsicamente Seguros. Nas bombas de combustíveis, estas PCI's estão ligadas em série entre sensores/transdutores e a PCI que recebe as informações destes sensores/transdutores, por este motivo podem ser alvo de alteração intencional com intuito de realizar fraudes. Na Figura 11 é apresentada uma típica PCI de proteção **Exi.**

Figura 11 - Barreira de proteção IS (ou Barreiras de segurança)

Fonte: Disme/Sinst

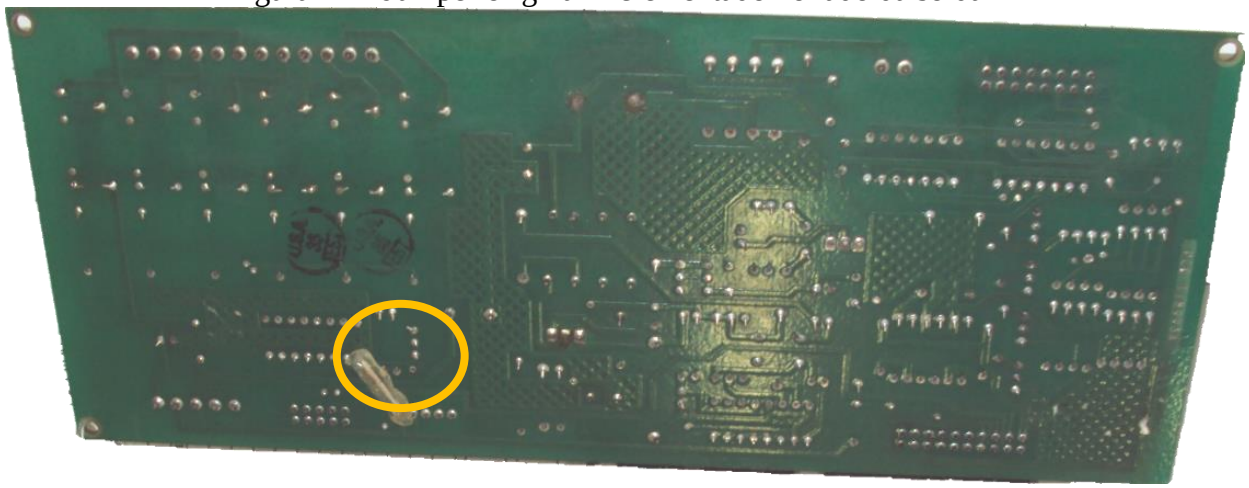
8.4 Alterações Permitidas nas PCI

8.4.1 As PCI's ao longo de sua vida útil são sujeitas a receberem modificações técnicas que não necessariamente representam fraudes metrológicas.

8.5 Manutenções

8.5.1 As manutenções corretivas realizadas em PCI nem sempre preservam todas as características originais da placa, sem, contudo, afetar seu funcionamento e desempenho. Algumas intervenções são feitas por necessidade de se refazer uma trilha, cujo rompimento foi ocasionado por curtos-circuitos. Este tipo de manutenção é normalmente realizado com a inserção de um fio curto (jumper) ligando pontos da placa, a fim de refazer o caminho original da trilha, conforme demonstrado na Figura 12. É comum ainda ocorrer a substituição de componentes danificados. Neste caso é possível perceber vestígios da manutenção a partir da coloração da solda e da placa.

Figura 12 – Jumper original incrementado no lado da solda



Fonte: Disme/Sinst

8.6 Implementações em Fábrica

8.6.1 As PCI's após serem fabricadas, podem sofrer alterações intencionais a fim de corrigir alguma falha de projeto, sem alterar seu desempenho desejado. Isso se dá pelo fato de algumas falhas só serem detectadas após o processo de fabricação, onde milhares de placas já foram fabricadas e medidas corretivas só poderão ser implementadas em outro lote (versão de placa). Até que essas medidas estejam implementadas, as placas são corrigidas com incremento de fios ou componentes extras para sanar a falha, conforme pode ser demonstrado nas Figuras 13 e 14.

Figura 13 – Capacitores originais incrementados na PCI após fabricação

Fonte: Disme/Sinst

Figura 14 – Inclusão de componente original

Fonte: Disme/Sinst

9 PROCEDIMENTO DE EXAME

9.1 Exames do Instrumento em Campo

9.1.1 Ensaios Metrológicos

9.1.1.1 Os ensaios metrológicos aplicáveis deverão ser realizados imediatamente na chegada ao posto, sem que haja tempo de qualquer mudança das condições de seu funcionamento. É altamente recomendável evitar que se proceda ao desligamento das bombas antes de se realizar os ensaios metrológicos, pois já se constatou que esse procedimento desabilita possíveis fraudes. Os ensaios metrológicos devem seguir o que preconiza a NIT-Seflu-005

9.1.2 Preenchimento do Registro de Medição

9.1.2.1 Durante a realização dos ensaios metrológicos, deve-se proceder ao preenchimento do registro de medição preferencialmente pelo SGI (registro de medições para bomba medidora de combustíveis líquidos). Na ausência deste, o preenchimento do registro de medição deve ser feito em documento próprio do órgão delegado ou ainda utilizando o Anexo A da NIT-Seflu-005. Cada instrumento de medição (bomba) deve ser univocamente identificado através de seu número de série, marca, modelo, número do Inmetro e/ou qualquer outra informação relevante para sua perfeita identificação.

9.1.3 Preenchimento do Auto de Apreensão

9.1.3.1 Todo material apreendido deve estar univocamente identificado em Auto de Apreensão próprio do órgão delegado, constando, no mínimo, as seguintes informações:

a) nome ou razão social do posto de combustível;
b) endereço completo;
c) CNPJ ou CPF;
d) identificação do instrumento (marca, modelo, nº de série, portaria de aprovação);
e) identificação dos itens apreendidos (PCI, *Pulser*, etc.) por meio de lacre de segurança vermelho preso com fio de nylon;
f) indicação do instrumento de medição ao qual pertencem os itens apreendidos; e
g) indicação do instrumento/item apreendido ao qual corresponde o registro de medição.

9.2 Cuidados

9.2.1 Desenergização

9.2.1.1 Antes de proceder a desenergização e desmontagem da bomba de combustível, realize todos os testes metrológicos cabíveis e preencha o laudo de medição para documentar o comportamento do instrumento no momento da fiscalização.

9.2.1.2 Antes de iniciar qualquer desmontagem, proceda ao desligamento da bomba de combustível no quadro de disjuntores mais próximo, sinalize indicando com a frase: "Não religar". Providencie o travamento do disjuntor ou do quadro de alimentação onde este se encontra para evitar religamento não intencional. Constate através de indicador de tensão ou voltímetro apropriado a total desenergização do

ponto de entrega de alimentação da bomba. Certifique-se que o instrumento utilizado para constatar a ausência de tensão esteja funcionando, fazendo um teste em um circuito conhecidamente energizado antes de testar seu circuito não energizado.

9.2.2 Desmontagem

9.2.2.1 Efetue a desmontagem utilizando chaves e ferramentas adequadas a cada tipo de bomba medidora. Caso seja necessário deixar a bomba desmontada (sem as placas) procure preservar os parafusos originais fixando-os novamente ou depositando estes em algum recipiente dentro da própria bomba medidora.

9.2.2.2 Certifique-se que não existam pontas de fios expostas que possam provocar curto-circuito após a desmontagem.

9.2.3 Conectores

9.2.3.1 As PCI's geralmente apresentam conectores onde são ligados cabos elétricos. Estes cabos são responsáveis pela comunicação/transmissão de sinais entre a PCI que se deseja retirar e as demais placas da bomba de combustível. Os cabos precisam ser desconectados antes da remoção da PCI de sua bomba. No momento da desconexão destes cabos, recomenda-se não utilizar os fios para puxar os conectores, pois isso pode ocasionar o rompimento destes. Segure o conector em sua base para realizar a extração, se necessário utilize uma chave de fenda pequena para servir como alavanca. Tome cuidado para não danificar os pinos, pois estes são muito frágeis e podem ser entortados com facilidade. Faça uma marcação nos cabos utilizando uma caneta e/ou fita para facilitar sua remontagem antes de desconectá-los.

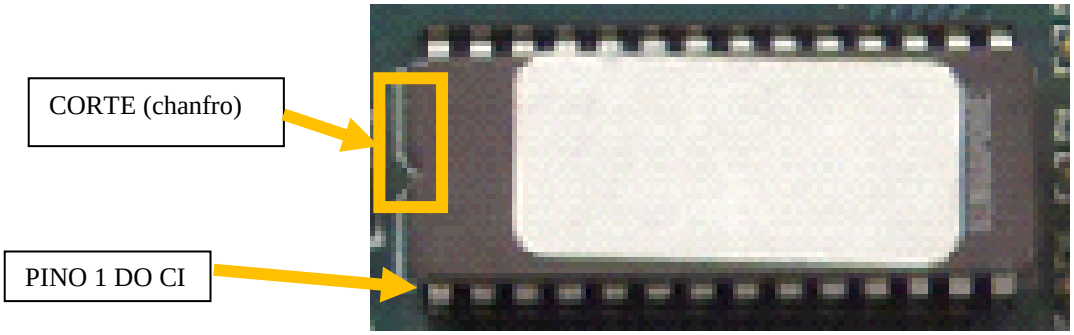
9.2.3.2 Siga se possível, uma sequência de desmontagem dos conectores removendo:

a) os conectores da fonte principal;
b) sensores (*pulser*);
c) conectores de comunicação;
d) outros; e
e) aterramentos, se houver.

9.2.4 Circuitos Integrados Montados em Soquetes

9.2.4.1 Alguns CI's são montados em soquetes que permitem sua retirada sem o uso de ferramentas para remoção de solda, como é o caso das memórias EPROM e das memórias de encerrante fiscal. Recomenda-se o uso de ferramental apropriado para a extração deste tipo de componente, ou na ausência desta, o uso de uma pequena chave de fenda para forçar sua saída sem danificar o componente. Ao se recolocar este tipo de CI, deve-se verificar que todos os pinos estão devidamente alinhados, pois facilmente são entortados ou danificados. Este tipo de componente apresenta uma marcação em seu encapsulamento que diferencia seu pino inicial (pino 1) conforme indicado pela figura 15. O componente deve ser recolocado na sua posição original.

Figura 15 – Detalhe do corte que indica o pino 1 do CI e sua posição na PCI



Fonte: Disme/Sinst

9.3 Placas a Serem Inspecionadas

9.3.1 As PCI que deverão ser alvo de uma perícia são as seguintes:

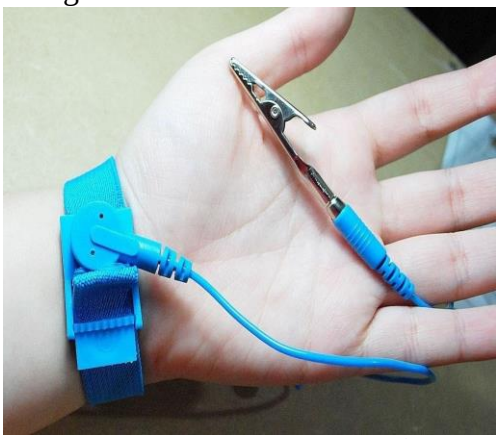
a) PCI CPU;
b) PCI Interface Hidráulica (quando houver); e
c) *Pulser*.

9.4 Manuseio

9.4.1 Ao manusear uma PCI, utilize suas bordas (arestas) para segurar, evitando assim contato desnecessário sobre os componentes. Alguns componentes são sensíveis à energia estática que pode estar presente no corpo humano. Ao manusear uma PCI é altamente recomendável utilizar uma pulseira antiestática (Figura 16), devidamente aterrada a fim de evitar danos aos componentes sensíveis da PCI.

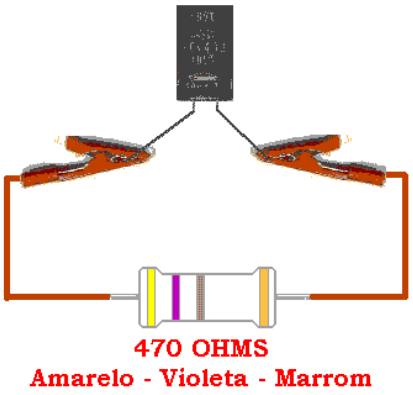
9.4.2 Nas fontes onde há presença de capacitores com baixa tensão contínua (NR-10) (entre 120 V e 1500 V DC) é recomendado descarregá-los antes do manuseio utilizando um resistor entre 47 Ω a 1 kΩ (1 W) montado previamente em uma giga de teste apropriada como na Figura 17. Não descarregue capacitores em áreas com atmosfera potencialmente explosivas, pois a descarga pode gerar fagulhas de ignição.

Figura 16 - Pulseira Antiestática



Fonte: https://i.ytimg.com/vi/n9_Q1GG5TII/maxresdefault.jpg

Figura 17 - Resistor de descarga



Fonte: http://www.oocities.org/br/alditeceletronica/CAPC.GIF

9.5 Transporte

9.5.1 O transporte de uma PCI é feito tomando cuidados especiais quanto a impactos, aquecimento, exposição a luz solar e a descargas eletrostáticas. Para o transporte de placas, o emissor tem que providenciar inicialmente sua identificação unívoca através de lacre preso com fio de nylon e sua embalagem em plástico bolha com proteção antiestática (ESD). As placas envolvidas em plástico bolha podem ser presas com um elástico, conforme Figura 18 (d). Depois de embaladas, as placas serão acondicionadas em caixas de papelão, devidamente protegidas contra impactos mecânicos. Aconselha-se sinalizar com uma etiqueta do lado de fora da caixa com a frase - "CUIDADO FRÁGIL".

Figura 18 – Plástico bolha com proteção ESD

(A)

(B)

(C)

(D)

Fonte: Disme/Sinst

9.6 Registro e Classificação do Material Apreendido

9.6.1 Todo material apreendido deve ser registrado em auto de apreensão próprio, relacionando-se cada item a bomba medidora de origem e ao bico de medição de origem, de forma que se mantenha uma cadeia ininterrupta de rastreabilidade do material apreendido ao local físico de origem de sua instalação/uso.

9.7 Inspeção Visual

9.7.1 A identificação das fraudes conhecidas se realizará por inspeção visual das PCI's comparando-se com as informações constantes no Anexo A da presente norma. Os casos omissos e suspeitos de fraudes ainda não confirmadas deverão ser enviados ao Inmetro, para análise em laboratório.

9.8 Emissão de Laudos de Perícia em Laboratório

9.8.1 Os laudos de perícia do Inmetro deverão ser emitidos/registrados conforme FOR-Dimel-288.

9.8.2 Os órgãos da RBMLQ-I usarão o FOR-Dimel-288 ou poderão adaptar o FOR-Dimel-288, desde que mantidas as informações solicitadas por ele.

10 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
00	Out/2022	▪ Esta Norma cancela e substitui a NIT-Sinst-002 rev02.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborada por:	Juliana Wilm Guedes	Auxiliar Adminstrativo
Verificado por:	Railson Oliveira Motta	Pesquisador –Tecnologista em Metrologia e Qualidade
Aprovado por:	Roberto Lima do Amaral	Chefe substituto da Disme

_____

/ANEXO A

ANEXO A – INSPEÇÃO VISUAL DE FRAUDES CONHECIDAS

A-1 O objetivo deste anexo é apresentar imagens e características das fraudes conhecidas até o momento. De posse deste material, o agente metrológico poderá identificar uma fraude em campo e atestar sua existência através de laudos de perícia tomando como base os casos aqui apresentados. As fraudes foram classificadas primeiramente de acordo com sua localização (*pulser*, placas de interface hidráulica, placas CPU e seus respectivos cabos de comunicação). Para cada tipo de fraude são apresentadas figuras ilustrando a forma como são implementadas e suas características são resumidas em tabelas.

A-2 FRAUDES EM TRANSDUTORES (*PULSER*)

A-2.1 Fraude em *Pulser* Utilizando Dois Discos

A-2.1.1 A Tabela 1 a seguir apresenta as características dessa fraude.

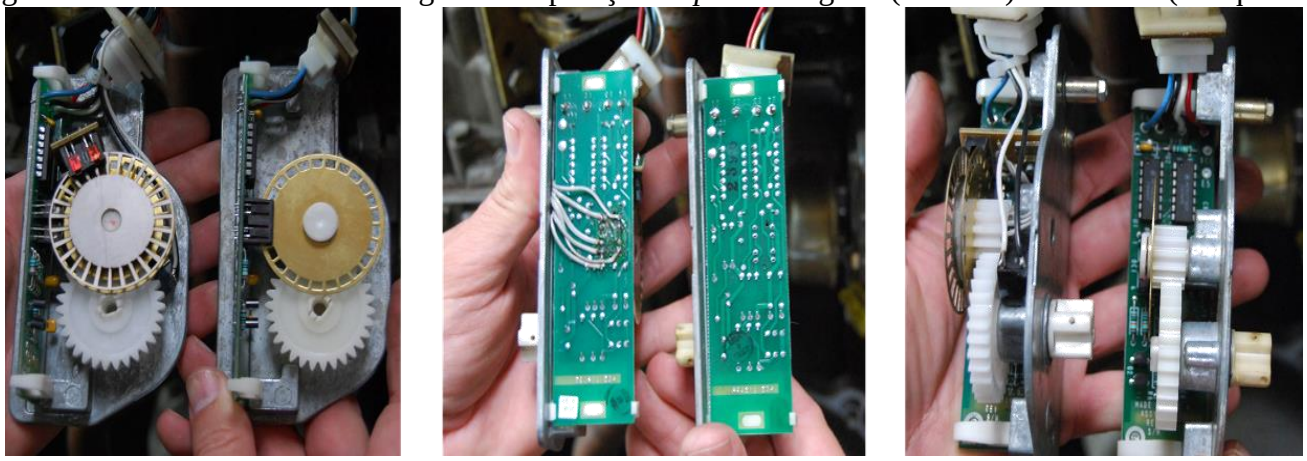
Tabela 1 – Características da fraude apresentada nas figuras A1, A2, A3 e A4

Componentes da fraude	Placa original do *pulser* com alterações Sensor óptico adicional Disco perfurado adicional com mais furos Fios adicionais
Operação	São acrescentados pulsos adicionais à quantidade original de pulsos gerados pelo transdutor da bomba através da utilização do disco com mais furos e respectivo sensor óptico. O disco e o sensor óptico originais são mantidos com o objetivo de a bomba funcionar corretamente no caso de uma verificação/fiscalização.
Forma de acionamento/inibição	O disco e o sensor adicionais são ativados através de comandos remotos recebidos por um circuito receptor de RF (PCI ou receptor comercial) que atuam em conjunto com pequenos relés eletromecânicos.
Efeito	O resultado [da medição] apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Seu valor pode variar entre -3% e -12%.

Fonte: Disme/Sinst

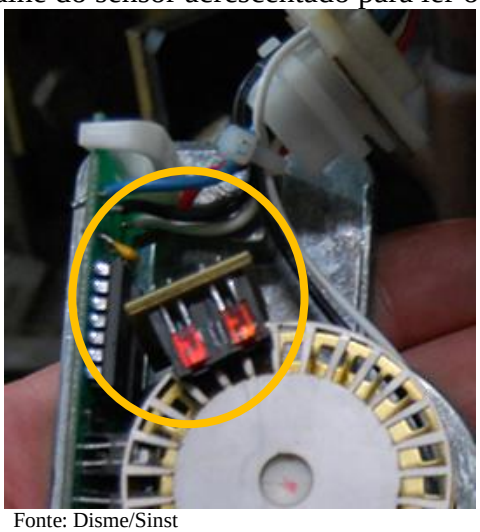
A-2.1.2 Nas figuras A2, A3 e A4 são apresentados os detalhes de implementação da fraude. Na figura A1 é apresentada uma sequência de três fotos onde se compara, em cada uma delas, um *pulser* original (a direita) e um *pulser* fraudado (a esquerda).

Figura A1 – Em cada uma das imagens: comparação de *pulser* original (à direita) e fraudado (à esquerda).



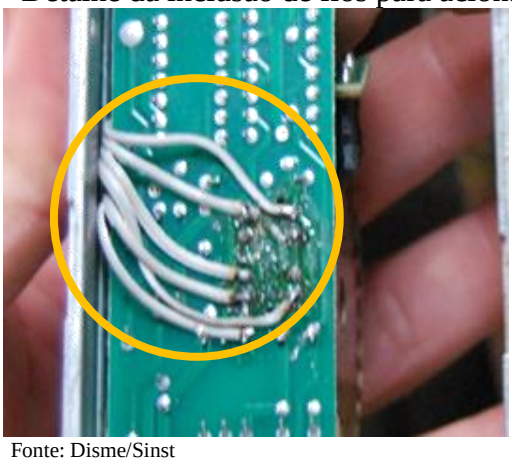
Fonte: Disme/Sinst

Figura A2 – Detalhe do sensor acrescentado para ler o disco fraudador.



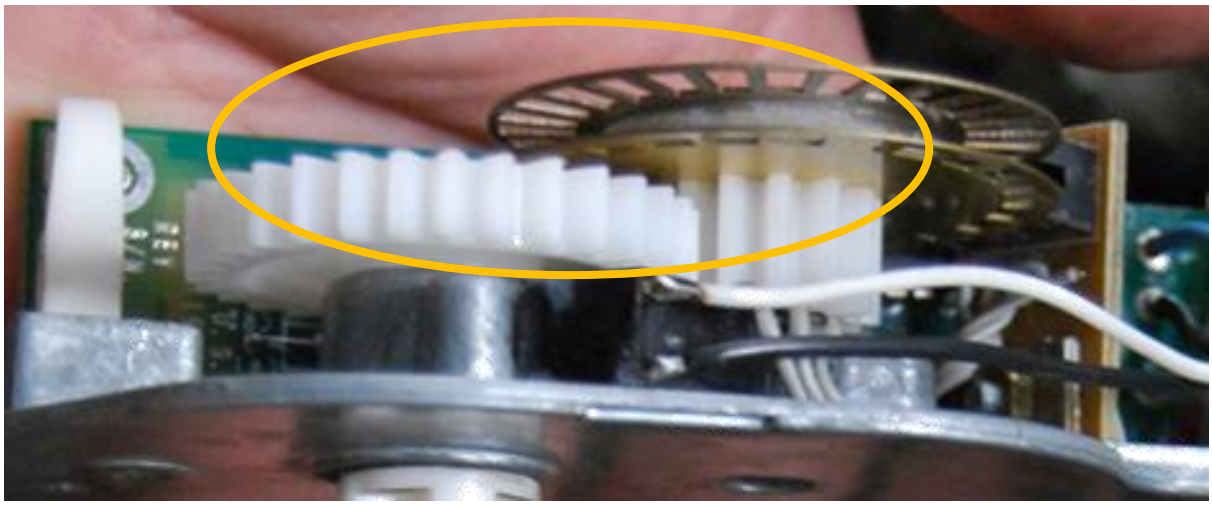
Fonte: Disme/Sinst

Figura A3 – Detalhe da inclusão de fios para acionar a fraude.



Fonte: Disme/Sinst

Figura A4 – Detalhe da inclusão do disco fraudador acima do original.



A-2.2 Fraude em *Pulser* Utilizando Receptor de RF e Microcontrolador

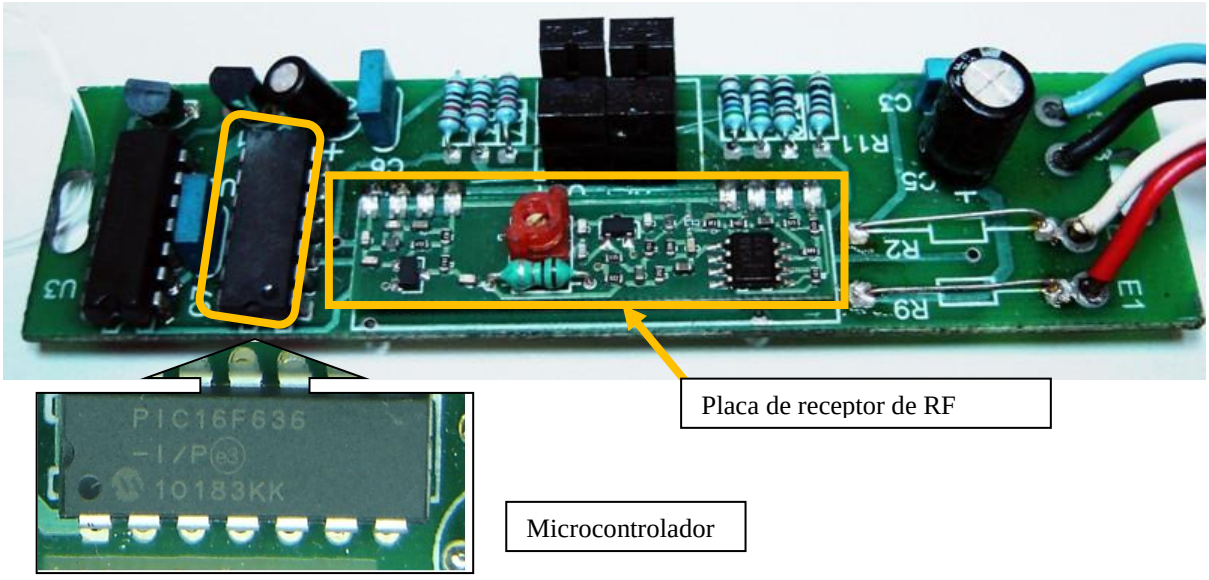
A-2.2.1 A tabela 2 e a figura A5 a seguir apresentam as características dessa fraude.

Tabela 2 – Características da fraude apresentada na figura A5

Componentes da fraude	Placa falsa do *pulser* Placa receptora de RF sobreposta à placa do *pulser* (Fig. A5 – centro) Microcontrolador (Fig. A5 – esquerda)
Operação	O microcontrolador presente na placa do *pulser* incrementa a quantidade de pulsos gerada em um abastecimento.
Forma de acionamento/inibição	Por controle remoto. O receptor de RF recebe comandos oriundos de um transmissor (controle remoto) e, atuando no microcontrolador, ativa/desativa a fraude. A desativação da fraude também pode ser feita pela interrupção do fornecimento de energia da bomba. Quando a bomba for novamente energizada a fraude estará sempre desativada. Por este motivo recomenda-se realizar os ensaios metrológicos imediatamente ao chegar ao posto e não permitir o desligamento das bombas.
Efeito	O resultado apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Os valores típicos de erro percentual encontrados para este tipo de fraude variam entre -3% e -12%.

Fonte: Disme/Sinst

Figura A5 – PCI falsa de *pulser* com inclusão de receptor de RF e microcontrolador



Fonte: Disme/Sinst

A-2.3 Fraude em *Pulser* Utilizando Microcontrolador

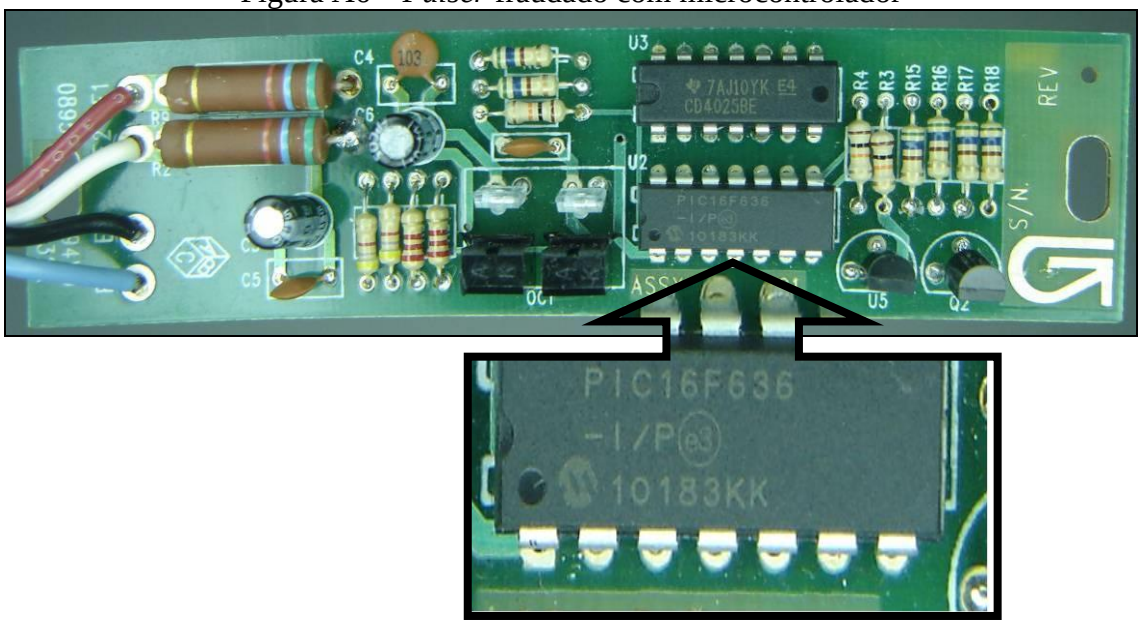
A-2.3.1 A tabela 3 e as figuras A6, A7 e A8 a seguir apresentam as características dessa fraude.

Tabela 3 – Características da fraude apresentada nas figuras A6, A7 e A8

Componentes da fraude	Placa falsa do *pulser*, muito similar à original Microcontrolador Receptor comercial de RF Contator
Operação	O microcontrolador presente na placa do *pulser* incrementa a quantidade de pulsos gerada em um abastecimento.
Forma de acionamento/inibição	Uma sequência de comandos liga/desliga, normalmente enviados por controle remoto. O microcontrolador é programado para identificar uma sequência específica de interrupções da energia da bomba (sequência liga/desliga). Quando a sequência correta é detectada, a fraude é ativada. A inibição da fraude é feita pela interrupção do fornecimento de energia da bomba. Quando a bomba for novamente energizada a fraude estará desativada. Por este motivo recomenda-se realizar os ensaios metrológicos imediatamente ao chegar ao posto e não permitir o desligamento das bombas. O sistema de ativação da fraude inclui ainda um receptor comercial de RF e um contator conectado ao circuito de alimentação da bomba, os quais implementam a sequência liga/desliga de acionamento da fraude.
Efeito	O resultado apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Os valores típicos de erro percentual encontrados para este tipo de fraude variam entre -3% e -12%.

Fonte: Disme/Sinst

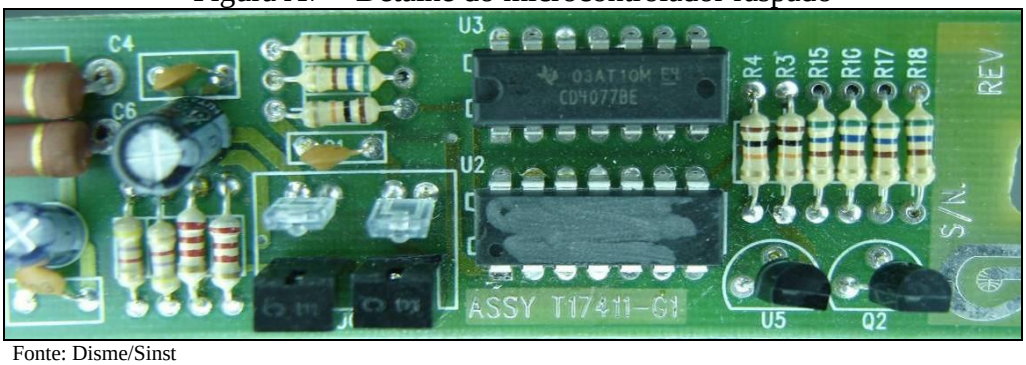
Figura A6 – *Pulser* fraudado com microcontrolador



Fonte: Disme/Sinst

A-2.3.2 Na maioria das vezes, este microcontrolador encontra-se com sua identificação raspada, como na figura A7:

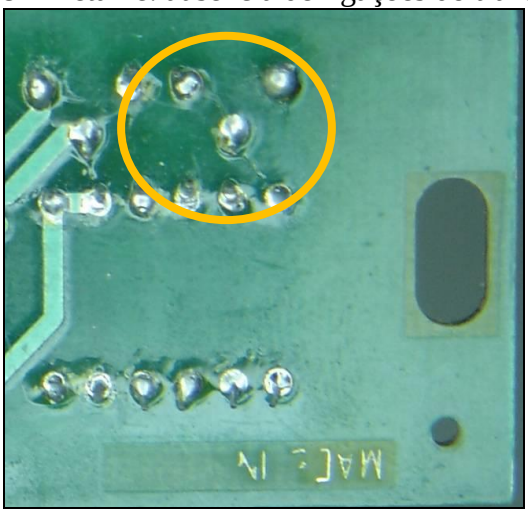
Figura A7 – Detalhe do microcontrolador raspado



Fonte: Disme/Sinst

A-2.3.3 Este tipo de fraude usa uma PCI falsa praticamente idêntica a original. Uma forma de diferenciá-la é através do microcontrolador ou do transistor Q2 que fica localizado ao lado direito da imagem acima. Este transistor foi colocado somente para que a PCI falsa tenha a mesma aparência da original. Seus terminais na verdade não estão ligados a nenhum outro componente conforme apresentado na figura A8 a seguir:

Figura A8 – Detalhe: ausência de ligações do transistor Q2

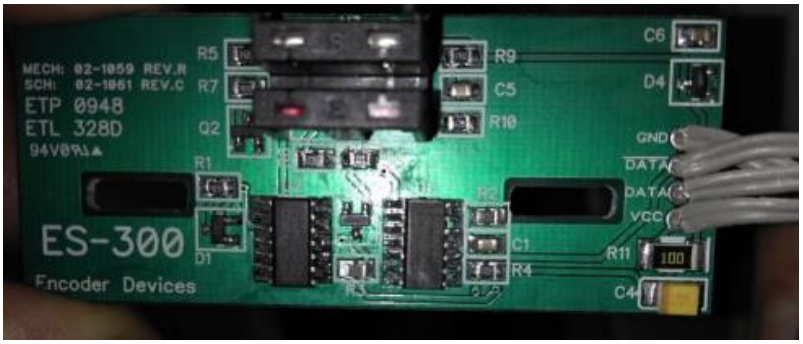


Fonte: Disme/Sinst

A-2.4 Fraude em *Pulser* por Troca de Componentes na Placa

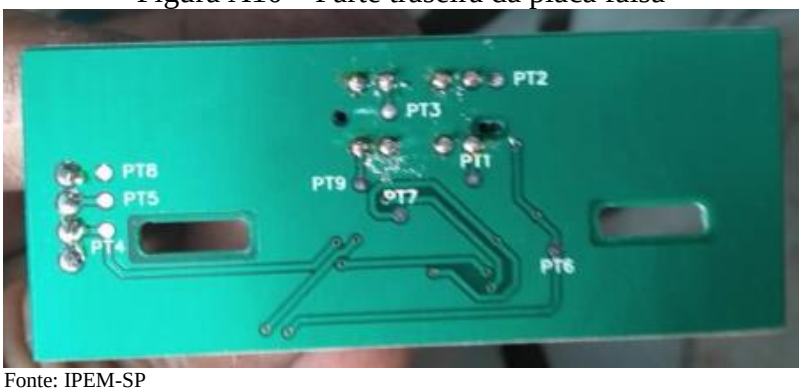
A-2.4.1 Nessa fraude, os componentes da placa são trocados por microcontroladores. A ativação se dá por sequência de liga e desliga. As figuras A9, A10, A11 e A12 são imagens de placas relacionadas a esse tipo de fraude.

Figura A9 - *Pulse*r usado na Bomba Gilbarco Veeder-Root Modelos KH12 (Nc1 NC2) com componentes trocados.



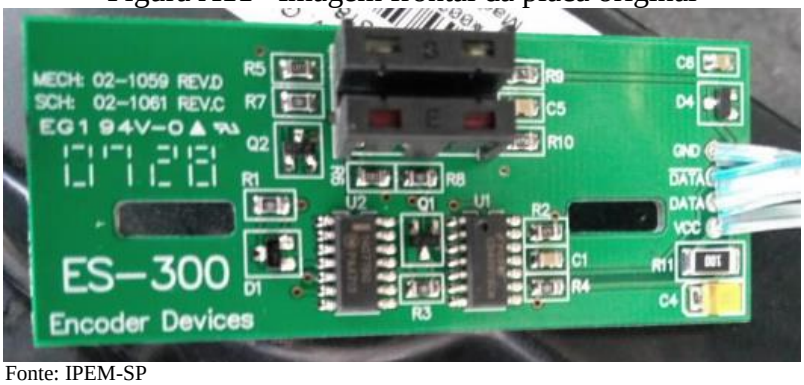
Fonte: IPEM-SP

Figura A10 – Parte traseira da placa falsa



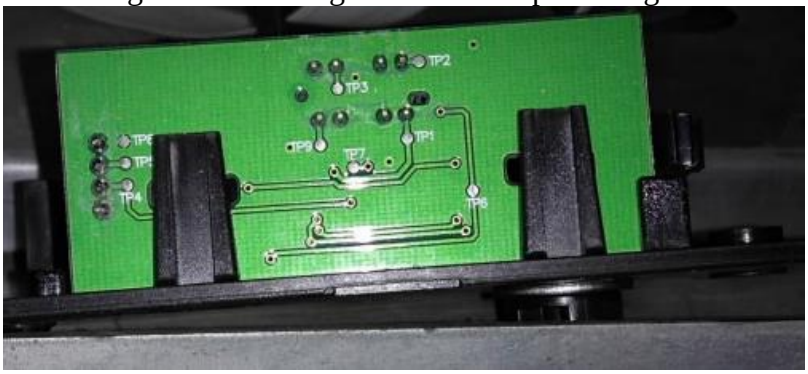
Fonte: IPEM-SP

Figura A11– Imagem frontal da placa original



Fonte: IPEM-SP

Figura A12 – Imagem traseira da placa original



Fonte: IPEM-SP

A-2.5 Pulser Falso Stratema modelo PHD 4821 e PHD 4822

A-2.5.1 Nessa fraude, um microcontrolador foi inserido na resina, como mostra a figura A13.

Figura A13 – Microcontrolador e componentes inseridos na resina.

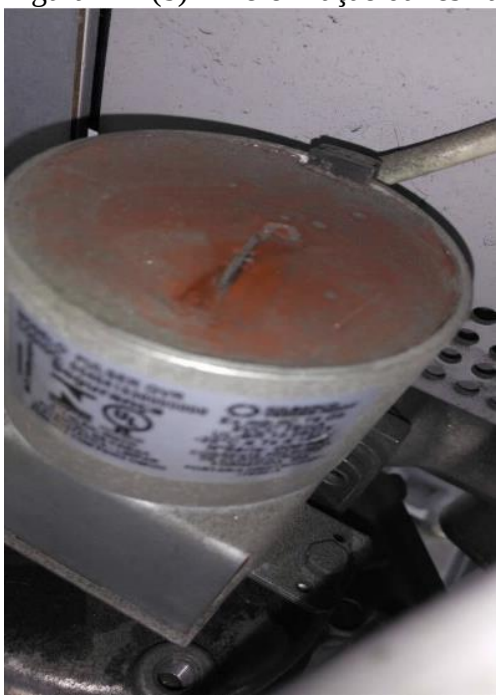
Fonte: IPEM-SP

Nota - Só foi possível visualizar a fraude (o microcontrolador, fios, etc.) após detectar que havia deformação na resina (figuras A14). Após consulta, descobriu-se que o plano de selagem foi dado como extraviado em outro estado e que não poderia ter sido utilizado. Neste caso, é preciso muita cautela para fazer o procedimento de testes.

Figura A14(a) – Deformação da resina

Fonte: IPEM-SP

Figura A14(b) – Deformação da resina



Fonte: IPEM-SP

A-3 FRAUDES EM PLACAS DE INTERFACE HIDRÁULICA (IH)

A-3.1 Fraude em Placa de IH original com Microcontroladores Adicionados (modelos 1, 2 e 3)

A-3.1.1 A tabela 4 a seguir apresenta as características dessa fraude.

Tabela 4 – Características da fraude apresentada nas figuras A15, A16, A17 e A18

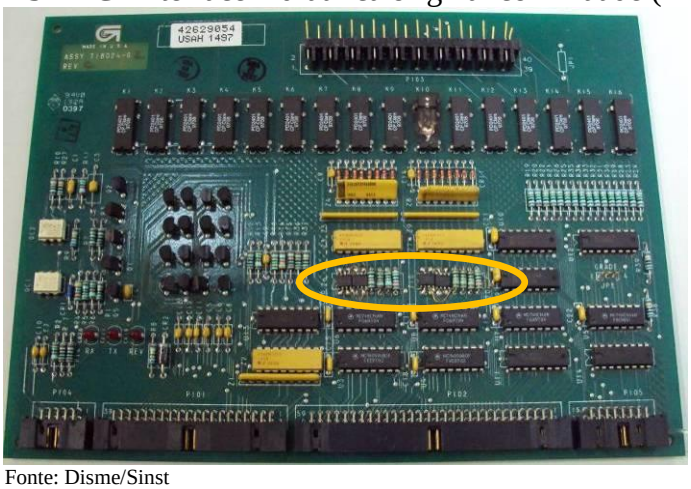
Componentes da fraude	Placa interface hidráulica original Microcontroladores adicionais (normalmente escondidos)
Operação	O microcontrolador presente na placa de IH incrementa a quantidade de pulsos gerados em um abastecimento.
Forma de acionamento/inibição	Uma sequência de comandos liga/desliga, normalmente enviados por controle remoto. O microcontrolador é programado para identificar uma sequência específica de interrupções da energia da bomba (sequência liga/desliga). Quando a sequência correta é detectada, a fraude é ativada. A inibição da fraude é feita pela interrupção do fornecimento de energia da bomba. Quando a bomba for novamente energizada a fraude estará desativada. Por este motivo recomenda-se realizar os ensaios metrológicos imediatamente ao chegar ao posto e não permitir o desligamento das bombas. O sistema de ativação da fraude inclui ainda um receptor comercial de RF e um contator conectado ao circuito de alimentação da bomba, os quais implementam a sequência liga/desliga de acionamento da fraude.
Efeito	O resultado [da medição] apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Os valores típicos de erro percentual encontrados para este tipo de fraude variam entre -3% e -12%.

Fonte: Disme/Sinst

A-3.1.2 Modelo 1 – Fraude em PCI de interface hidráulica com inserção de microcontroladores no lugar de componentes passivos

A-3.1.2.1 A figura A15 apresenta uma PCI de interface hidráulica original. A fraude se dá pela inserção de microcontroladores no lugar de componentes passivos. No exemplo a seguir, o fraudador não se preocupou em esconder a alteração, mas, na maioria dos casos, o componente original é usado na tentativa de esconder a alteração e dificultar sua identificação.

Figura A15 – PCI Interface hidráulica original com fraude (modelo 1)



Fonte: Disme/Sinst

A-3.1.2.2 Na figura A16, destacamos o local da fraude, bem como os componentes utilizados:

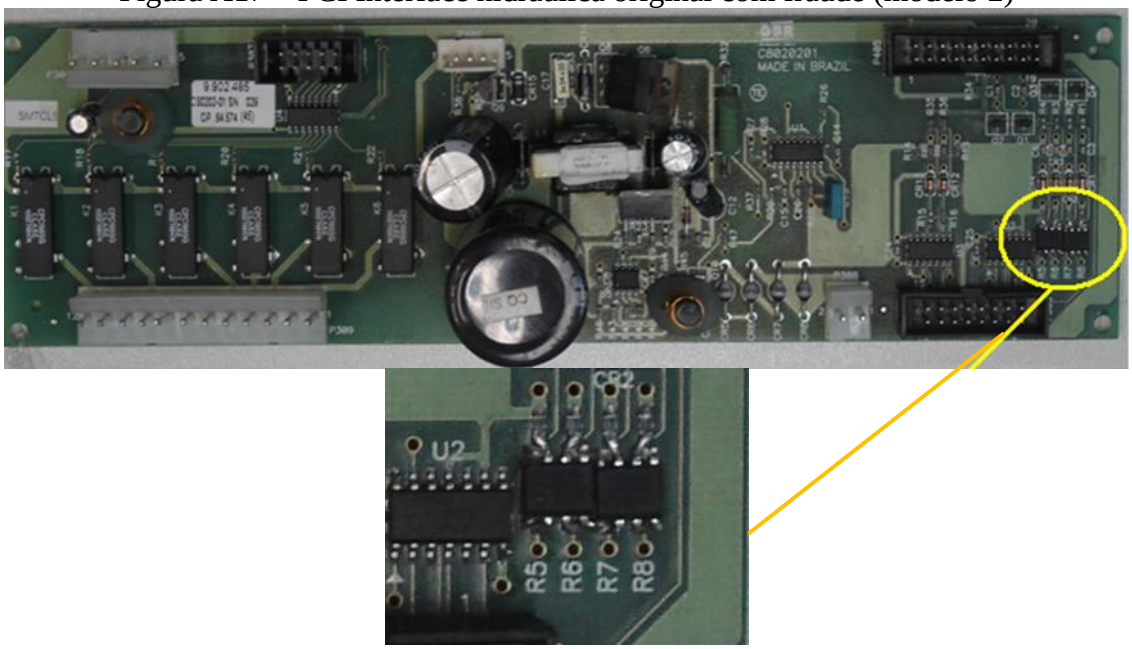
Figura A16 – Detalhes de ligações com fios "*Wire up*"

Fonte: Disme/Sinst

A-3.1.3 Modelo 2 – Fraude na interface hidráulica com inclusão de microcontroladores SMD

A-3.1.3.1 A figura A17 apresenta um outro modelo de interface hidráulica original (modelo 2) com inclusão de microcontroladores SMD, para implementação da fraude, no lugar em que havia resistores.

Figura A17 – PCI Interface hidráulica original com fraude (modelo 2)

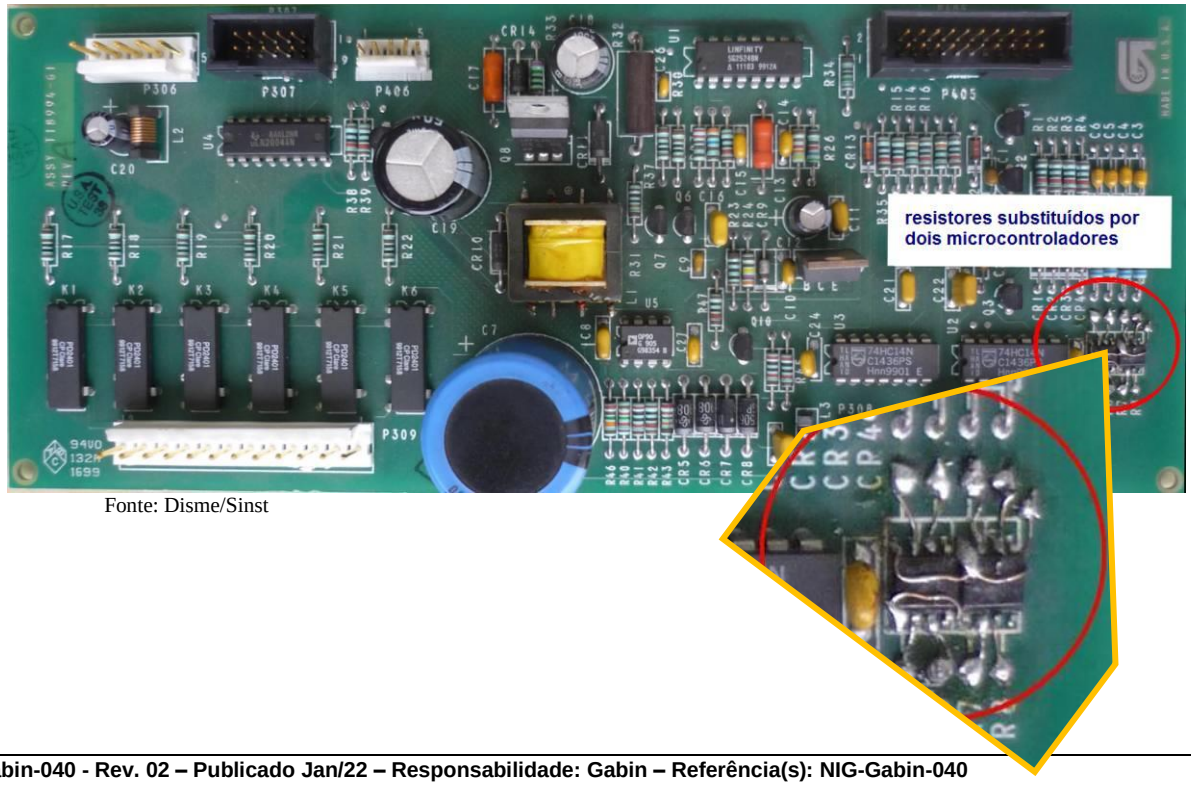


Fonte: Disme/Sinst

A-3.1.4 Modelo 3 – Fraude na interface hidráulica com a inclusão de microcontroladores

A-3.1.4.1 A figura A18 apresenta uma interface hidráulica original que foi modificada com a inclusão de microcontroladores (modelo 3).

Figura A18 – PCI Interface hidráulica original com fraude (modelo 3)

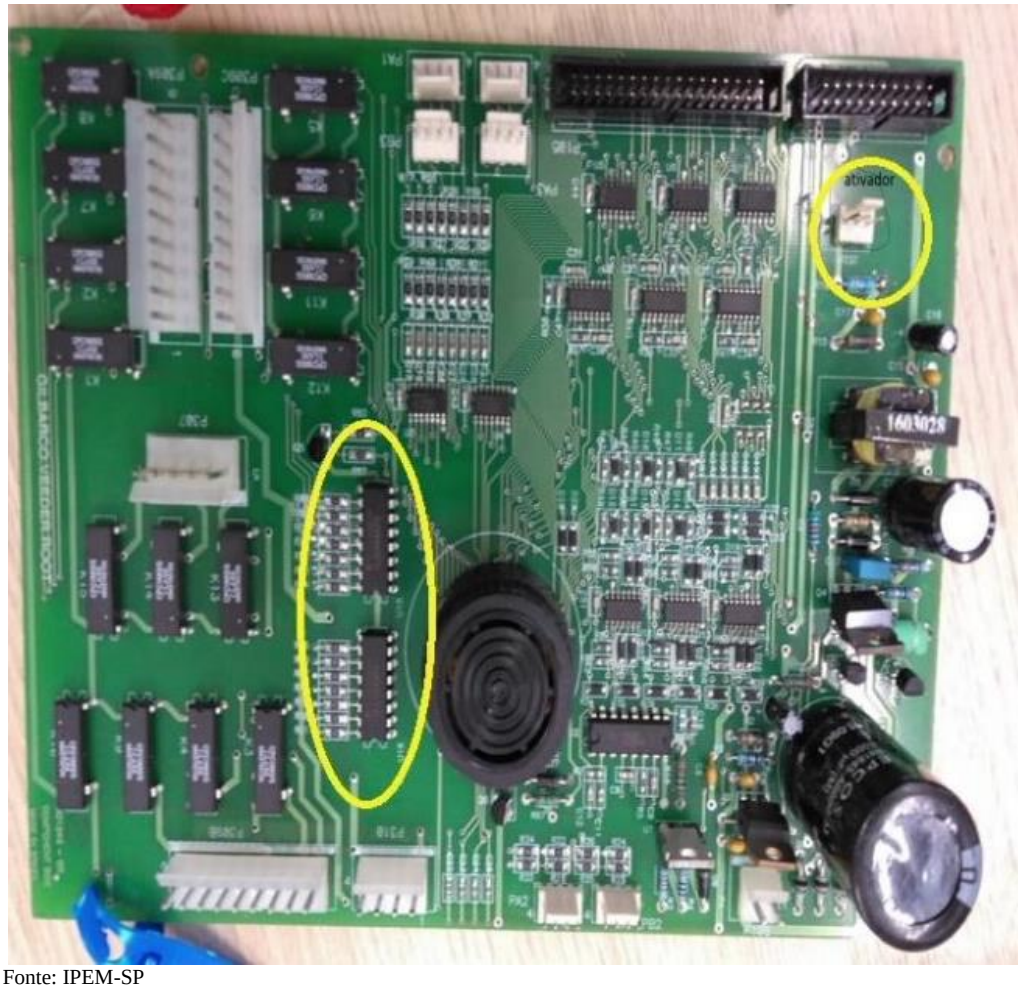


Fonte: Disme/Sinst

A-3.1.5 Fraude na interface hidráulica falsa com a inclusão de microcontroladores [modelo 1]

A-3.1.5.1 A figura A19 apresenta uma interface hidráulica falsa com a inclusão de microcontroladores (modelo 1).

Figura A19 – Interface hidráulica falsa com microcontroladores [modelo 1].



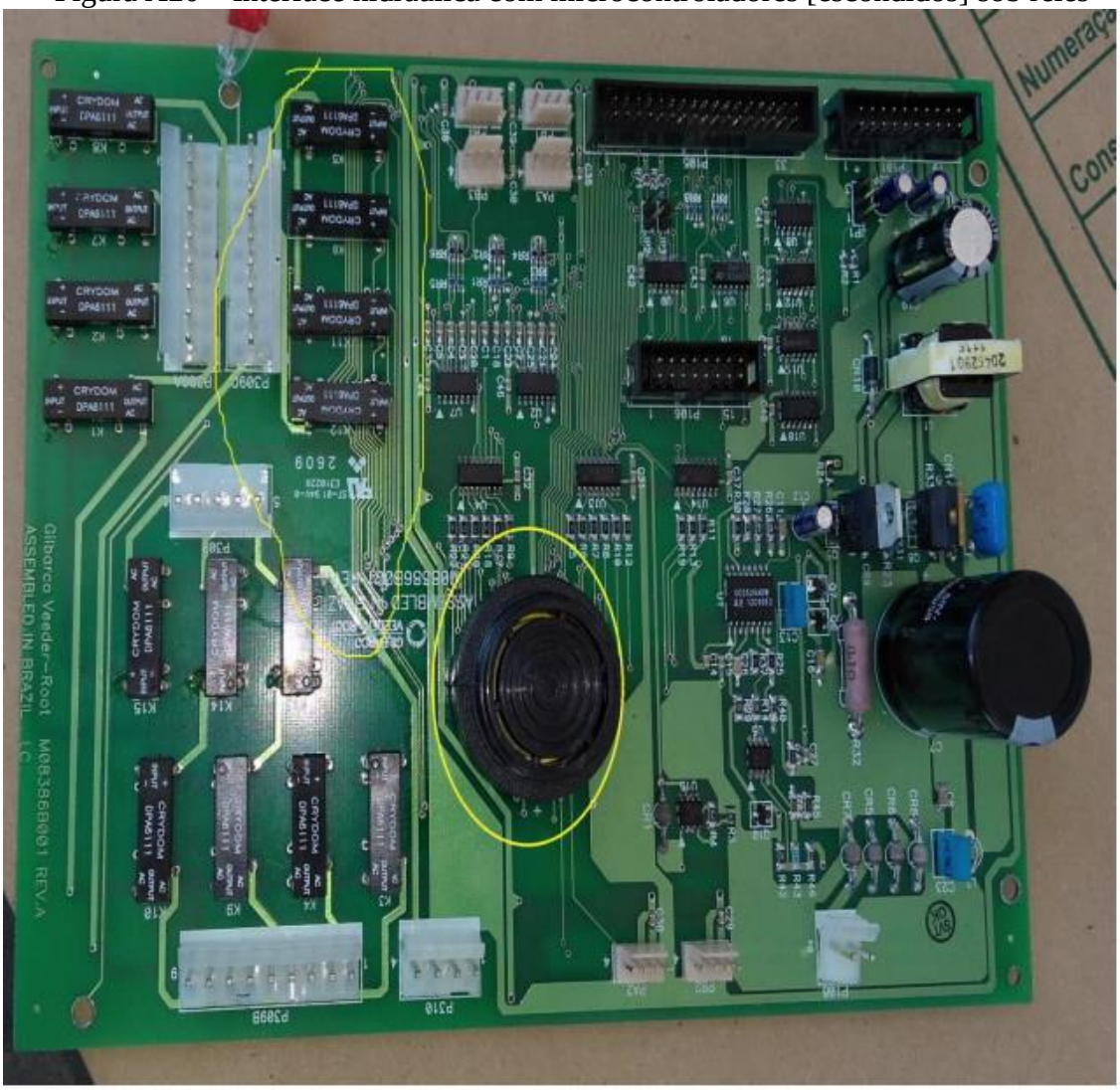
Fonte: IPEM-SP

A-3.1.5.2 - Os componentes em destaque são utilizados para fraudes, e o conector do lado direito superior é o ativador. Geralmente os componentes utilizados (microcontroladores) são PIC's.

A-3.1.6 Interface hidráulica falsa com microcontrolador embutido [modelo 2]

A-3.1.6.1 A figura A20 apresenta uma interface hidráulica falsa com a inclusão de microcontroladores (modelo 2).

Figura A20 – Interface hidráulica com microcontroladores [escondidos] sob relês



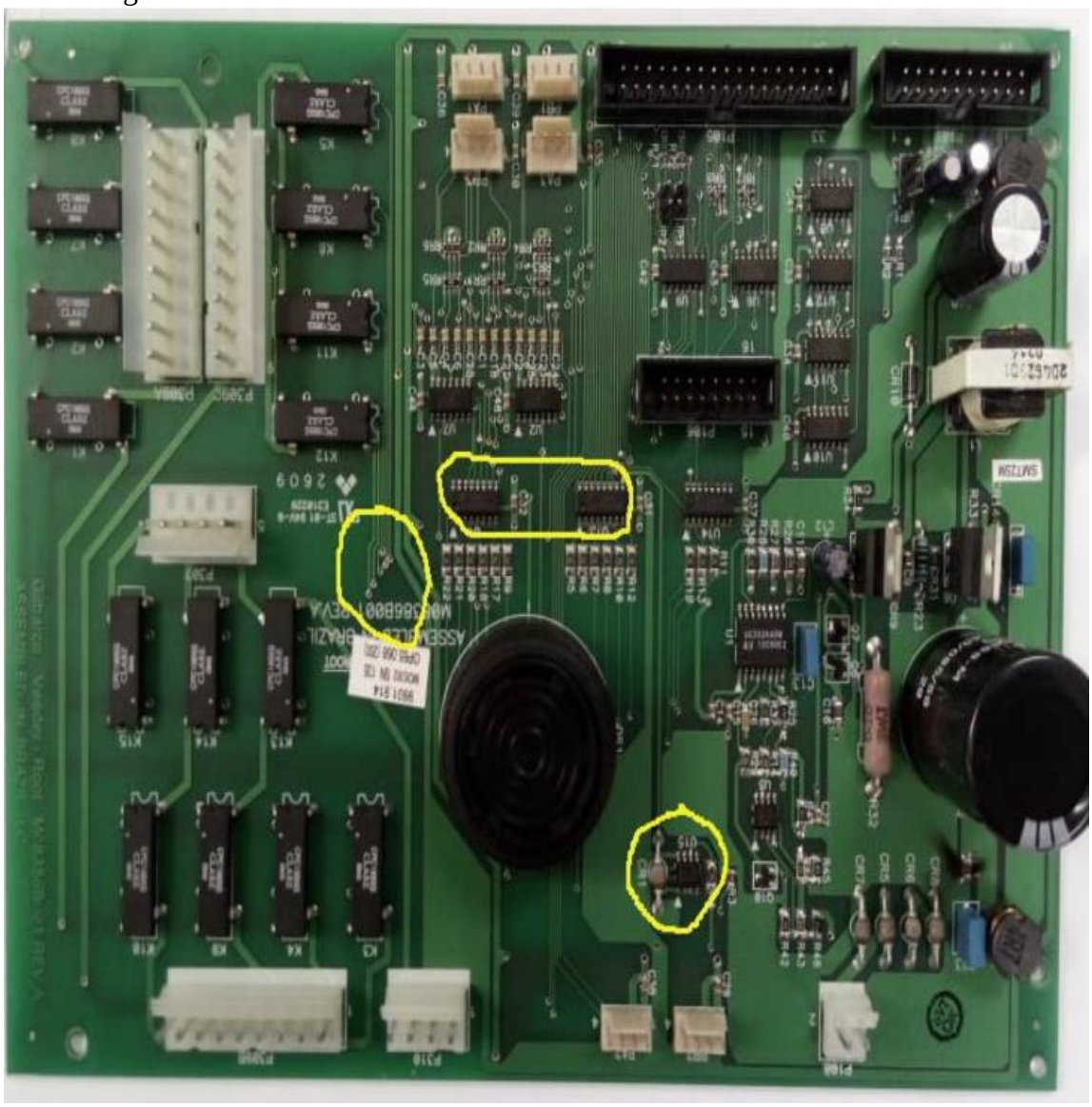
Fonte: IPEM-SP

A–3.1.6.2 Os relês de estado sólido em destaque, estão paralelos a um conjunto de trilhas que levam um sinal de 5 V para os microcontroladores que se encontram escondidos sob o mesmo. Nas placas originais, essas trilhas sob o relê com marcação K12 não existem. Ainda não se tem parâmetros para a ativação dessa fraude.

A-3.1.7 Interface hidráulica falsa com microcontrolador embutido [modelo 3]

A-3.1.7.1 A figura A21 apresenta uma interface hidráulica falsa com a inclusão de microcontroladores.

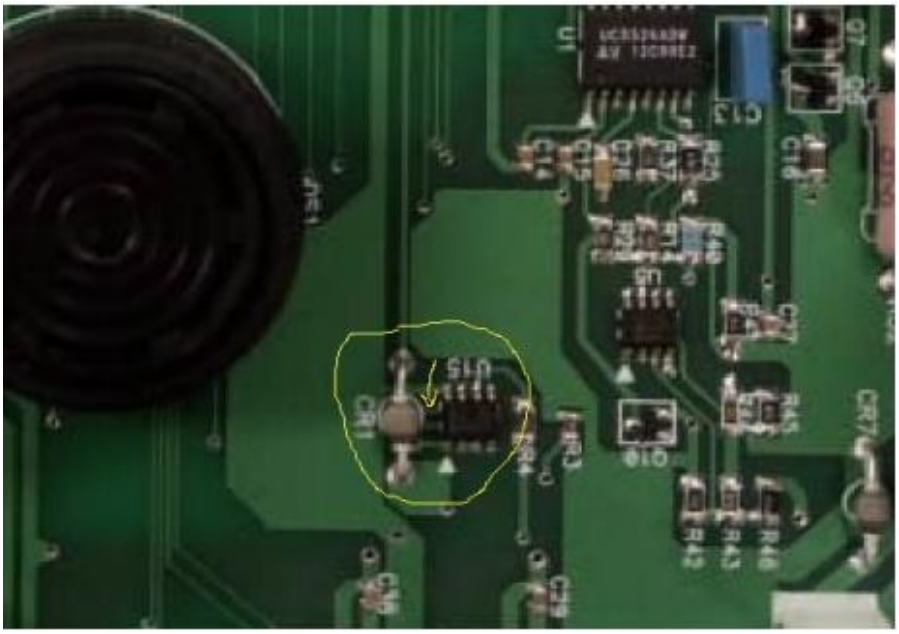
Figura A21 – Interface hidráulica falsa com inclusão de microcontrolador



Fonte: IPEM-SP

Nota - Neste modelo de fraude ainda não se tem parâmetros para a ativação, e a característica é semelhante à anterior. Difere apenas que as trilhas sob o relê K12 não existem mais e os componentes em destaque U2 e U7 são substituídos por microcontroladores da famila PIC ou Atmel. As trilhas próximas ao K12 estão em 7, diferente da placa original que tem apenas 5. E, ainda, o componente U15 encontra-se com ligação ao CR1, que nas placas originais também não existe. Destaque na figura A22 a seguir.

Figura A22 – Ligação de U15 ao CR1.



Fonte: IPEM-SP

A-3.1.8 Interface hidráulica com microcontrolador (raspado e regravado)

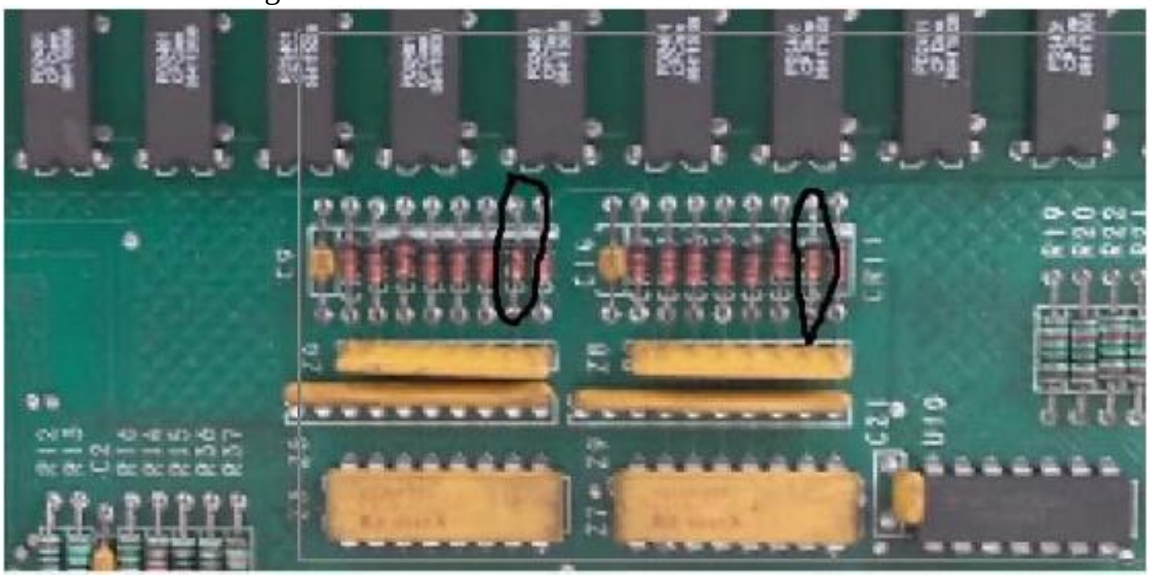
A-3.1.8.1 Nessa fraude, os componentes Z6 e Z10 (vide figura A23) foram substituídos por microcontrolador da família PIC (raspado e regravado).

Figura A23 - Placa Hidráulica utilizada em bombas Pro-2, HH 2/4, E 2/4, E2/6, Titan, Encore KH12 e ADV 2/1, 2/4, 2/6

Fonte: IPEM-SP

A-3.1.8.2 Para ter certeza que é uma fraude, verificar um fio soldado discretamente sob o CR11 conforme destaque na figura A24 a seguir. Às vezes é necessária a utilização de lupa, pois o fio é capilar o que dificulta a visualização.

Figura A24 – Fio soldado discretamente sob o CR11



Fonte: IPEM-SP

A-3.1.9 Interface hidráulica com microcontrolador (lixado e carimbado)

A-3.1.9.1 Nessa fraude, o componente original da placa (vide figura A25) foi substituído por um microcontrolador que foi lixado e carimbado.

Figura A25 - A placa de interface hidráulica da figura abaixo é utilizada nas bombas GBR pro 2, pro 2/4 e HH 2/4.

Fonte: IPEM-SP

A-3.1.9.2 Com a ajuda de uma lupa, visualize o componente P305, que se encontra deformado e com a grafia por cima (vide figura A26). O acionamento se dá por sequência de liga/desliga.

Figura A26 – Componente P305

Fonte: IPEM-SP

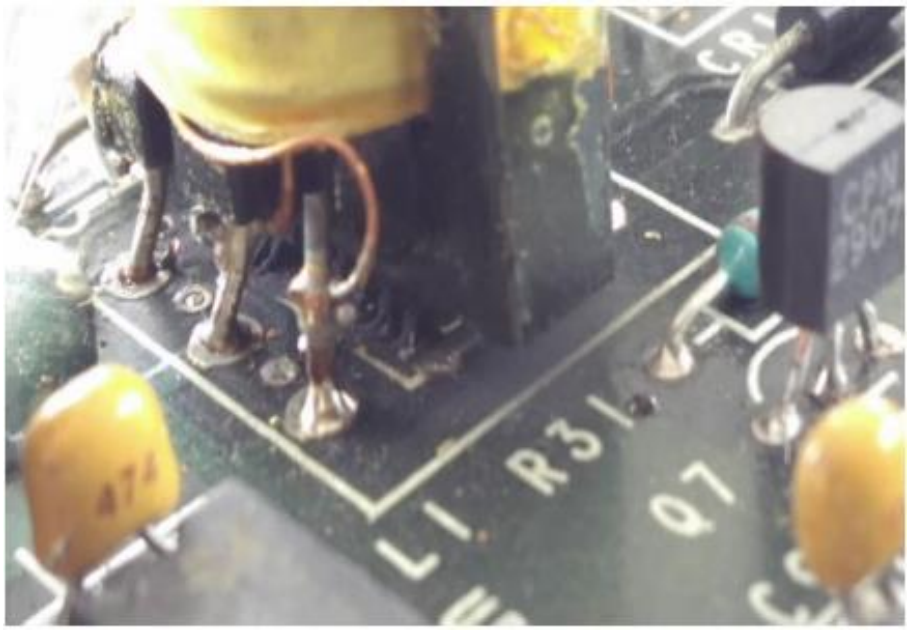
A-3.1.10 Interface hidráulica com microcontrolador escondido

A-3.1.10.1 Nessa fraude, numa placa falsa (figura A27), um microcontrolador encontra-se escondido. Na figura A28, o microcontrolador está sob um transformador.

Figura A27 - Placa de interface hidráulica falsa utilizada nas bombas GBR pro 2, pro 2/4 e HH 2/4.

Fonte:IPEM-SP

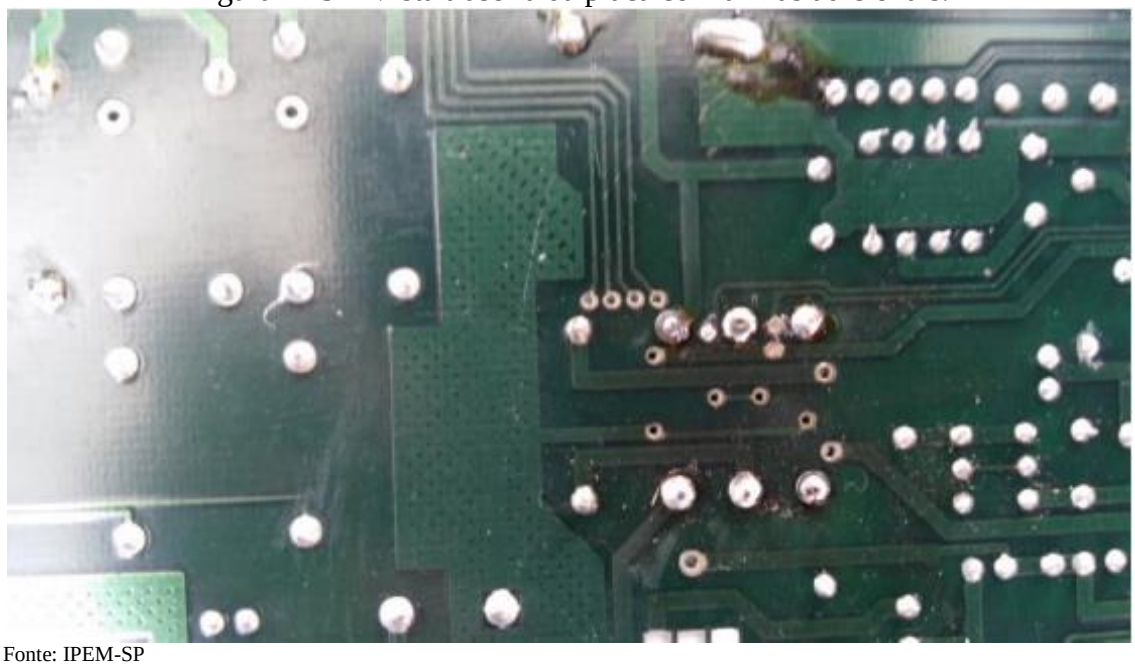
Figura A28 – Microcontrolador sob transformador.



Fonte: IPEM-SP

A-3.1.10.2 Observar a parte de trás da placa, onde pode-se notar 4 trilhas adicionais para acionamento da fraude (vide figura A29).

Figura A29 – Vista traseira da placa com trilhas adicionais.



Fonte: IPEM-SP

A-3.2 Fraude em Placa Falsa de IH Acionada por Tensão de 12V (modelos 1 e 2)

A-3.2.1 A tabela 5 e as figuras A30 e A31 a seguir apresentam as características dessa fraude.

Tabela 5 – Características da fraude apresentada nas figuras A30 e A31

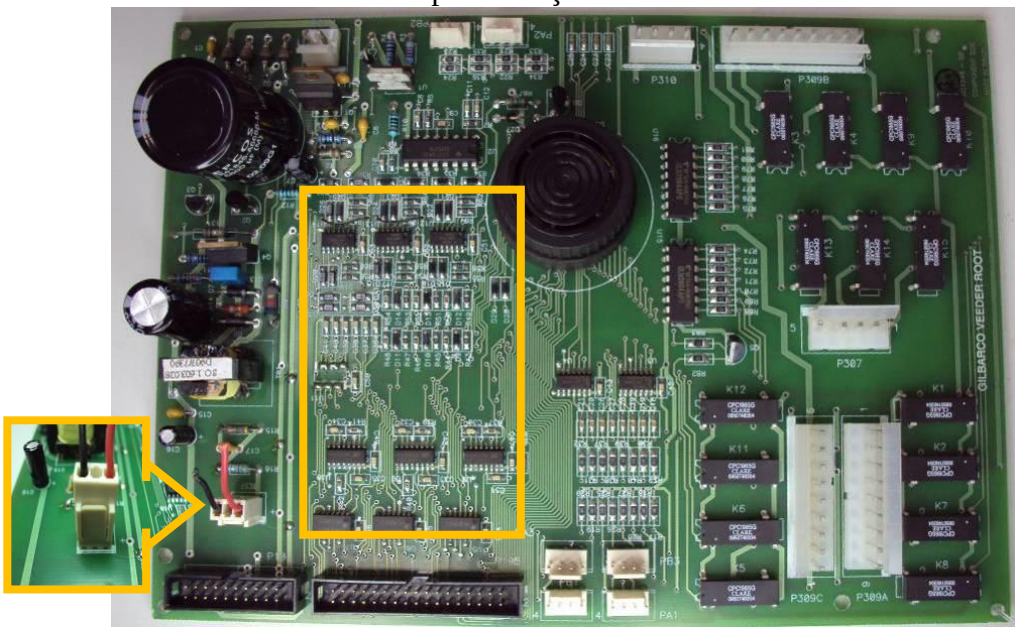
Componentes da fraude	Placa de IH falsa
Operação	Os componentes em destaque nas Figuras A30 e A31 formam o circuito responsável pelo incremento da quantidade de pulsos gerados em um abastecimento.
Forma de acionamento/inibição	Aplicação de uma tensão de 12V a um conector da placa. Quando a tensão é retirada, a fraude é inibida. Até o momento não é conhecida a forma de acionamento externo. Este acionamento/inibição poderia se dar através de controle remoto, de forma semelhante aos casos anteriores, ou através de um interruptor instalado no instrumento.
Efeito	O resultado [da medição] apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Os valores típicos de erro percentual encontrados para este tipo de fraude variam entre -3% e -12%.

Fonte: Disme/Sinst

A-3.2.2 Modelo 1 – Fraude em PCI falsa com a inclusão de diversos componentes eletrônicos e de um conector

A-3.2.2.1 Esta PCI (modelo 1) é uma placa falsa, diferenciando-se da placa original pela inclusão de diversos componentes eletrônicos responsáveis pela fraude e de um conector, ao qual é aplicada a tensão que controla o acionamento da fraude.

Figura A30 – Placa IH falsa com fraude (modelo 1). Destaque: conector e componentes utilizados para implementação da fraude.

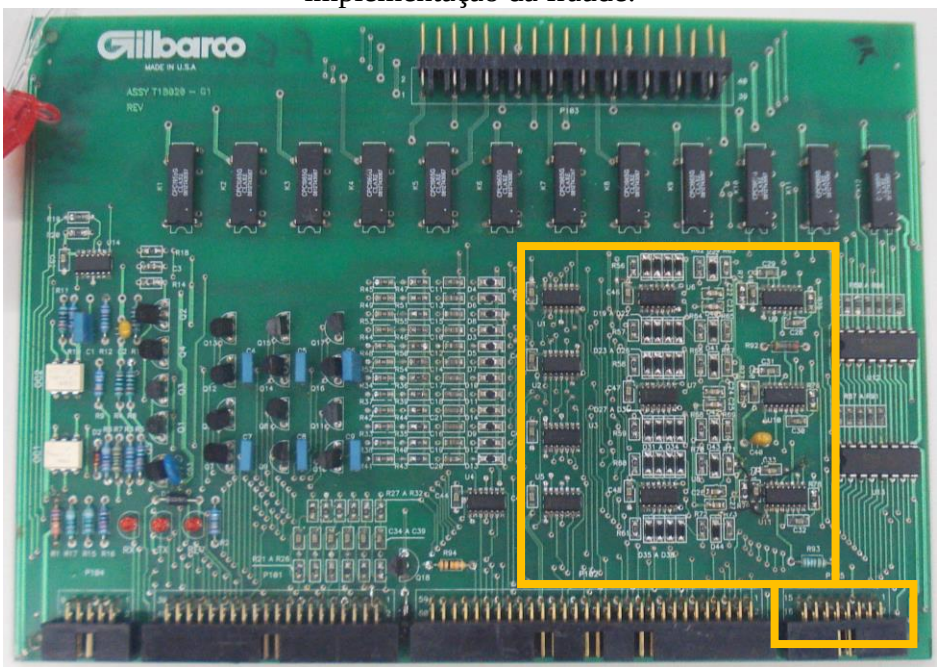


Fonte: Disme/Sinst

A-3.2.3 Modelo 2 - Fraude em interface hidráulica com a inclusão de diversos componentes eletrônicos e de um conector

A-3.2.3.1 Na Figura A31 é apresentado outro modelo de interface hidráulica (modelo 2) que possui o mesmo tipo de fraude.

Figura A31 – Placa IH falsa com fraude (modelo 2). Destaque: conector e componentes utilizados para implementação da fraude.



Fonte: Disme/Sinst

A-3.3 Fraude em Placa Falsa de Interface Hidráulica Acionada por Comandos Remotos

A-3.3.1 A tabela 6 e as figuras A32 e A33 a seguir apresentam as características dessa fraude.

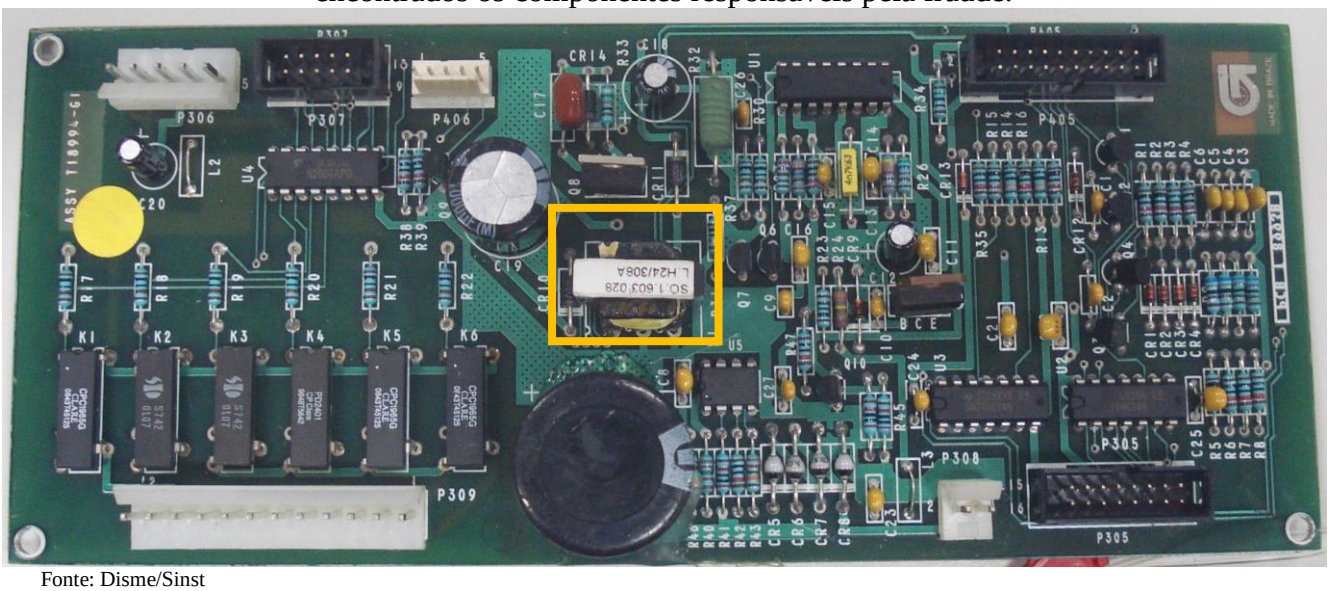
Tabela 6 – Características da fraude apresentada nas figuras A32 e A33

Componentes da fraude	Placa IH falsa. Componentes eletrônicos escondidos (transceptor RS-485 e microcontroladores). Programa falso de computador.
Operação	Os componentes eletrônicos em destaque na figura A32 recebem comandos de acionamento/inibição da fraude (transceptores) e incrementam a quantidade de pulsos gerados em um abastecimento (microcontroladores).
Forma de acionamento/inibição	Através de comandos remotos enviados por um computador. O computador possui um software falso, com aparência de um programa de teste de desempenho, o qual é responsável pelo envio dos comandos. Normalmente é utilizado meio físico para transmissão dos comandos (cabos de comunicação/automação). Os comandos chegam inicialmente ao transceptor RS-485 o qual os direciona para os microcontroladores responsáveis pela adulteração do resultado da medição.
Efeito	O resultado apresentado no *display* da bomba é maior do que o volume abastecido. O erro percentual da medida pode ser ajustado para cada abastecimento. Seu valor pode variar entre 0% e -50%.

Fonte: Disme/Sinst

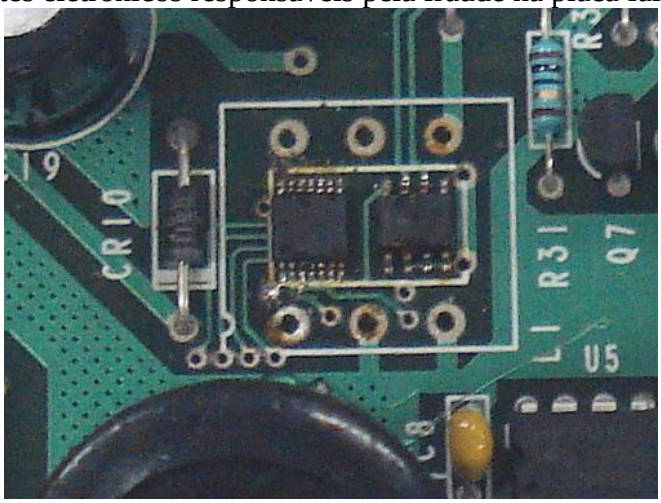
A-3.3.2 A PCI apresentada a seguir (figura A32) é uma placa de interface hidráulica falsa. Os componentes responsáveis pela fraude encontram-se escondidos embaixo do transformador situado na região central da placa (em destaque na figura A33).

Figura A32 – Placa de interface hidráulica falsa com fraude. Destaque: transformador sob o qual são encontrados os componentes responsáveis pela fraude.



Fonte: Disme/Sinst

Figura A33 – Componentes eletrônicos responsáveis pela fraude na placa falsa de interface hidráulica



Fonte: Disme/Sinst

A-4 FRAUDES EM PLACAS DE CPU

A-4.1 Fraude em Placa de CPU Original com Microcontroladores Adicionados (modelos 1 e 2)

A-4.1.1 A tabela 7 e as figuras A34, A35, A36 e A37 a seguir apresentam as características dessa fraude.

Tabela 7 – Características da fraude apresentada nas figuras A34, A35, A36 e A37

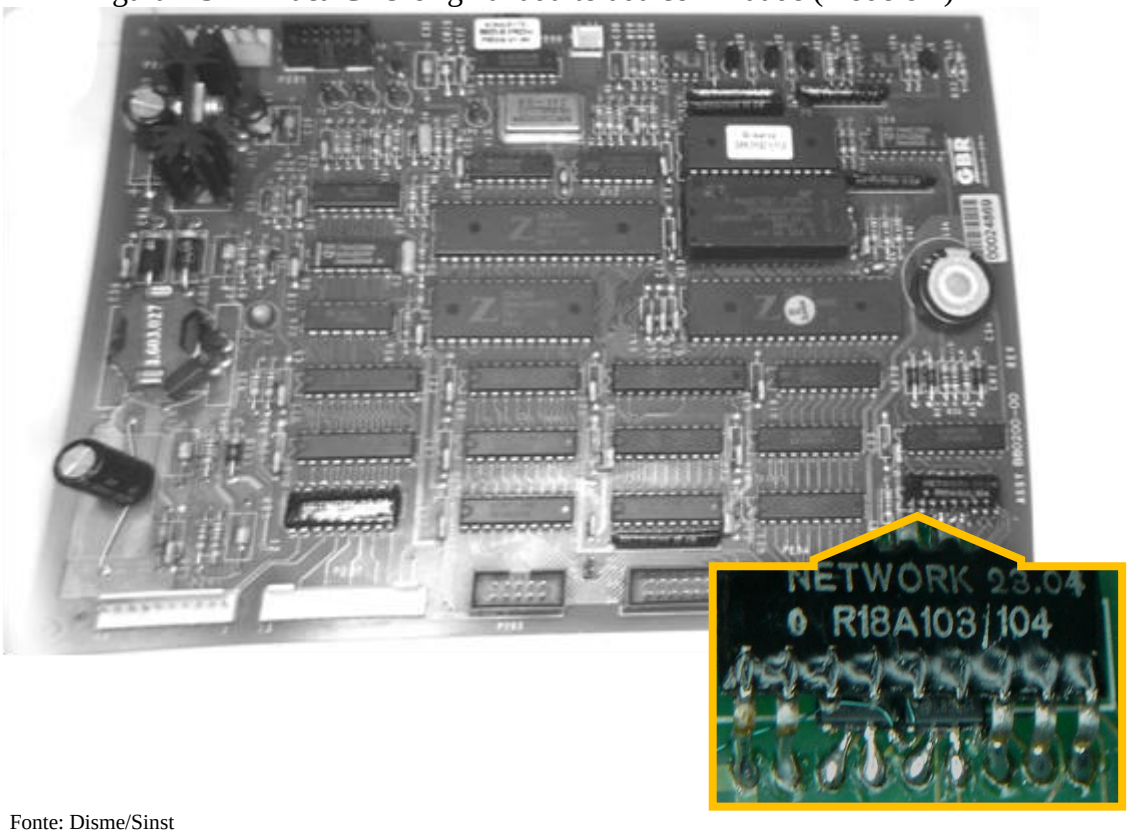
Componentes da fraude	Placa CPU original Microcontroladores adicionais (normalmente escondidos)
Operação	O(s) microcontrolador(es) são os responsáveis pelo incremento da quantidade de pulsos errados em um abastecimento.
Forma de acionamento/inibição	Uma sequência de comandos liga/desliga, normalmente enviados por controle remoto. O microcontrolador é programado para identificar uma sequência específica de interrupções da energia da bomba (sequência liga/desliga). Quando a sequência correta é detectada, a fraude é ativada. A inibição da fraude é feita pela interrupção do fornecimento de energia da bomba. Quando a bomba for novamente energizada a fraude estará desativada. Por este motivo recomenda-se realizar os ensaios metrológicos imediatamente ao chegar ao posto e não permitir o desligamento das bombas. O sistema de ativação da fraude inclui ainda um receptor comercial de RF e um contator conectado ao circuito de alimentação da bomba, os quais implementam a sequência liga/desliga de acionamento da fraude.
Efeito	O resultado apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Os valores típicos de erro percentual encontrados para este tipo de fraude variam entre -3% e -12%.

Fonte: Disme/Sinst

A-4.1.2 Modelo 1 – Fraude em Placa CPU Modificada com a Inclusão de Microcontroladores

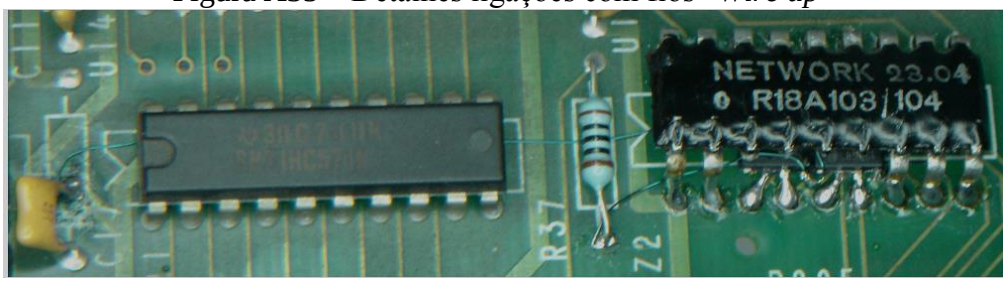
A-4.1.2.1 A figura A34 apresenta a inserção de microcontroladores escondidos abaixo de outro componente original da placa. É visível a interligação de pequenos fios *wire up* para conexão do microcontrolador responsável pela fraude conforme detalhe na figura A35.

Figura A34 – Placa CPU original adulterada com fraude (modelo 1)



Fonte: Disme/Sinst

Figura A35 – Detalhes ligações com fios "*Wire up*"

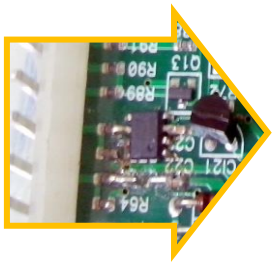


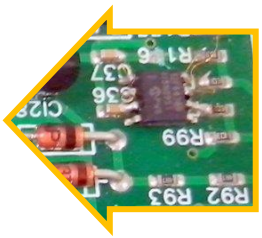
Fonte: Disme/Sinst

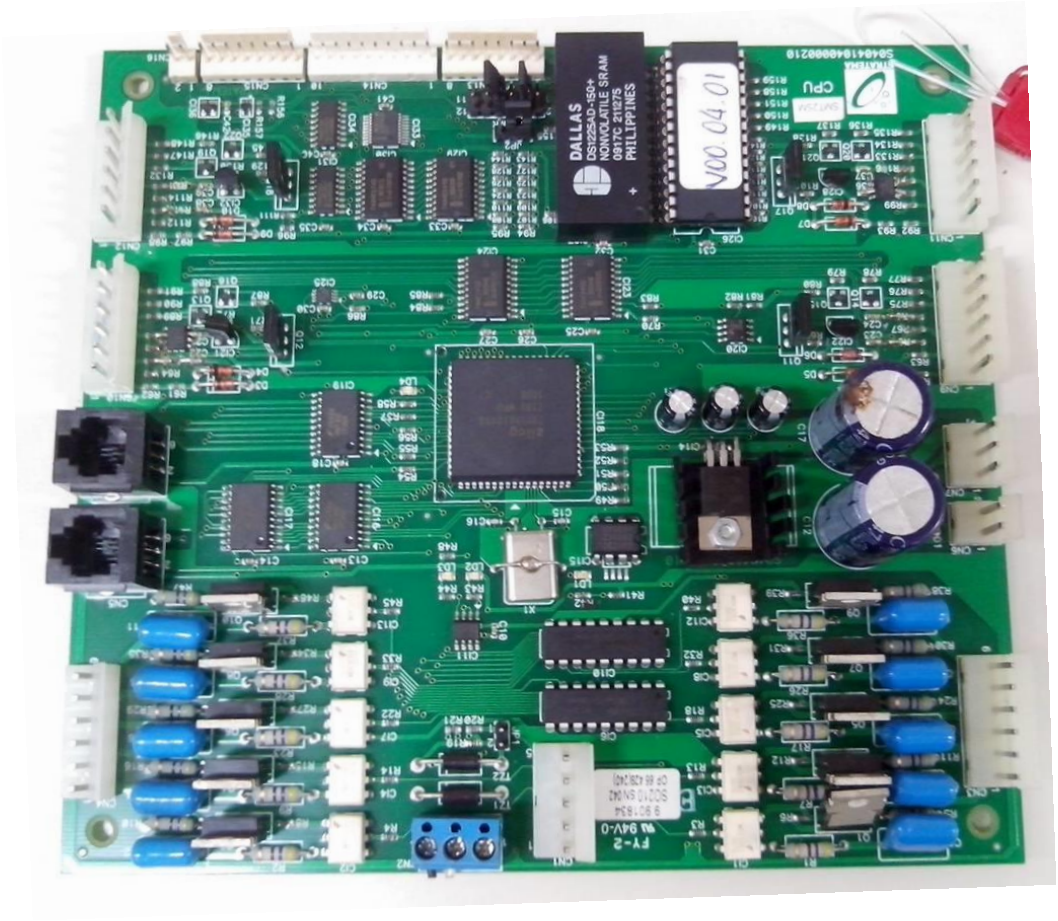
A-4.1.3 Modelo 2 – Fraude em Placa CPU Modificada com a Inclusão de Microcontroladores

A-4.1.3.1 A figura A36 apresenta outra placa CPU original que foi modificada com a inclusão de microcontroladores. Esta fraude apresenta as mesmas características descritas na tabela 7.

Figura A36 – Placa CPU original adulterada com fraude (modelo 2); detalhe dos componentes acrescentados.



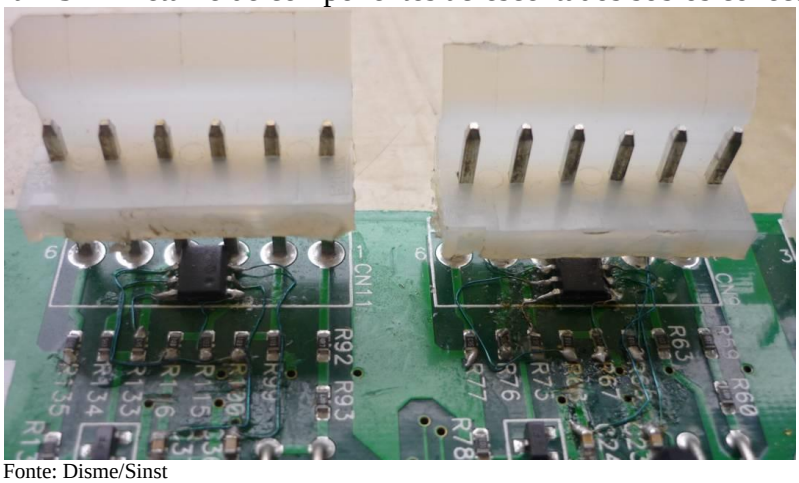




Fonte: Disme/Sinst

A-4.1.3.2 Uma variante desta fraude (figura A37) foi identificada com a inserção dos microcontroladores sob os conectores originais.

Figura A37 – Detalhe de componentes acrescentados sob os conectores



Fonte: Disme/Sinst

A-4.2 Fraude em Placa de CPU Acionada por Comandos Remotos (modelos 1, 2, 3, 4 e 5)

A tabela 8 e as figuras A38 a A52 a seguir apresentam as características dessa fraude.

Tabela 8 – Características da fraude apresentada nas figuras A38 a A52

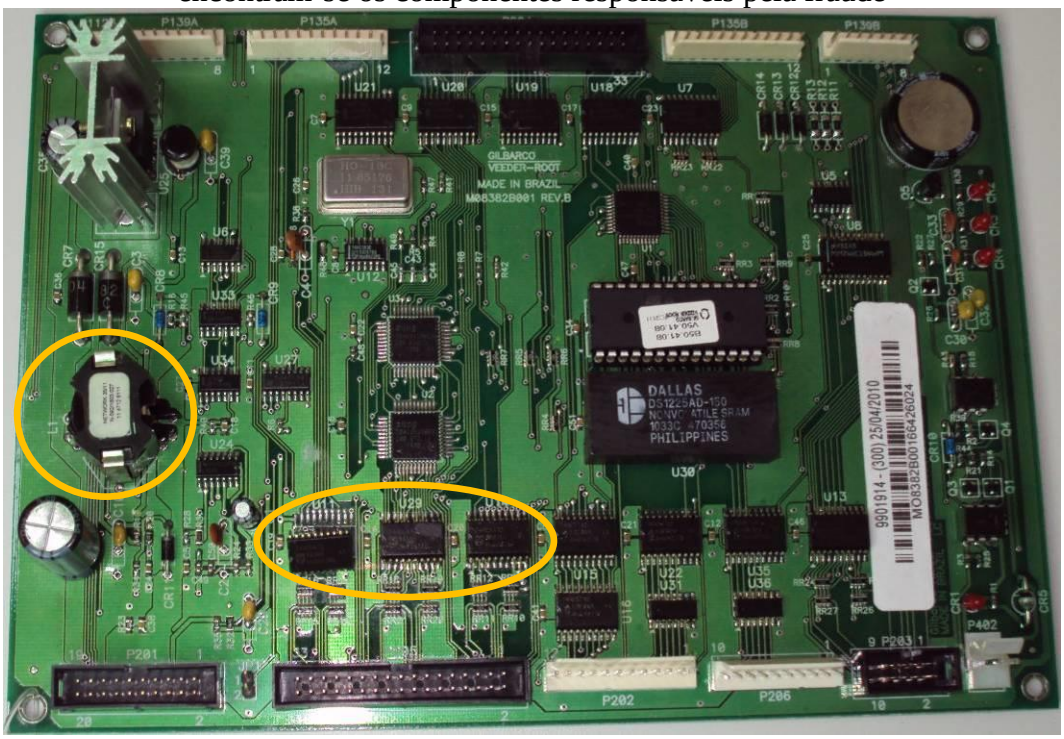
Componentes da fraude	Placas CPU originais ou falsas conforme descrito nas Figuras A38 a A52. Componentes eletrônicos escondidos (transceptor RS-485 e microcontroladores). Programa falso de computador.
Operação	Os componentes eletrônicos em destaque nas Figuras A38 a A52 recebem comandos de acionamento/inibição da fraude (transceptores) e incrementam a quantidade de pulsos gerados em um abastecimento (microcontroladores).
Forma de acionamento/inibição	Através de comandos remotos enviados por um computador. O computador possui um software falso, com aparência de um programa de teste de desempenho, o qual é responsável pelo envio dos comandos. Normalmente é utilizado meio físico para transmissão dos comandos (cabos de comunicação/automação). Os comandos chegam inicialmente ao transceptor RS-485 o qual direciona os comandos para os microcontroladores responsáveis pela adulteração do resultado da medição.
Efeito	O resultado [da medição] apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida pode ser ajustado para cada abastecimento. Seu valor pode variar entre 0% e -50%.

Fonte: Disme/Sinst

A-4.2.1 Modelo 1 – Placa de CPU falsa com montagem tipo SMD, similar a placa de CPU marca Veeder-Root para bombas modelo ADV.

A-4.2.1.1 A PCI apresentada a seguir (figura A38) é uma placa CPU falsa similar a placa Veeder–Root para bombas modelo ADV. Todos os componentes responsáveis pela fraude encontram-se escondidos embaixo de outros componentes utilizados na placa (em destaque nas figuras A39 e A40), o que faz com que estes se encontrem sutilmente levantados em relação aos componentes próximos. Esta é a forma mais prática de identificação visual deste tipo de fraude.

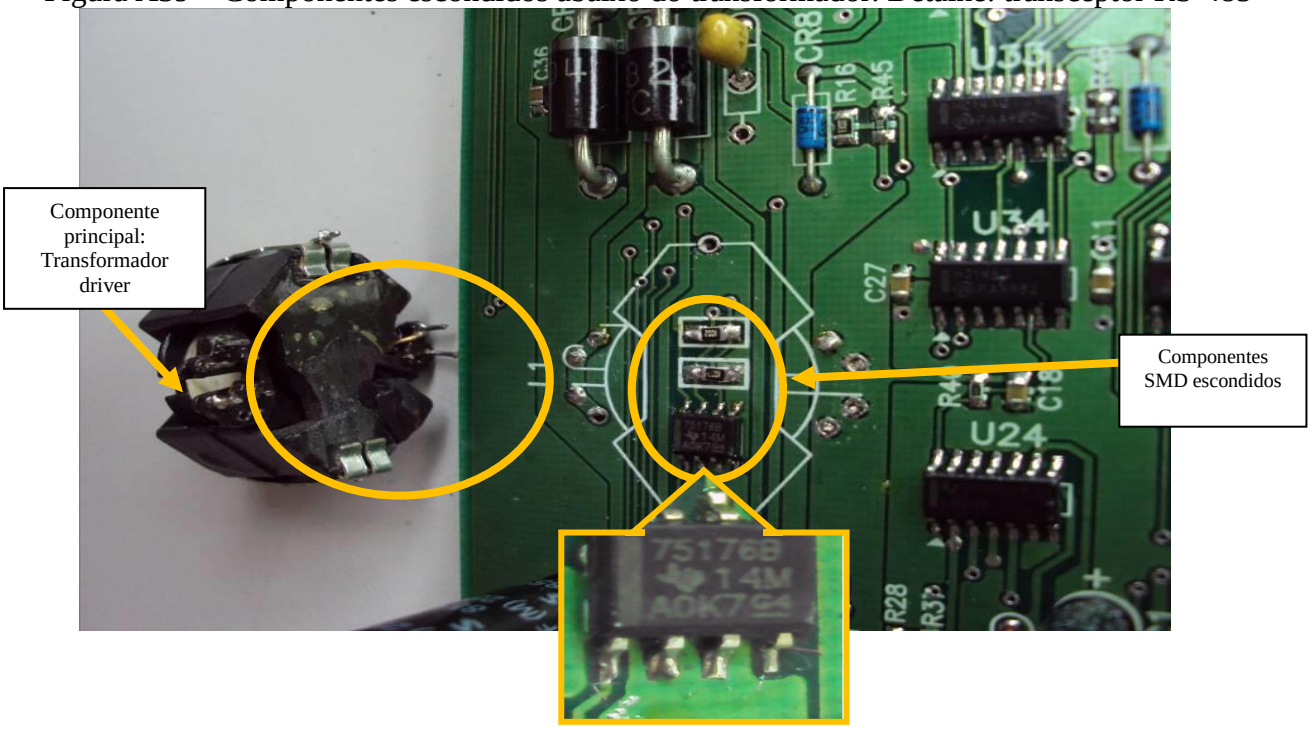
Figura A38 – PCI CPU falsa com fraude (modelo 1). Em destaque: componentes da placa sob os quais encontram-se os componentes responsáveis pela fraude



Fonte: Disme/Sinst

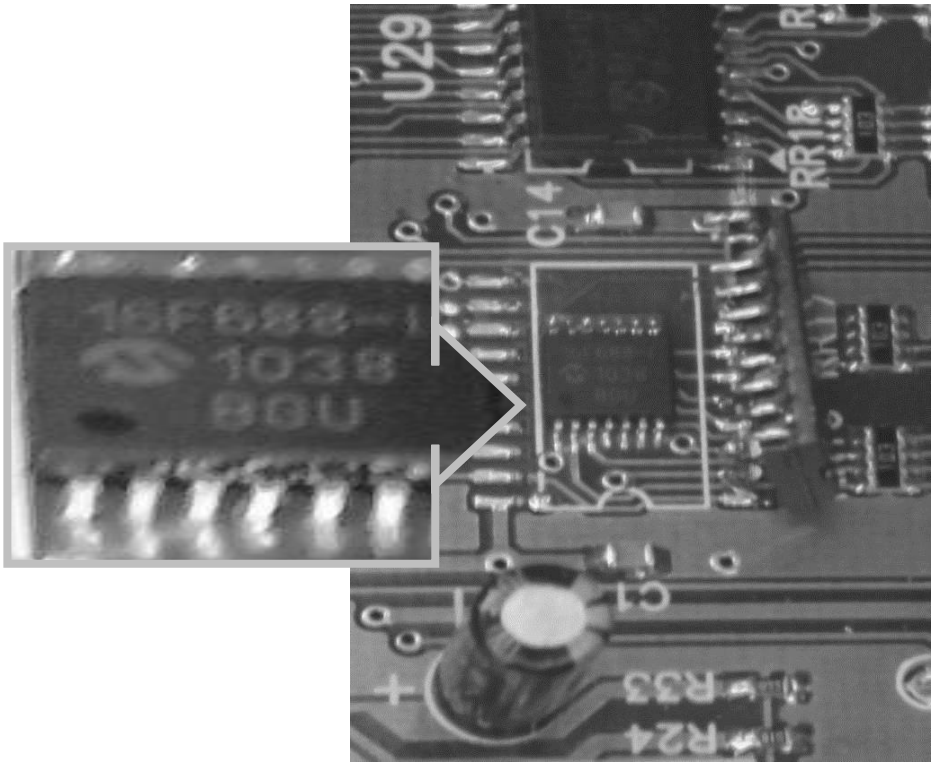
A-4.2.1.2 Na figura A39 são destacadas as posições na PCI onde estão localizados os componentes responsáveis pela fraude escondidos sob os componentes originais:

Figura A39 – Componentes escondidos abaixo do transformador. Detalhe: transceptor RS-485



A-4.2.1.3 Na mesma PCI, foram escondidos os microcontroladores conforme figura A40.

Figura A40 – Microcontrolador escondido sob outro componente SMD

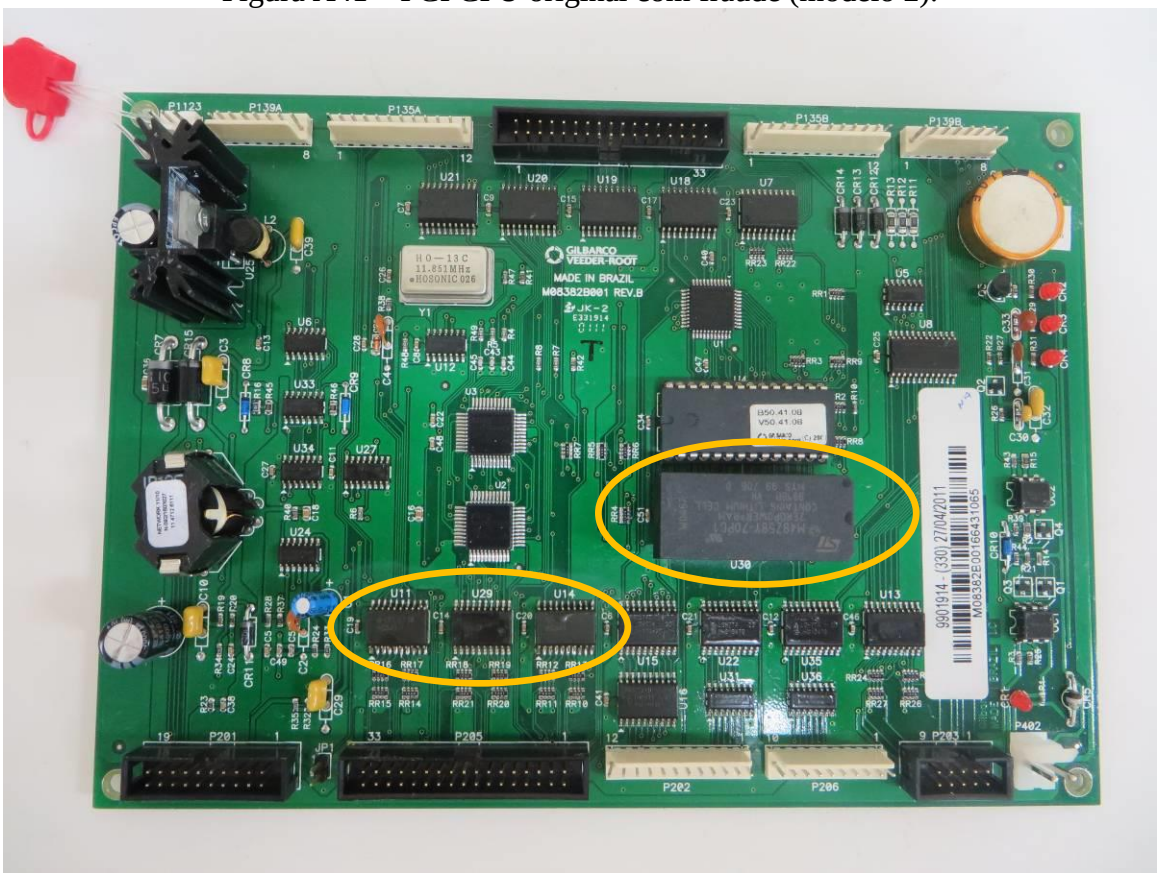


Fonte: Disme/Sinst

A-4.2.2 Modelo 2 – Placa de CPU original com montagem tipo SMD, marca Veeder-Root para bombas modelo ADV.

A-4.2.2.1 A PCI apresentada a seguir (Fig. A41) é uma CPU original que foi modificada para abrigar os componentes eletrônicos que implementam a fraude. O transceptor RS-485 é encontrado sob a memória SRAM (figura A42) e os microcontroladores ficam sob outros componentes originais da placa (em destaque na Fig. A43). Pequenos fios podem ser visualizados tanto sob a memória SRAM quanto no verso da placa, o que permite a identificação da fraude.

Figura A41 – PCI CPU original com fraude (modelo 2).



Fonte: Disme/Sinst

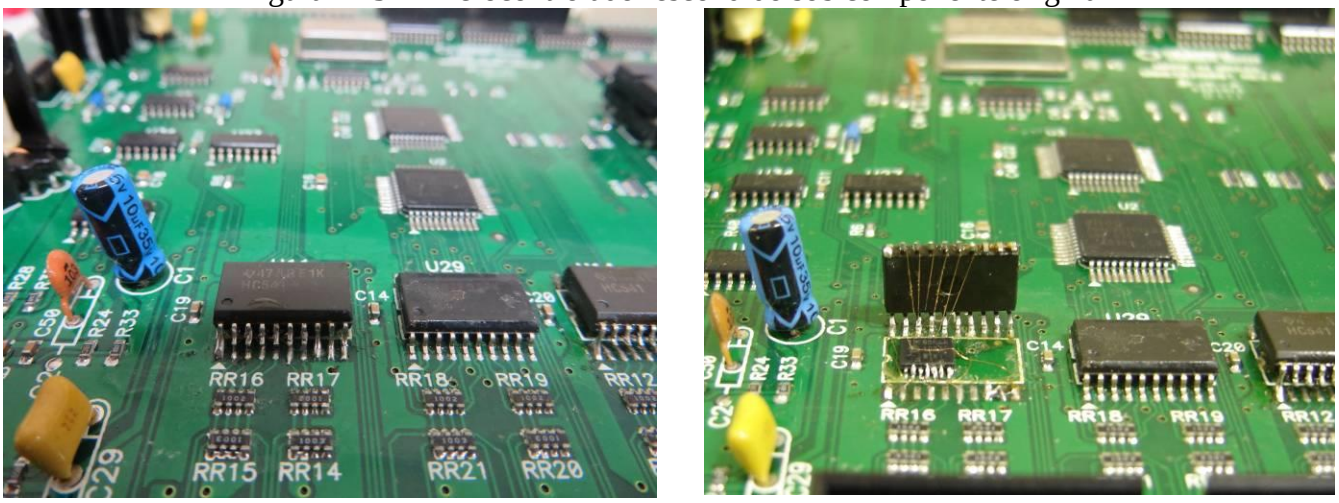
A-4.2.2.2 A seguir (figura A42) é mostrada a posição do transceptor RS-485, sob a memória SRAM.

Figura A42 – Componente escondido sob a memória SRAM. Detalhe: transceptor RS-485

Fonte: Disme/Sinst

A-4.2.2.3 Na mesma PCI, foram escondidos microcontroladores como apresentado na figura A43 a seguir.

Figura A43 – Microcontrolador escondido sob componente original



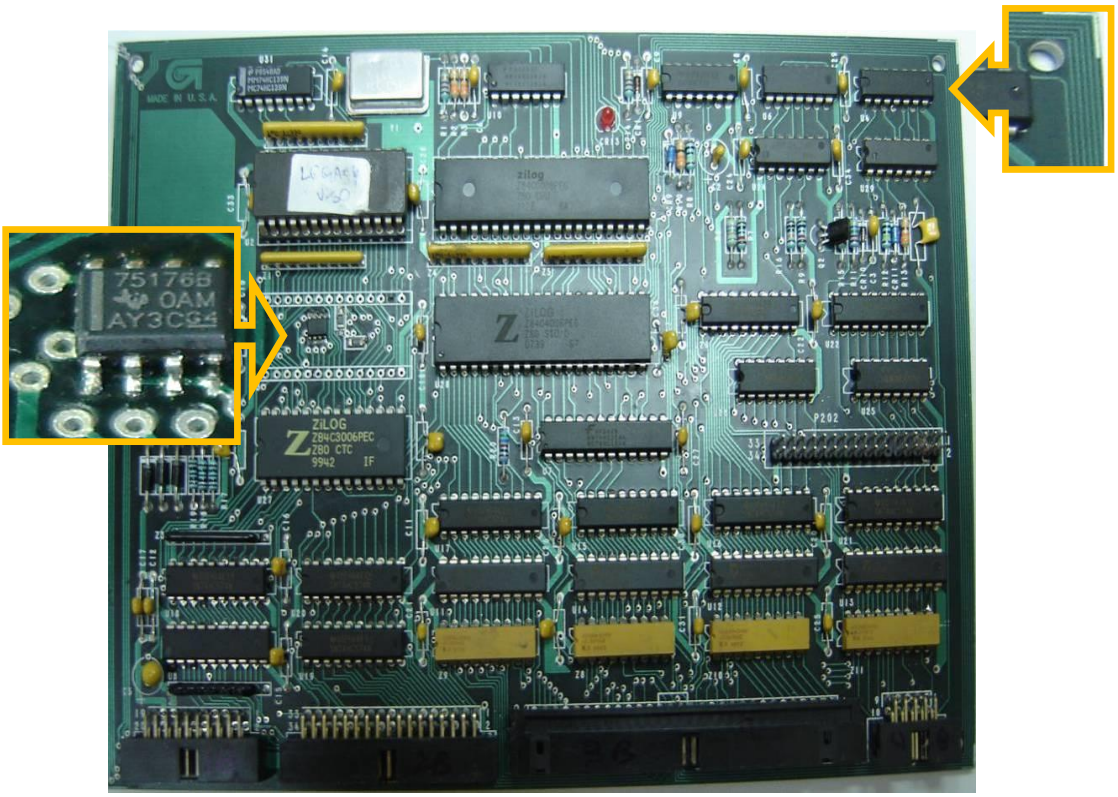
(A) (B)

Fonte: Disme/Sinst

A-4.2.3 Modelo 3 – Placa CPU falsa similar a placa da marca GBR para bombas modelo PRO ADV de 4 a 8 bicos, com montagem convencional.

A-4.2.3.1 A PCI a seguir (figuras A44) é uma CPU falsa que possui os componentes responsáveis pela fraude escondidos sob a memória que armazena o encerrante fiscal e sob o processador. Na imagem abaixo foi retirado o CI de memória do encerrante fiscal e é possível ver o transceptor RS-485 montado, responsável pela recepção dos comandos de acionamento/inibição da fraude. O acionamento se dá por comandos num computador, que chega até as bombas por cabo de rede. Uma forma fácil de identificar esta PCI fraudada é sua diferença em relação a original no tocante a inclusão de trilhas na região das bordas, conforme destaque na figura a seguir:

Figura A44(a) – PCI CPU falsa com fraude (modelo 3). Detalhes: transceptor RS-485 escondido sob o CI de memória (esquerda) e localização de trilhas adicionais na PCI que facilitam identificação da placa falsificada (direita).



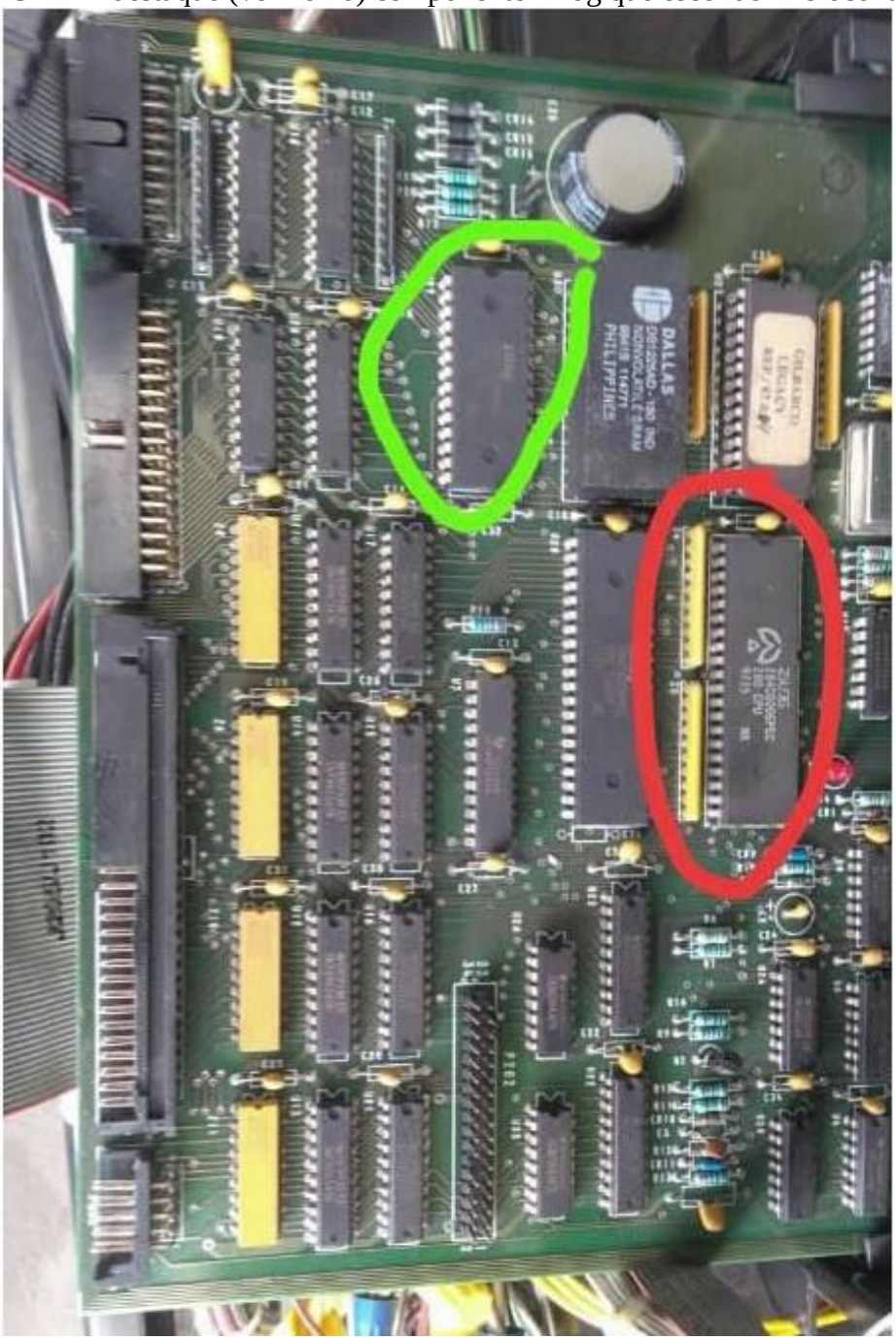
Fonte: Disme/Sinst

Figura A44 (b) - trilhas na lateral da placa, que somente são visualizadas após a remoção total

Fonte: IPEM-SP

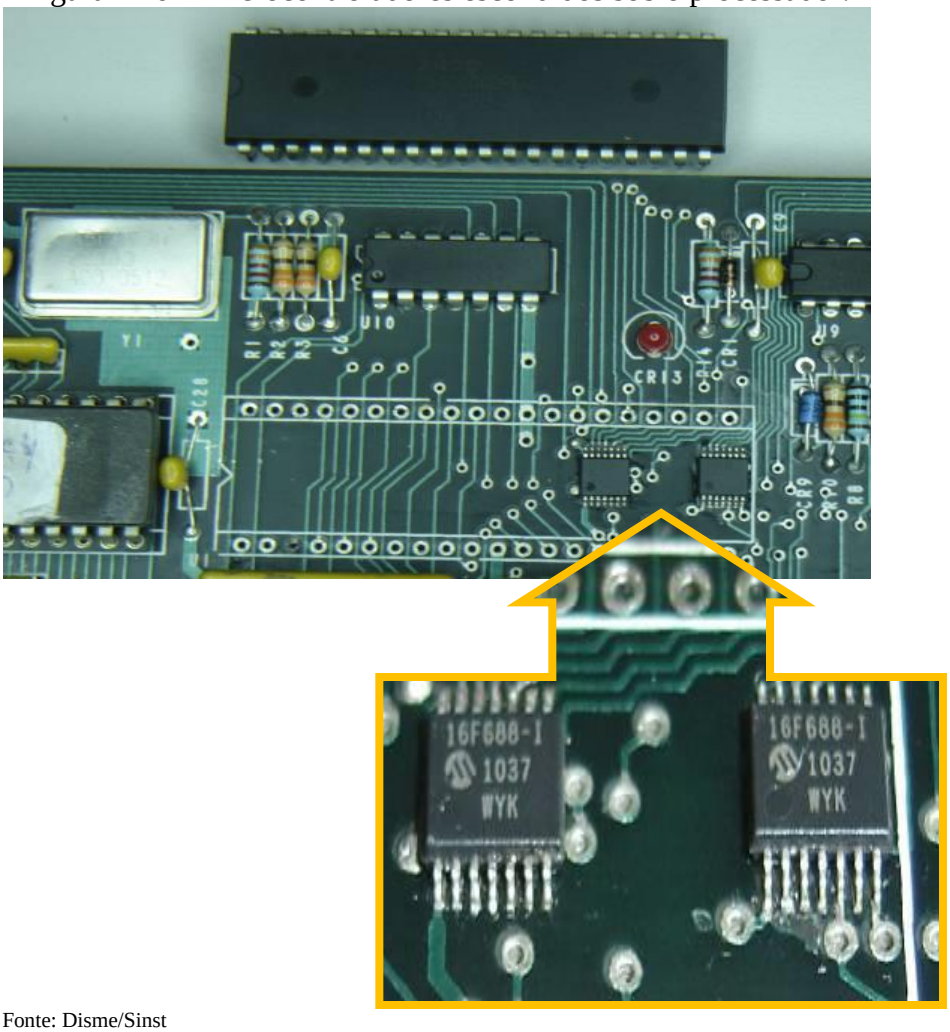
A-4.2.3.2 Nessa fraude, há microcontroladores embutidos sob Zilog, em destaque na figura A45. Na figura A46 é mostrado o detalhe dos microcontroladores escondidos sob o processador da placa CPU.

Figura A45 – Em destaque (vermelho) componente Zilog que esconde microcontroladoes.



Fonte: IPEM-SP

Figura A46 – Microcontroladores escondidos sob o processador.

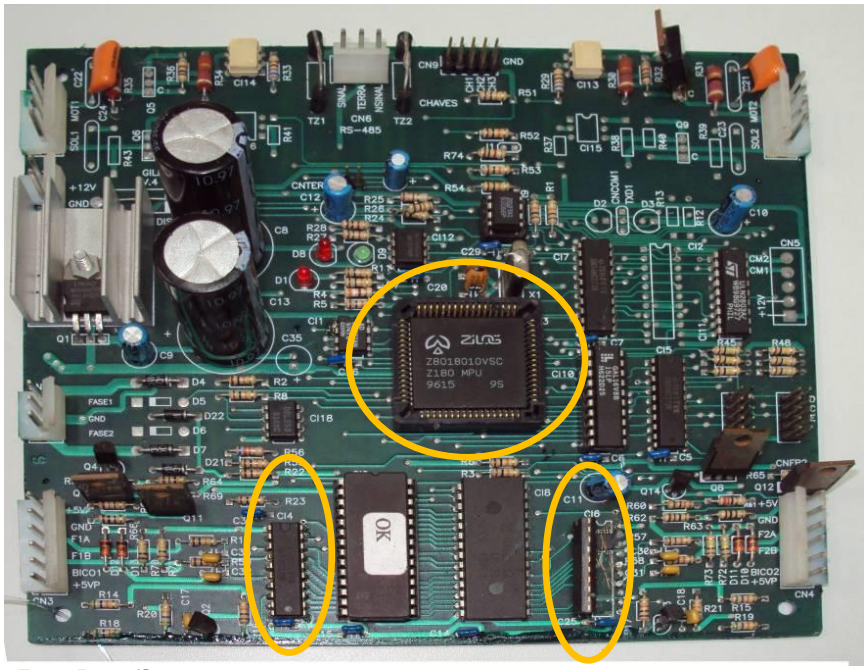


Fonte: Disme/Sinst

A-4.2.4 Modelo 4 – Placa de CPU marca Gilbarco para bomba modelo G180

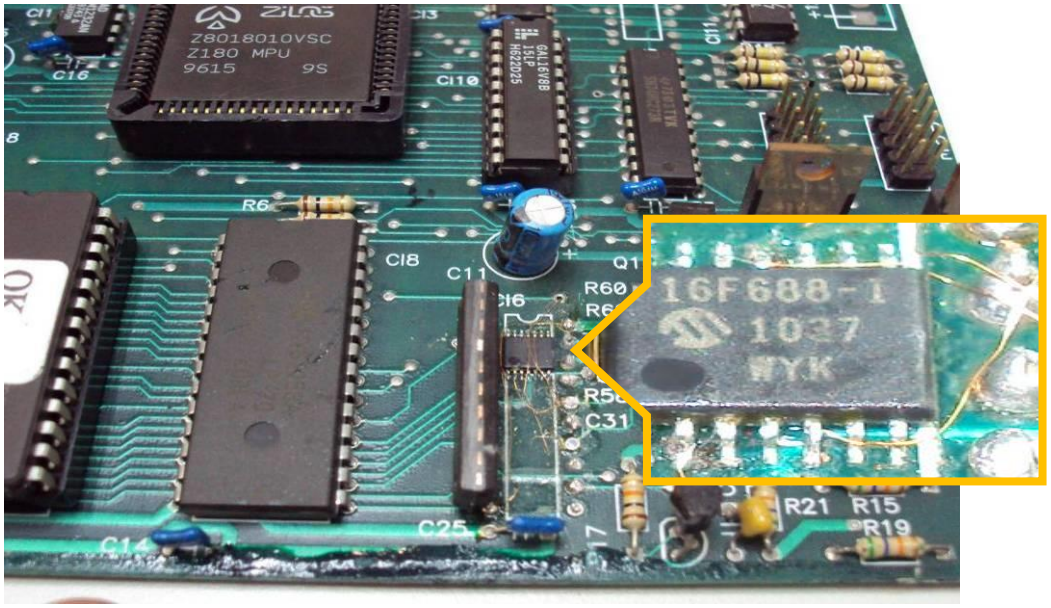
A-4.2.4.1 A figura A47 apresenta uma PCI de uma CPU original onde foram inseridos os componentes responsáveis pela fraude sob componentes originais (em destaque). Nas figuras A48 e A49 a seguir é possível observar detalhes da fraude.

Figura A47 – PCI CPU original com fraude (modelo 4). Destaque: pontos onde são inseridos componentes que implementam a fraude.



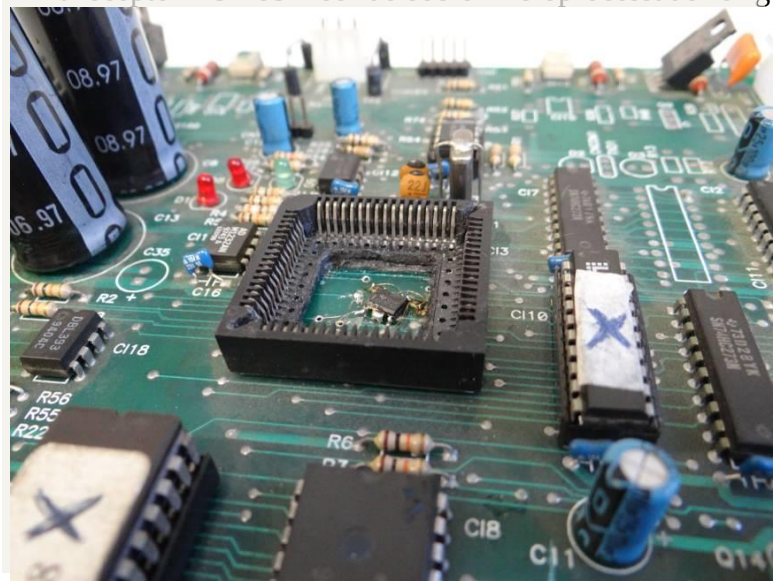
Fonte: Disme/Sinst

Figura A48 – Microcontrolador (destaque) e ligações com fios "*wire up*"



Fonte: Disme/Sinst

Figura A49 – Transceptor RS-485 inserido sob o microprocessador original da placa

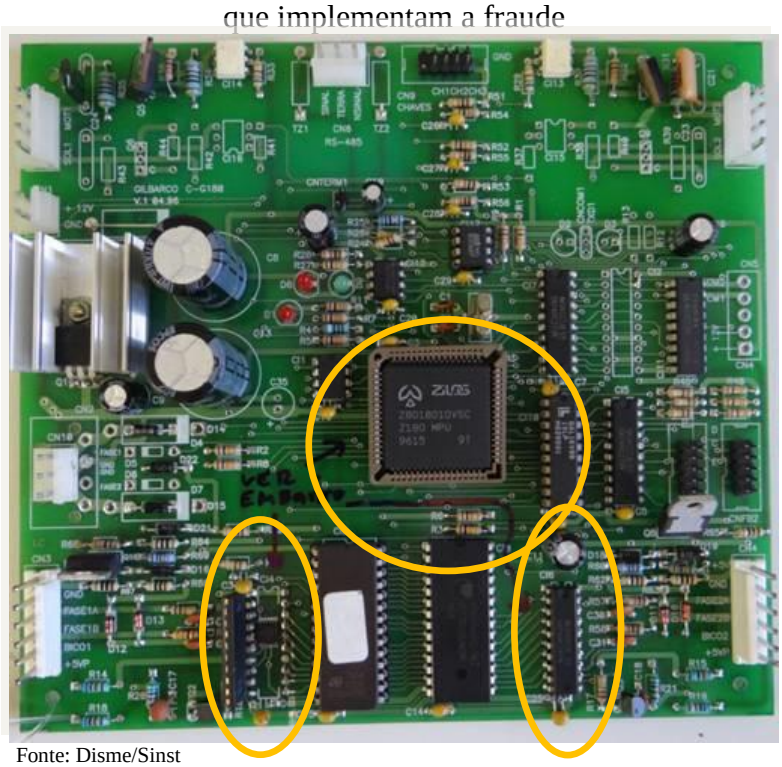


Fonte: Disme/Sinst

A-4.2.5 Modelo 5 – Placa CPU falsa similar a placa da marca Gilbarco para bombas modelo G180

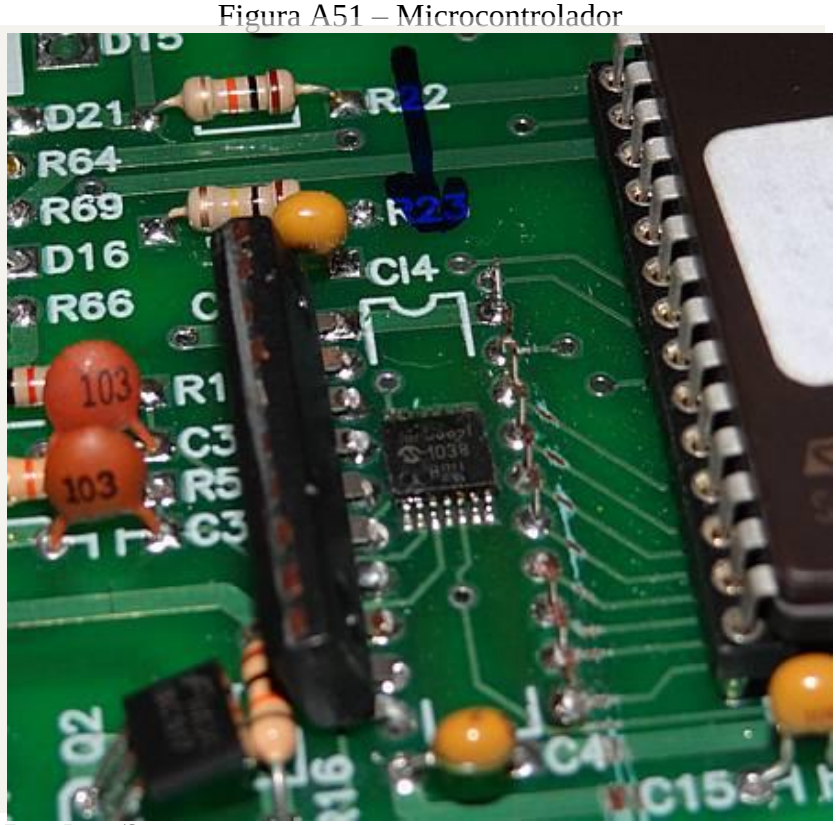
A-4.2.5.1 A figura A50 apresenta uma PCI que é uma CPU falsa. Os componentes responsáveis pela fraude estão escondidos sob outros componentes (em destaque). Nas figuras A51 e A52 abaixo é possível observar detalhes da fraude.

Figura A50 – PCI CPU falsa com fraude (modelo 5). Destaque: pontos onde são inseridos componentes que implementam a fraude



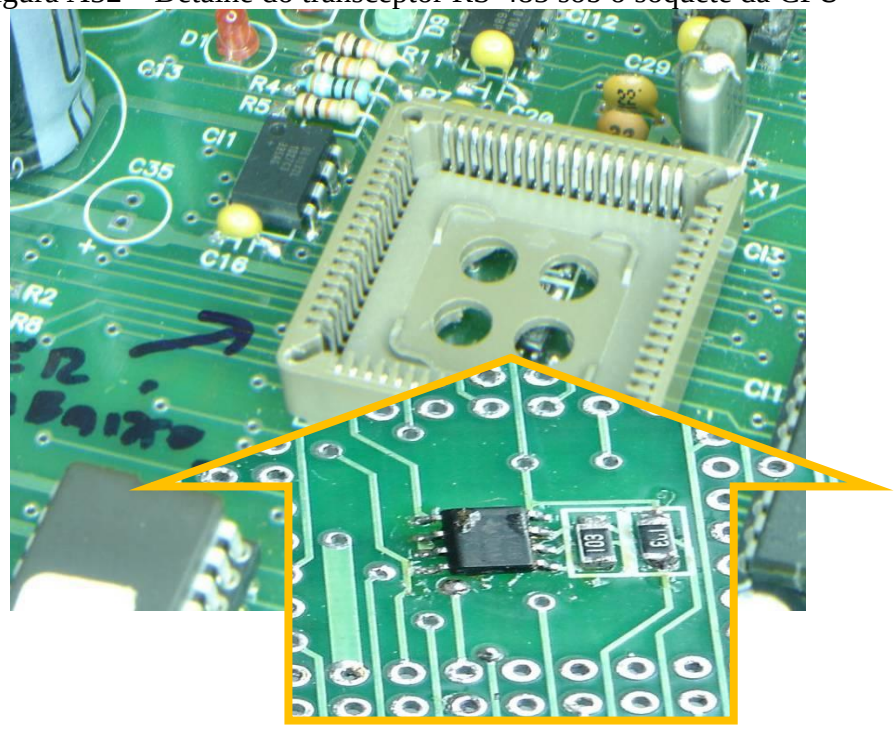
Fonte: Disme/Sinst

Figura A51 – Microcontrolador



Fonte: Disme/Sinst

Figura A52 – Detalhe do transceptor RS-485 sob o soquete da CPU



Fonte: Disme/Sinst

A-4.3 Fraude em Placa Falsa de CPU Acionada por Tensão de 12V

A-4.3.1 A tabela 9 a seguir apresenta as características dessa fraude.

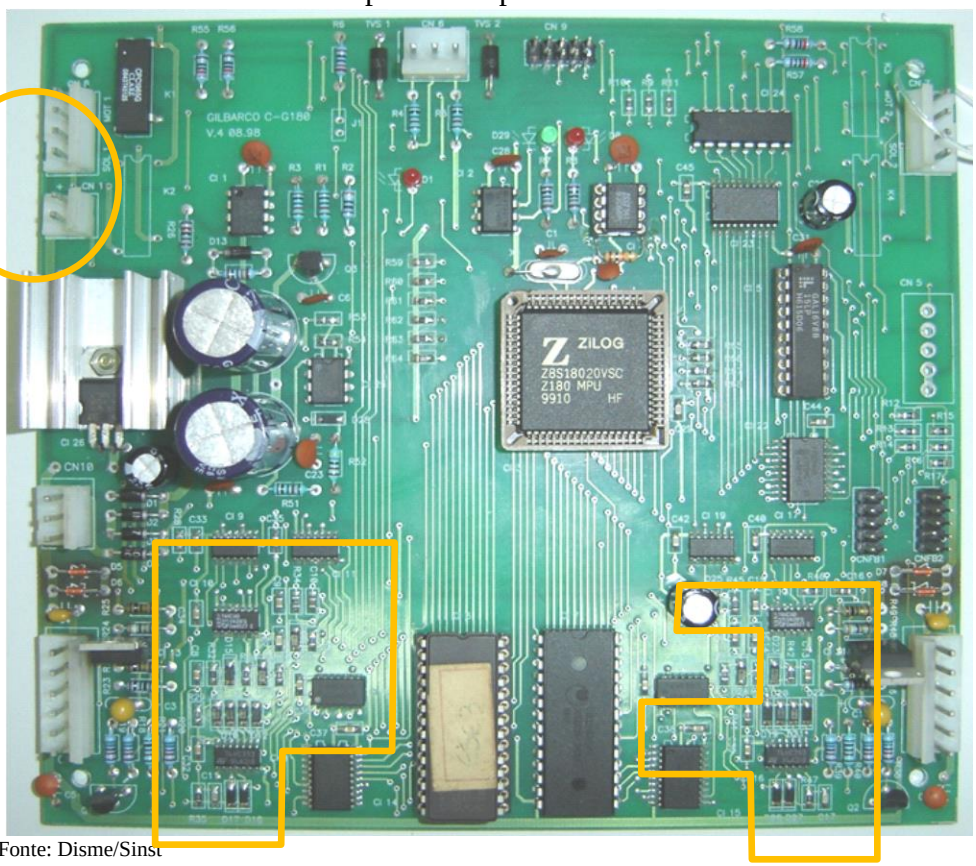
Tabela 9 – Características da fraude apresentada na figura A53

Componentes da fraude	Placa CPU falsificada
Operação	Os componentes em destaque na Figura A53 formam o circuito responsável pelo incremento da quantidade de pulsos gerados em um abastecimento.
Forma de acionamento/inibição	Aplicação de uma tensão de 12V ao conector da placa identificado como "CN1". Quando a tensão é retirada, a fraude é inibida. Até o momento não é conhecida a forma de acionamento externo. Este acionamento/inibição poderia se dar através de controle remoto, de forma semelhante aos casos anteriores, ou através de um interruptor instalado no instrumento.
Efeito	O resultado [da medição] apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Os valores típicos de erro percentual encontrados para este tipo de fraude variam entre -3% e -12%.

Fonte: Disme/Sinst

A-4.3.2 A PCI apresentada a seguir (figura A53) constitui uma fraude semelhante à que foi apresentada no subitem A-2.2.

Figura A53 – PCI CPU falsa com componentes adicionados. Destaque componentes e conector responsáveis pela fraude.



Fonte: Disme/Sinst

A-4.4 Fraude no Encerrante Fiscal

A-4.4.1 As fraudes no "encerrante fiscal" (ou totalizador) caracterizam-se pela utilização de uma modificação técnica não autorizada, que permite o fracionamento de informações de totalização do combustível vendido ao longo de um determinado tempo. Esta informação é importante para efeitos de fiscalização de arrecadação de impostos nos estados. A fraude se dá de forma permanente ou controlada, dividindo-se a quantidade total em duas partes e armazenando-as em posições diferentes de memória. Isso faz com que durante uma fiscalização de rotina seja apresentado um total das vendas menor daquele efetivamente praticado, incorrendo em sonegação de impostos. A tabela 10 e a figura A54 apresentam as características dessa fraude.

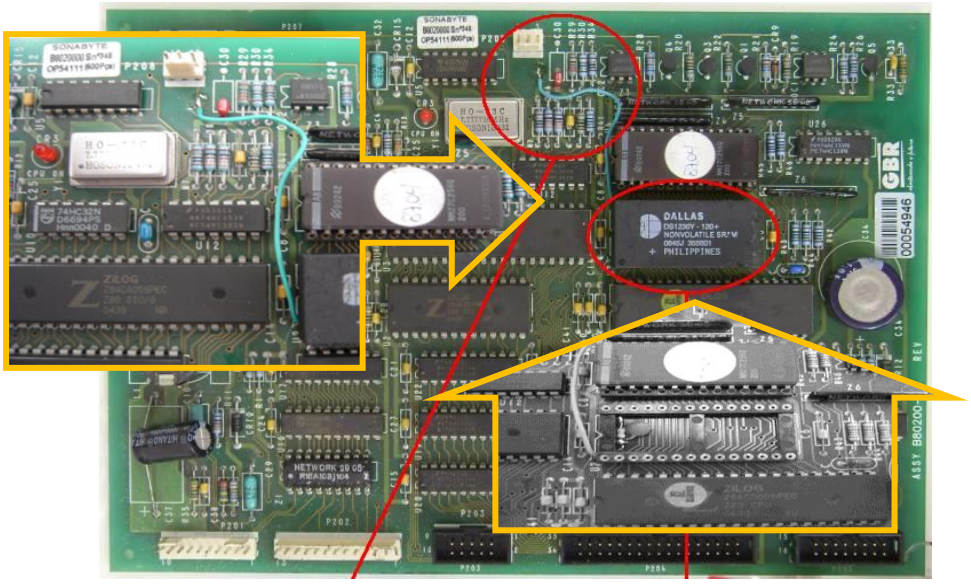
Tabela 10 – Características da fraude apresentada na figura A54

Componentes da fraude	Placa CPU original Memória SRAM Componentes eletrônicos passivos (resistor, capacitor) e fios
Operação	Consiste na alteração do endereço de memória onde é registrada a totalização das vendas de combustível. Isto é feito através da aplicação de uma tensão elétrica em um terminal específico da memória SRAM. O resistor, capacitor e fio conduzem a tensão a este terminal que não é utilizado no projeto original do fabricante. O fraudador pode escolher em qual endereço de memória será registrada a totalização das vendas, dividindo-a em duas partes.
Forma de acionamento/inibição	Desconhecida. Pode ser utilizado algum tipo de interruptor/chave para acionar a fraude e, consequentemente, alterar o endereço de memória.
Efeito	Apresenta às autoridades de controle de impostos um total de vendas menor do que o praticado. Não afeta o resultado da medição de volume de vendas individuais.

Fonte: Disme/Sinst

A-4.4.2 A imagem a seguir (figura A54) apresenta detalhes da inclusão de um fio para possibilitar a ativação/inibição da fraude e a inclusão de um capacitor e um resistor que configuram o endereço de memória dividindo a informação original em duas partes. O resistor e o capacitor podem tanto estar presentes na PCI, junto ao soquete da memória SRAM, como soldados nos próprios terminais desta memória

Figura A54 (a) – Detalhe de implementação da fraude encerrante.

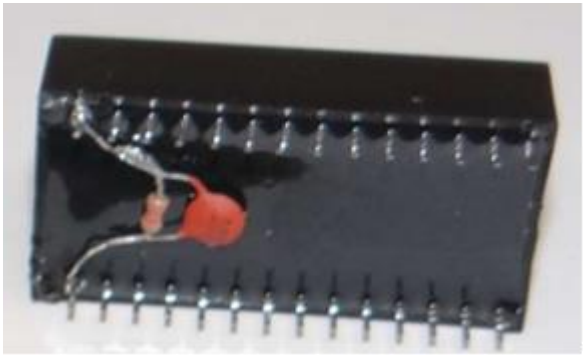


Fonte: Disme/Sinst

Figura A54 (b) – Detalhe de implementação da fraude de encerrante no soquete da memória SRAM.

Fonte: Disme/Sinst

Figura A54 (c) – Detalhe de implementação da fraude de encerrante na memória SRAM.



Fonte: Disme/Sinst

A – 4.5 Fraude em Placa Adulterada em BMC

A-4.5.1 Nessa fraude são colocados microcontroladores e *wire-up's* sob a memória RAM. A figura A55 apresenta uma visão da placa.

Figura A55 – Placa [CPU com fonte]

Fonte: IPEM-SP

A-4.5.2 A figura A56 apresenta uma visão do microcontrolador e dos fios (*wire-up's*) após a retirada da memória RAM.

Figura A56 – Microcontrolador e *wire-up's* sob a memória RAM da placa

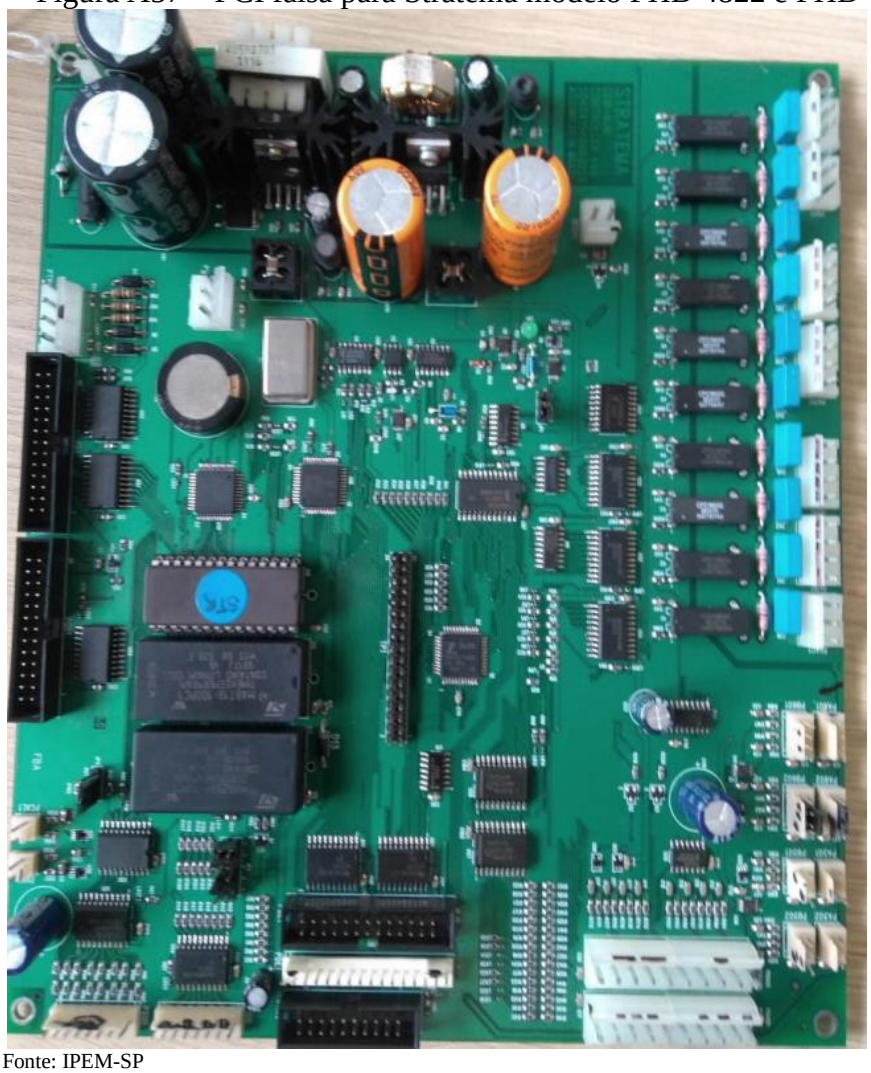
Fonte: IPEM-SP

A – 4.6 CPU Falsa Stratema Modelo PHD 4822 e PHD 4821

A-4.6.1 Nessa fraude, constatada numa PCI falsa para Stratema modelo PHD 4822 e PHD 4821 (vide figura A57) existe um microcontrolador sob a memória em destaque na figura A58.

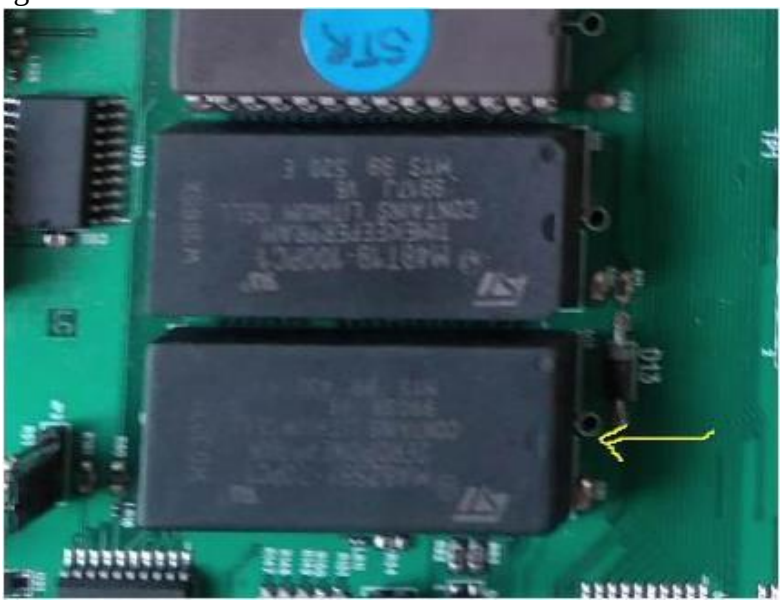
A-4.6.2 Para facilitar a constatação, desligue a bomba no disjuntor e passe uma tira plástica por baixo dos componentes. Caso tenha alguma obstrução, utilize uma lupa para visualizar o microcontrolador.

Figura A57 – PCI falsa para Stratema modelo PHD 4822 e PHD 4821



Fonte: IPEM-SP

Figura A58 – Há um microcontrolador sob a memória indicada



Fonte: IPEM-SP

A-4.6.3 Esta fraude é ativada por comandos através de computador, e ainda não se sabe a quantidade da fraude, e, também, maiores informações sobre o acionamento.

A-4.7 Fraude em Placa de CPU Acionada por via rede de automação

A-4.7.1 A identificação do material examinado é realizada através de inspeção visual, pois trata-se de fraude conhecida.

A-4.7.2 A localização de instalação dos itens que compõem a fraude, no instrumento de medição, é ampla. Diversos componentes originais são substituídos ou modificados para o funcionamento da bomba medidora de combustíveis.

A-4.7.3 Os itens componentes da fraude são os *pulsers*, *displays*, transformador, contatores e placa de CPU.

A-4.7.4 São apresentados a seguir os componentes que modificam o instrumento e não estão conformes à PAM original da BMC:

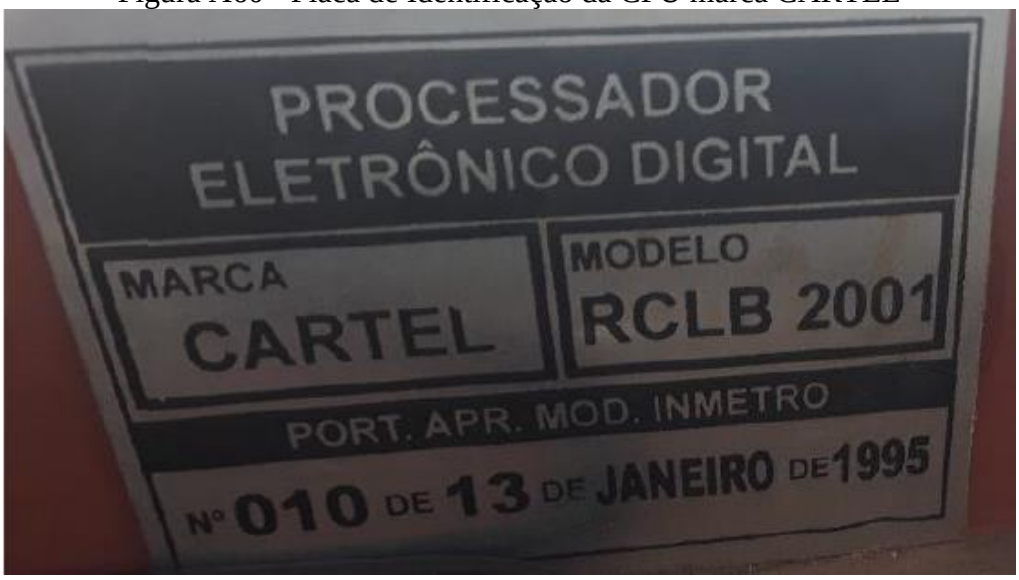
a) CPU: a placa CPU apresentada na Figura A59 reúne as funções de fonte de alimentação, CPU, interface hidráulica, interface de teclado e canal de comunicação. Esta placa dispõe de um software capaz de receber comandos pela interface de comunicação para acionar/inibir a fraude. A versão do software é apresentada através de inscrição DDMMAAAA, correspondendo à data em que o software foi carregado na CPU. As possíveis inscrições WNEW3, GNEW3, W50, G25, Sxx, correspondem a BMC de Fabricante/vazão máxima em que as fraudes forem instaladas;

Figura A59 – Placa de CPU marca CARTEL

Fonte: Disme/Sinst

b) identificação: a placa CPU recebe identificação interna à BMC com uma placa conforme a Figura A60;

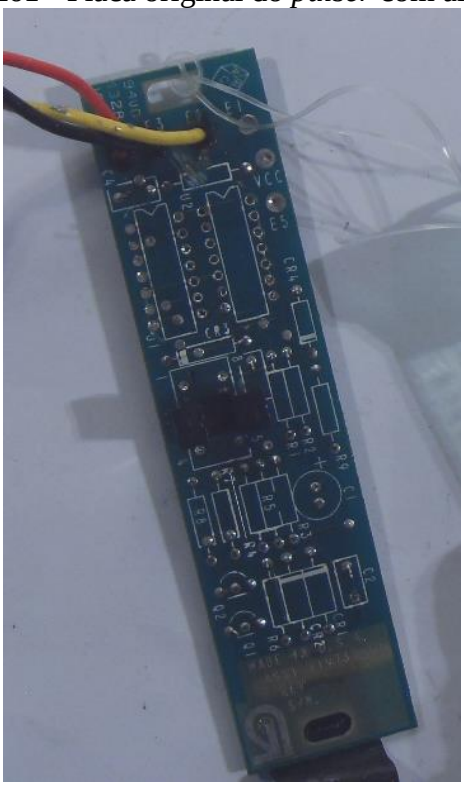
Figura A60 - Placa de Identificação da CPU marca CARTEL



Fonte: Disme/Sinst

c) pulsers: as placas originais dos *pulsers* podem receber alterações, conforme apresentado na Figura A61;

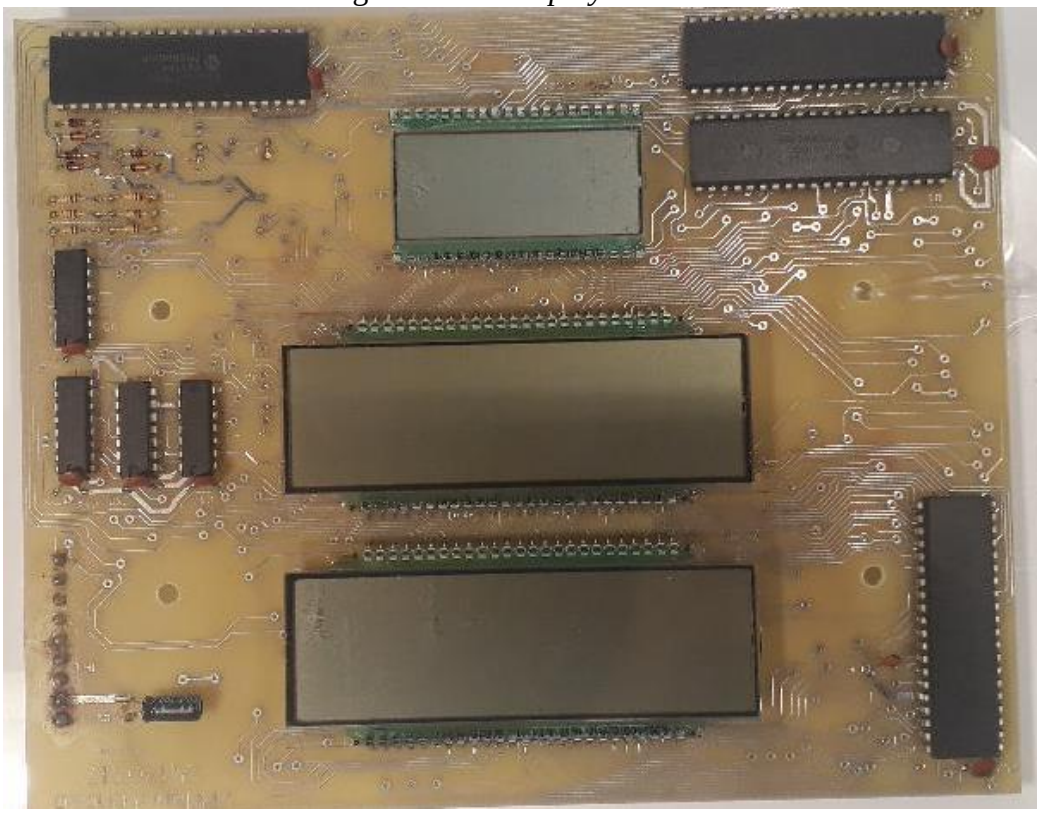
Figura A61 - Placa original do *pulser* com alterações



Fonte: Disme/Sinst

d) displays: os *displays* são substituídos por placas modificadas, conforme a Figura A62. Estas placas são sistematicamente instaladas em diversos modelos de BMC;

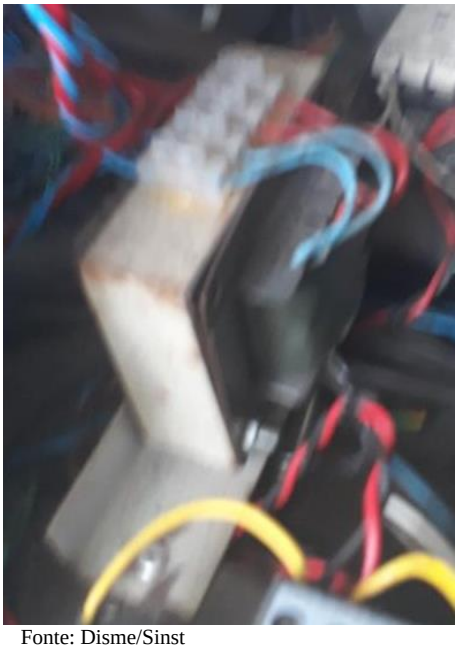
Figura A62 – *Display* de LCD



Fonte: Disme/Sinst

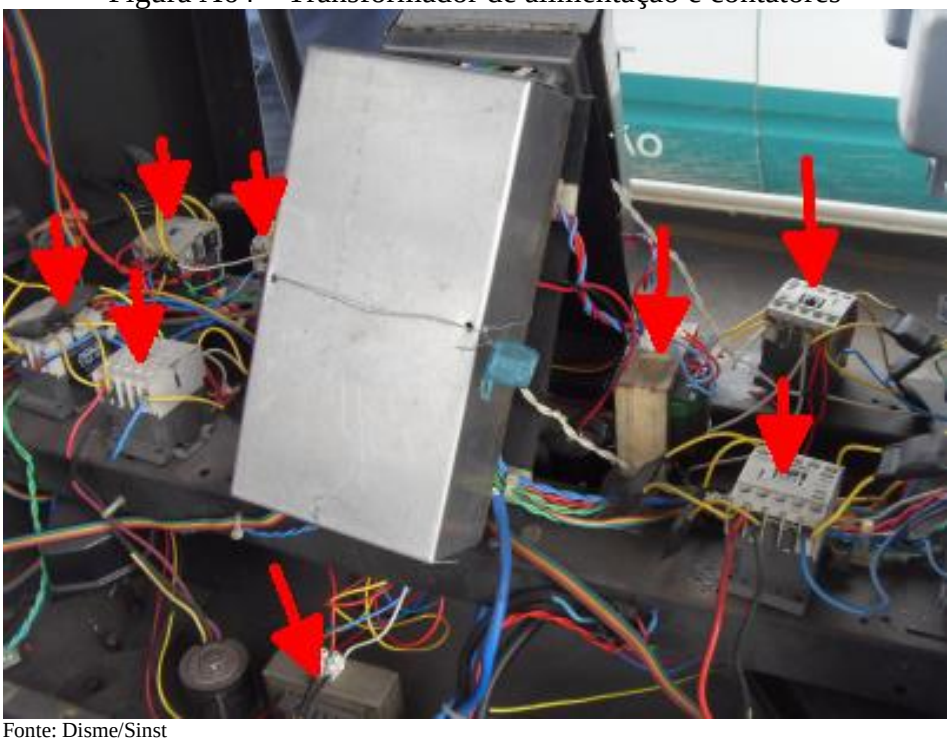
e) transformadores: são adicionados transformadores para a fonte de alimentação, conforme as Figuras A63 e A64;

Figura A63 - Transformador de alimentação



Fonte: Disme/Sinst

Figura A64 – Transformador de alimentação e contatores



Fonte: Disme/Sinst

f) contatores: para acionamento dos motores e solenóides são adicionados contatores, conforme a Figura A64;

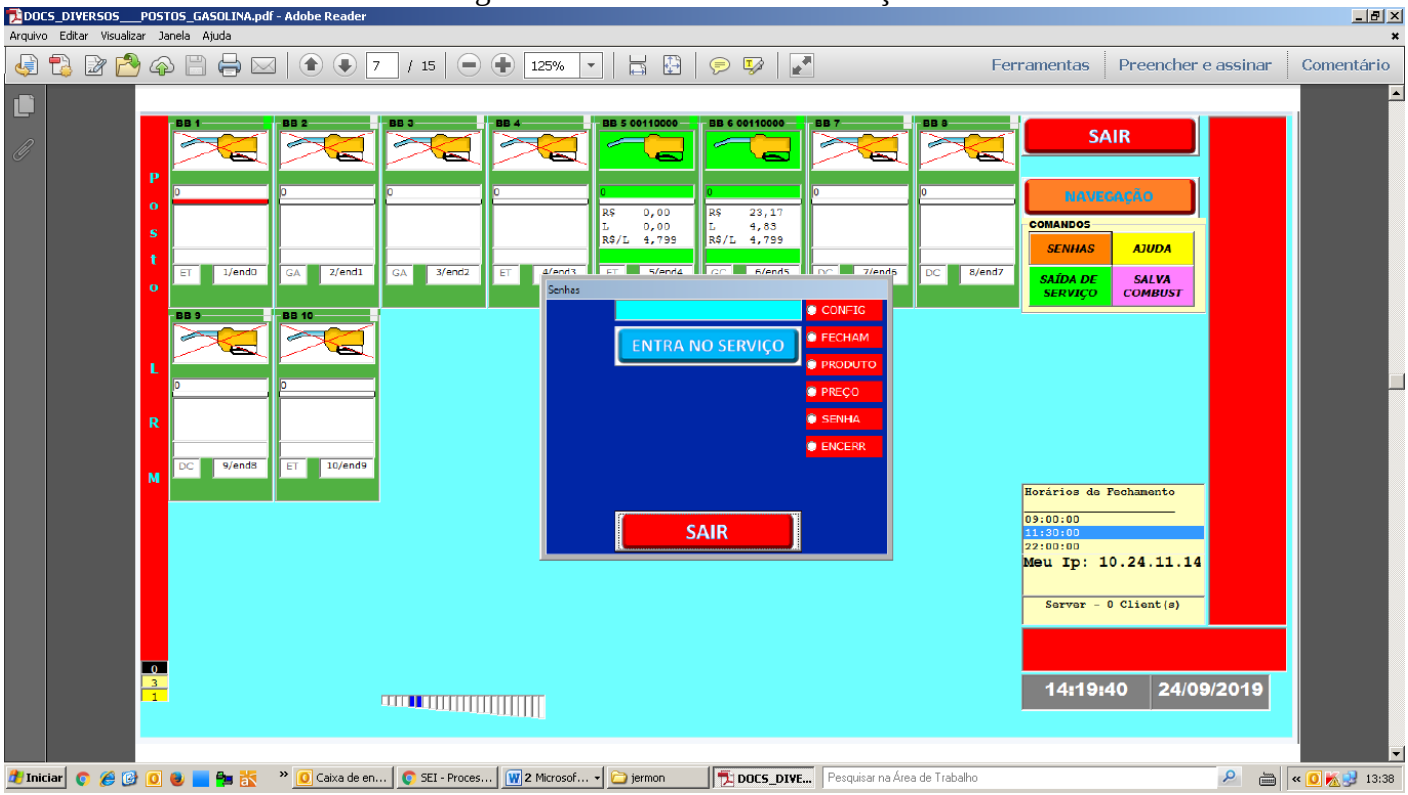
g) conversor de interface RS-232/RS-485: a rede de comunicação entre a placa CPU instalada na BMC é feita através de um conversor de interface RS-232/RS-485, normalmente localizado próximo e diretamente conectado ao computador que gerencia o abastecimento ou o gerenciamento das bombas medidoras. Este adaptador é mostrado na Figura A65. Em alguns exemplares destas caixas há disponível uma chave que permite ativar/inibir a fraude independente do software de controle; e

Figura A65 - Conversor RS-232 para RS-485

Fonte: Disme/Sinst

h) sistema de automação: através de comandos remotos enviados por um programa em um computador ligado às bombas através de uma rede RS-485. O sistema de automação (figura A66) possui uma tela secreta onde é possível enviar comandos para ativação da fraude. Os comandos são transmitidos à placa CPU através da rede de automação RS-485.

Figura A66 – Sistema de Automação



Fonte: Disme/Sinst

A.4.7.5 A tabela 11 a seguir apresenta as características dessa fraude.

Tabela 11 – Características da fraude apresentada nas figuras A59 a A66

Componentes da fraude	Placas CPU (Figura A59) marca Cartel acompanhada de placa de identificação com inscrição da portaria de aprovação de modelo nº 10 de 13 de janeiro de 2001 (Figura A60). *Pulsers* alterados (Figura A61). *Display* de LCD (Figura A62). Transformador de alimentação e contatores (Figuras A63 e A64). Conversor RS-232 para RS-485 (Figura A65) Computador externo à bomba interligado através de rede RS-485.
Operação	A CPU destacada na Figura A59 recebe comandos de acionamento/inibição da fraude através da rede de automação e incrementam a quantidade de pulsos gerados em um abastecimento. Um sinal elétrico de aterramento pode ser enviado para a placa CPU e acionar/inibir a fraude, através de uma chave instalada na caixa do conversor RS-232 para RS-485.
Forma de acionamento/inibição	Através de comandos remotos enviados por um programa em um computador ligado as bombas através de uma rede RS-485. O sistema de automação (Figura A66) possui uma tela secreta onde é possível enviar comandos para ativação da fraude. Os comandos são transmitidos à CPU através da rede de automação RS-485. Uma chave elétrica instalada na caixa do conversor RS-232 para RS-485 pode inibir a fraude, independente do comando enviado pelo computador.

(continua)

Efeito	O volume apresentado pelo *display* da bomba é maior do que o volume abastecido. O erro percentual da medida é configurável, podendo variar entre 4% e 12% em desfavor do consumidor.

Fonte: Disme/Sinst

A-5 FRAUDES LOCALIZADAS NOS CABOS DE COMUNICAÇÃO ENTRE PCI E ENTRE PCI E TRANSDUTORES (modelos 1, 2, 3, 4 e 5)

A-5.1 As fraudes observadas anteriormente consistem na alteração do sinal que é gerado no *pulser* e que é utilizado para determinação do resultado da medição de volume. Como os fios que fazem as conexões elétricas entre as placas do instrumento também conduzem este sinal, esta vulnerabilidade também é explorada por fraudadores. Estes fios são rompidos e neste caminho são inseridos componentes que efetuam fraudes.

A-5.2 A tabela 12 a seguir apresenta as características dessa fraude.

Tabela 12 – Características da fraude apresentada nas Figuras A67 a A109

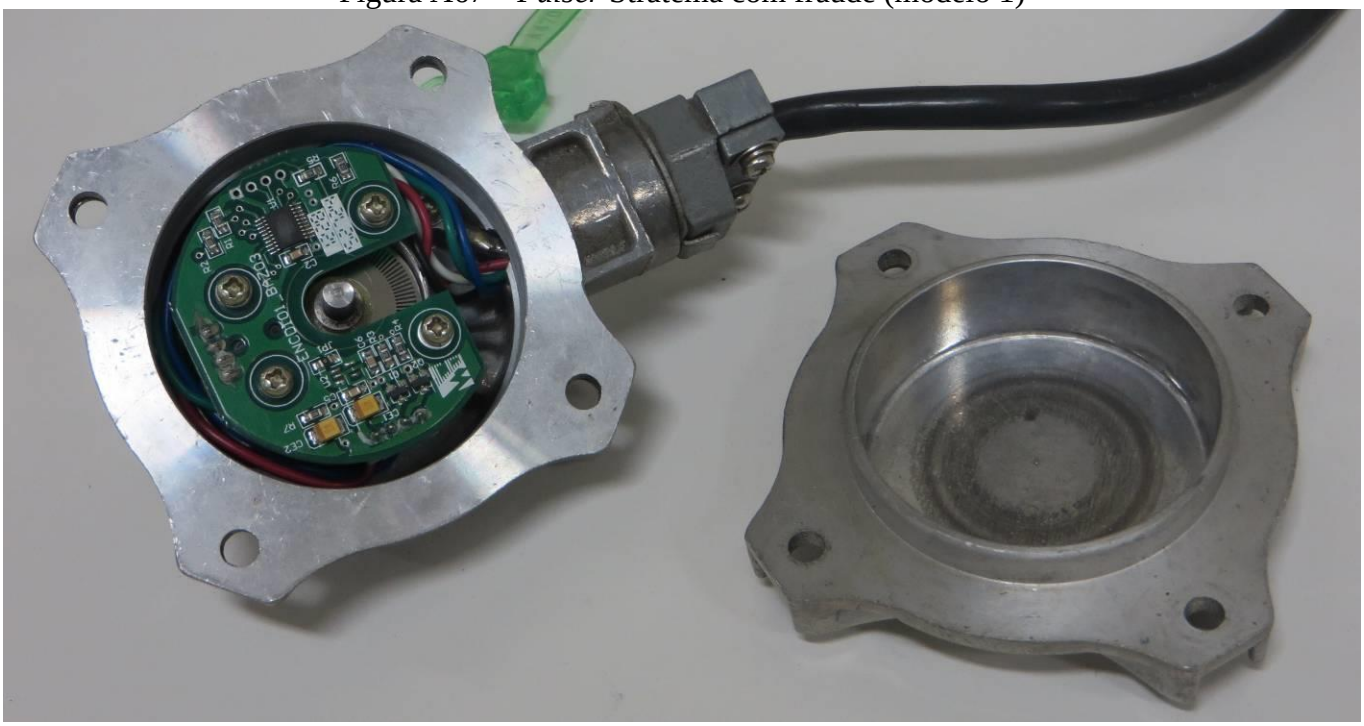
Componentes da fraude	PCI pequena Microcontrolador
Operação	Os fios que conduzem o sinal utilizado para determinação do resultado da medição são interrompidos. Microcontroladores ou circuitos digitais são inseridos neste caminho. Uma pequena PCI pode estar presente ou não. Os componentes inseridos incrementam a quantidade de pulsos originais gerados em um abastecimento.
Forma de acionamento/inibição	Existe a possibilidade de acionamento/inibição remoto da fraude. Para todos os casos analisados, foi identificado que o acionamento da fraude se dá através da conexão de um terminal com o aterramento do instrumento. Este acionamento/inibição externo poderia se dar através de controle remoto, de forma semelhante aos casos anteriores, ou através de um interruptor instalado no instrumento. O uso de sequência de liga e desliga da alimentação da cabeça da BMC, também pode ser utilizada para acionamento desta fraude, em destaque para Figuras A83 a A85 que consiste neste tipo de acionamento.
Efeito	O resultado apresentado no *display* da bomba é maior do que o volume realmente abastecido. O erro percentual da medida é fixo para cada abastecimento. Seu valor pode variar entre -6% e -25%.

Fonte: Disme/Sinst

A-5.3 Modelo 1 – *Pulser* Stratema com Fraude no Fio/Conector

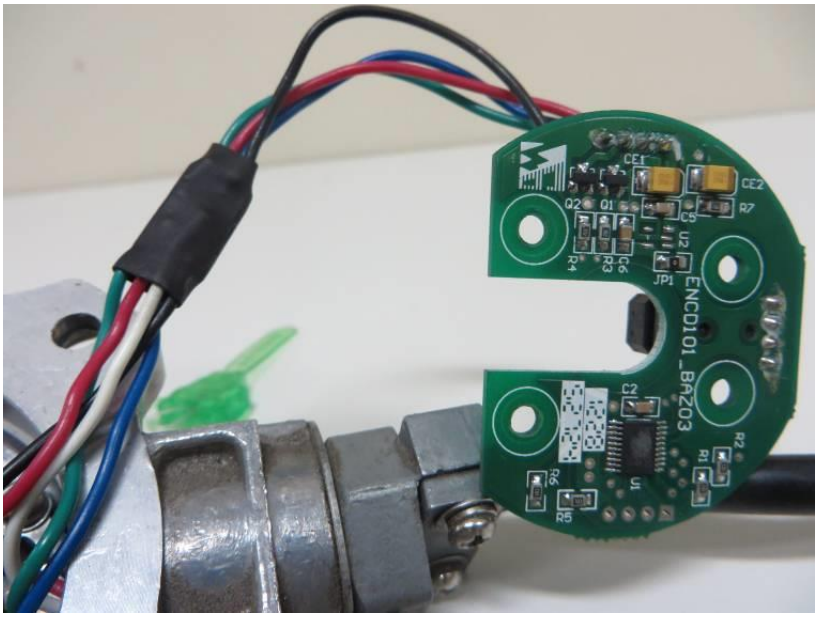
A-5.3.1 A figura A67 a seguir apresenta um *pulser* Stratema onde é implementada uma fraude no cabo que conduz os pulsos gerados durante o abastecimento. É necessário desmontar o *pulser* e retirar a PCI com a fraude de seu interior para a correta identificação, já que a placa com a fraude se encontra normalmente envolvida por material isolante (Fig. A68).

Figura A67 – *Pulser* Stratema com fraude (modelo 1)



Fonte: Disme/Sinst

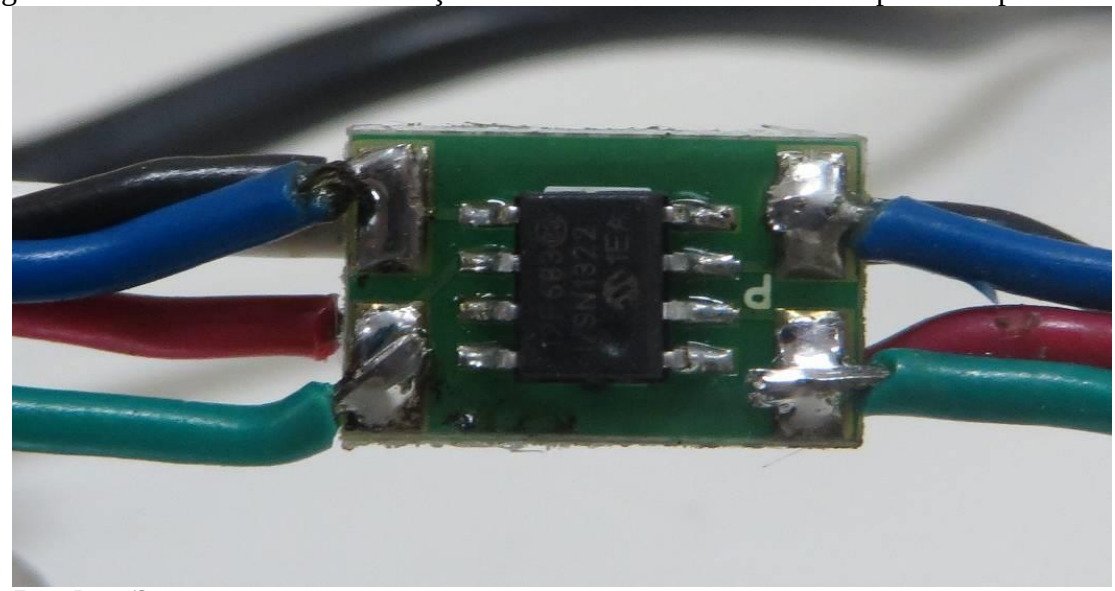
Figura A68 – Retirando a placa do *pulser*, encontra-se parte da fiação envolvida em material isolante.



Fonte: Disme/Sinst

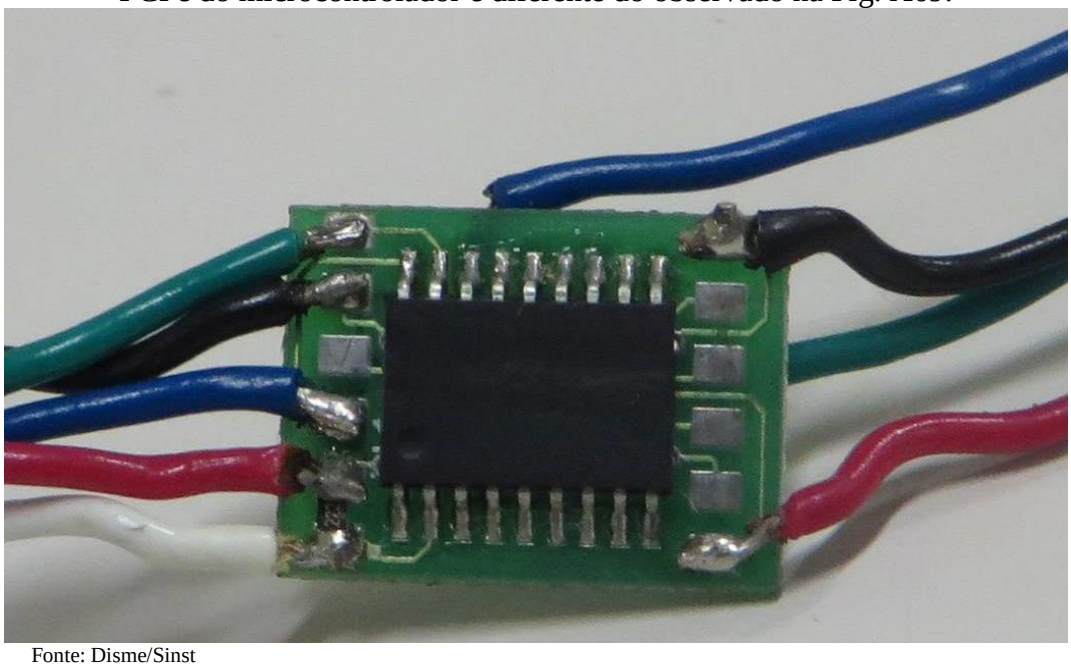
A-5.3.2 A placa e o microcontrolador podem ter tamanhos ligeiramente diferentes dependendo dos componentes utilizados na fraude (figura A69 e A70).

Figura A69 – PCI encontrada na fiação contendo microcontrolador responsável pela fraude.



Fonte: Disme/Sinst

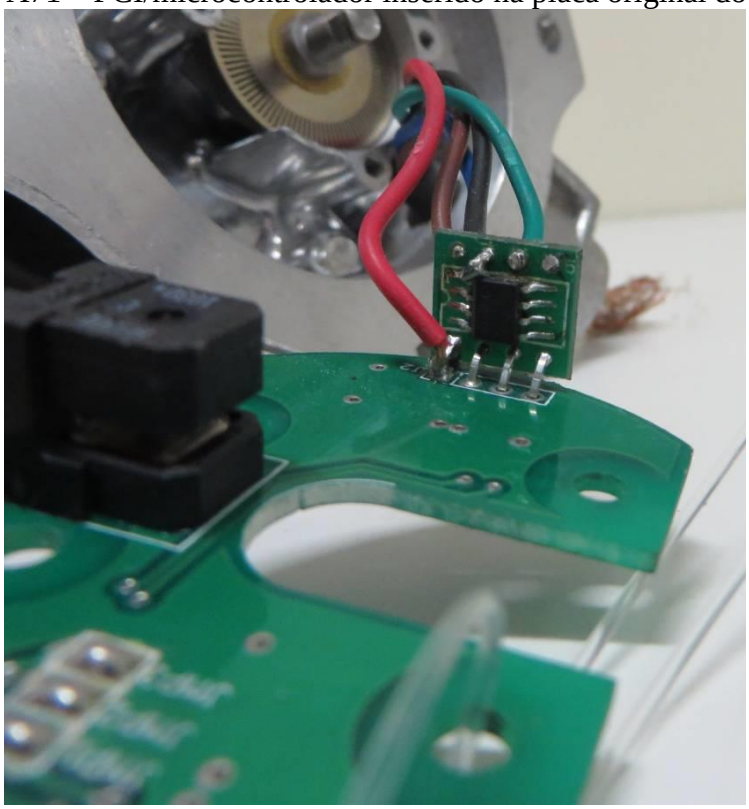
Figura A70 – PCI encontrada na fiação contendo microcontrolador responsável pela fraude. O formato da PCI e do microcontrolador é diferente do observado na Fig. A69.



Fonte: Disme/Sinst

A-5.3.3 Outra forma encontrada de inserção da fraude é apresentada na figura A71. Neste caso, a pequena placa contendo o microcontrolador responsável pela fraude foi inserida na própria placa original do *pulser*.

Figura A71 – PCI/microcontrolador inserido na placa original do *pulser*

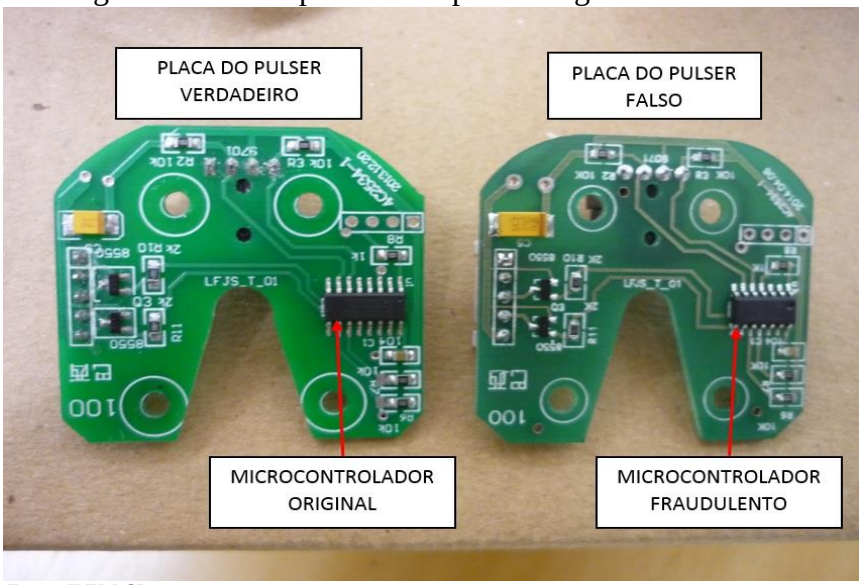


Fonte: Disme/Sinst

A-5.4 Modelo 2 *Pulser* Falso Similar ao Stratema (trilha de acionamento na face oposta)

A-5.4.1 A figura A72 a seguir, mostra o detalhamento do *Pulser* Stratema e comparativo com o falso.

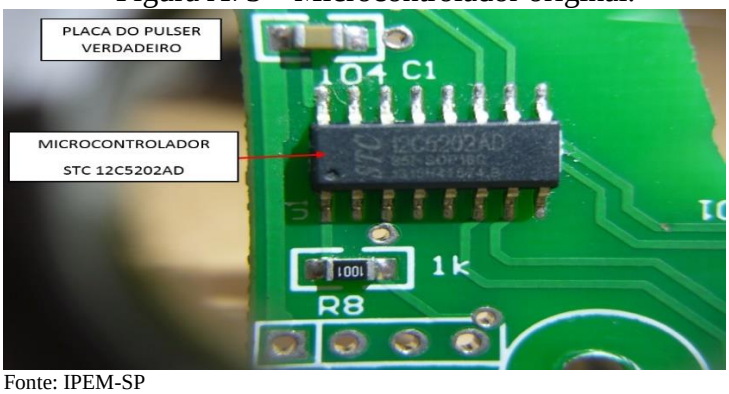
Figura A72 –Comparativo do pulser original com o falso



Fonte: IPEM-SP

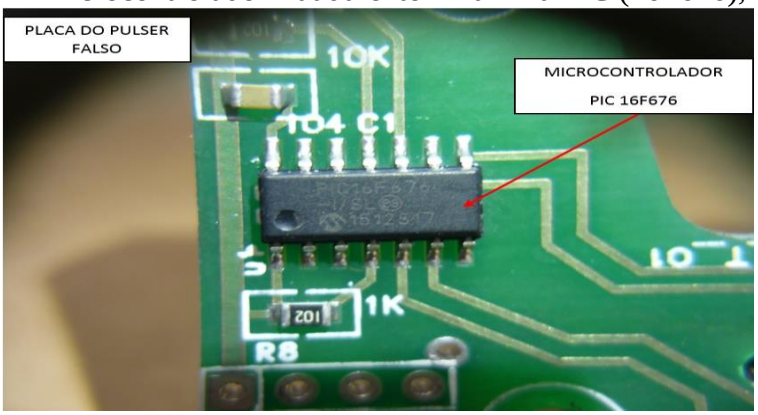
A-5.4.2 Analisando-se a face frontal da PCI não se percebe qualquer diferença; para verificar se a PCI é falsa, é necessário analisar o microcontrolador: nas PCI's falsas são utilizados microcontroladores das famílias PIC ou ATMEL, conforme as figuras A73, A74 e A75.

Figura A73 – Microcontrolador original.



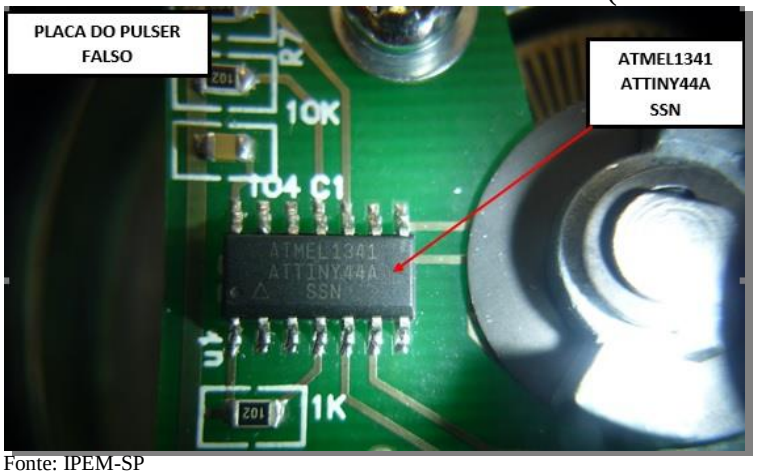
Fonte: IPEM-SP

Figura A74 – Microcontrolador fraudulento – Família PIC (16F676), neste caso.



Fonte: IPEM-SP

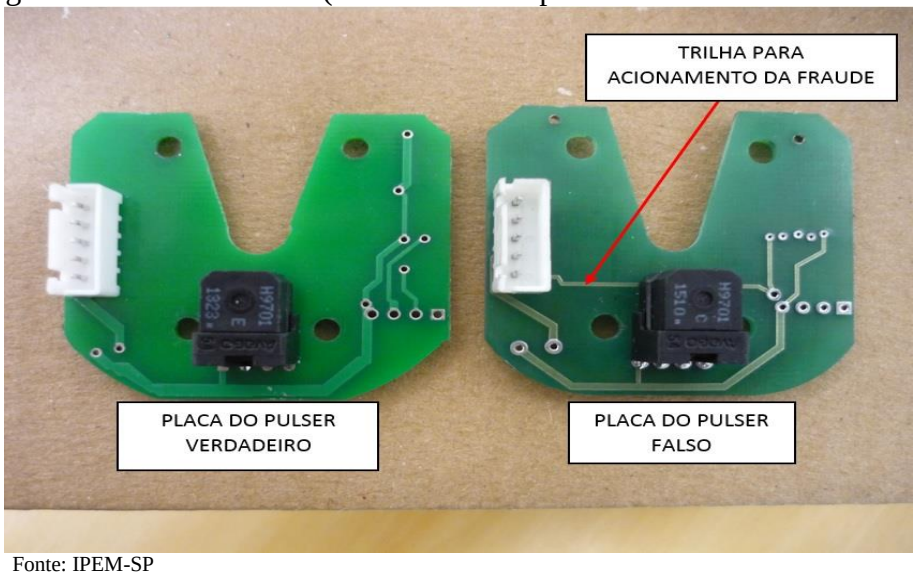
Figura A75 – Microcontrolador fraudulento – Família ATMEL (ATMEL1341), neste caso.



Fonte: IPEM-SP

A-5.4.3 Outro indício para constatar se o *pulser* é falso pode ser obtido retirando-se a PCI do *Pulser* para verificar se sua face oposta contém uma trilha adicional para o acionamento da fraude, conforme figura A76.

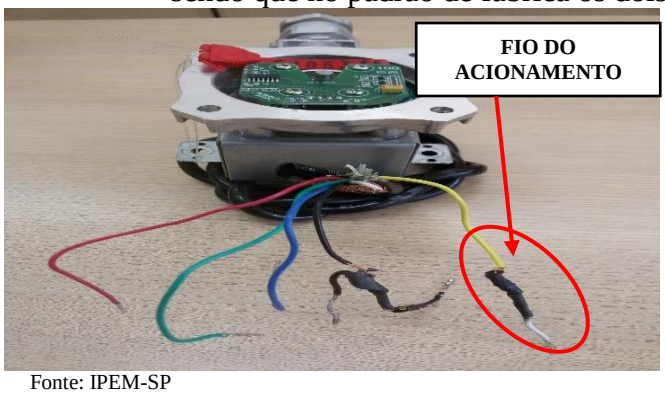
Figura A76 – Face da PCI (falsa com trilha para o acionamento da fraude).



Fonte: IPEM-SP

A-5.4.4 O acionamento, geralmente é feito através de um dos fios que compõe o cabo de comunicação do *pulser*, geralmente o fio de cor amarela, conforme mostrado na figura A77. Normalmente o fio amarelo está junto com o fio preto – neutro.

Figura A77 – O fio amarelo que deveria estar junto com o preto está sendo usado para o acionamento, sendo que no padrão de fábrica os dois ficam juntos geralmente.



Fonte: IPEM-SP

Fonte: IPEM-SP

A-5.4.5 Neste tipo de fraude, o volume abastecido é menor que o resultado da medição apresentado no display da bomba em questão. O erro percentual da medida é por volta de -10% para cada abastecimento.

A-5.5 Modelo 3 – *Pulser* Falso - Similar ao *Pulser* da marca Stratema (trilha de acionamento – placa multicamada)

A-5.5.1 As figuras A78 e A79, a seguir, mostram o detalhamento e comparativo da PCI do *pulser* original com a falsa.

Figura A78 – PCI original

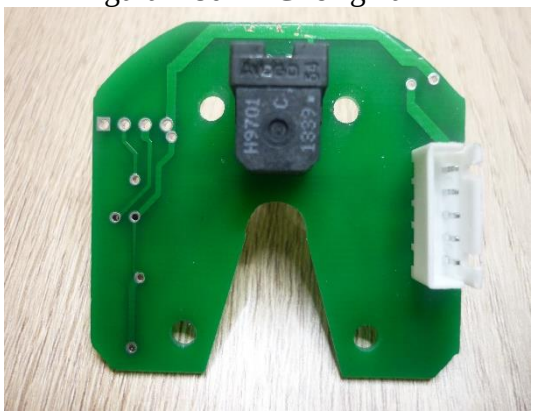
Fonte: IPEM-SP

Figura A79 - PCI falsa

Fonte: IPEM-SP

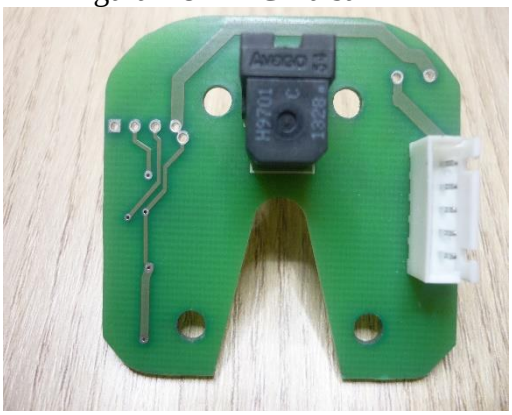
A-5.5.2 Ao se observar a face oposta contra a luz, verifica-se a presença de uma trilha adicional (vide figura A80 e A81) com o objetivo de acionar a fraude.

Figura A80 – PCI original



Fonte: IPEM-SP

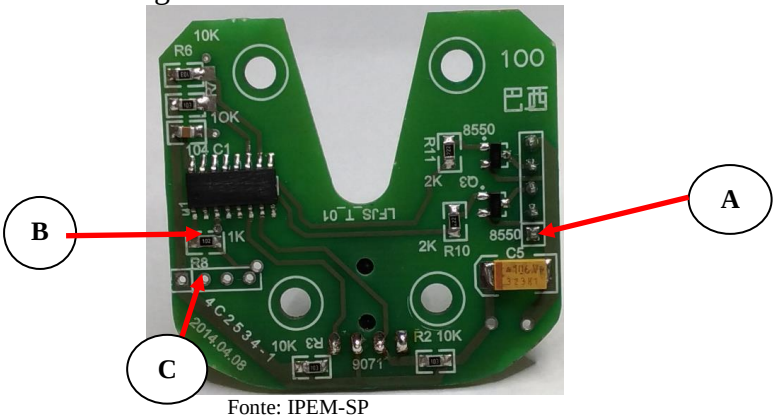
Figura A81 - PCI falsa



Fonte: IPEM-SP

A-5.5.3 De modo geral, as placas de circuito impresso (PCI) são praticamente idênticas, sendo que o diferencial é apenas na tonalidade e uma marcação ou outra. Porém o layout é idêntico e os microcontroladores podem ter a marcação dos fabricantes PIC, ATMEL ou estarem raspados para dificultar a verificação visual. A maneira segura de descobrir se é falsa ou verdadeira é por intermédio de medições com o auxílio de um multímetro, conforme mostrado a seguir na figura A82.

Figura A82– Detalhes da PCI falsa.



Fonte: IPEM-SP

A-5.5.4 Pela figura A82, são destacados os pontos A B e C que serão medidos com o auxílio de um multímetro. Para o Ponto A, existe um fio na cor amarela normalmente conectado em conjunto com fio preto ao conector da CPU da BMC. Para a PCI falsa, a partir do ponto A existe uma trilha entre as camadas da PCI que se conecta aos pontos B e C.

A-5.5.5 Com o auxílio do multímetro ajustado para a função de teste de continuidade, conecta-se as pontas de prova entre os pontos A e B, ou entre os pontos A e C. Se for indicada continuidade entre estes pontos fica confirmada a presença da trilha adicional com objetivo de fraude.

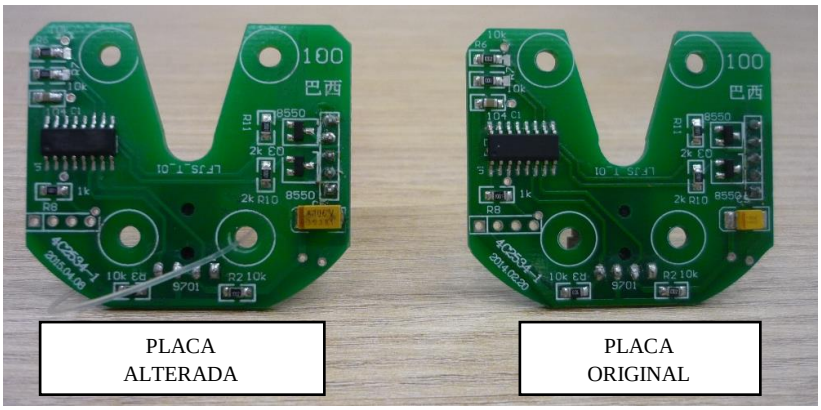
A-5.5.6 O efeito dessa fraude só é percebido quando a BMC for acionada em vazão intermediária. Para vazão alta ou baixa, o erro praticamente não existe, mesmo com o acionamento da fraude.

A-5.5.7 Neste deste tipo de fraude, o volume abastecido é menor do que o resultado da medição apresentado no *display* da bomba em questão. O erro percentual da medida é por volta de -10% à -15% para cada abastecimento.

A-5.6 Modelo 4 - *Pulser* Stratema Adulterado (troca do microcontrolador)

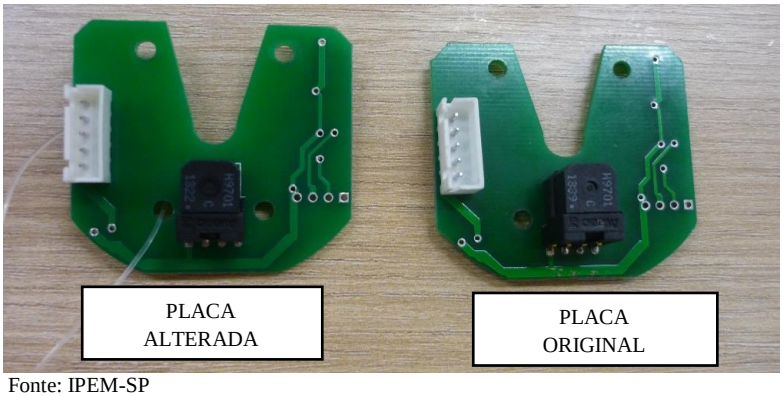
A-5.6.1 As figuras A83 e A84, a seguir, mostram o detalhamento e o comparativo das PCIs do p*ulser* Stratema adulterado com a original.

Figura A83 –Visão superficial do pulser original e alterado.



Fonte: IPEM-SP

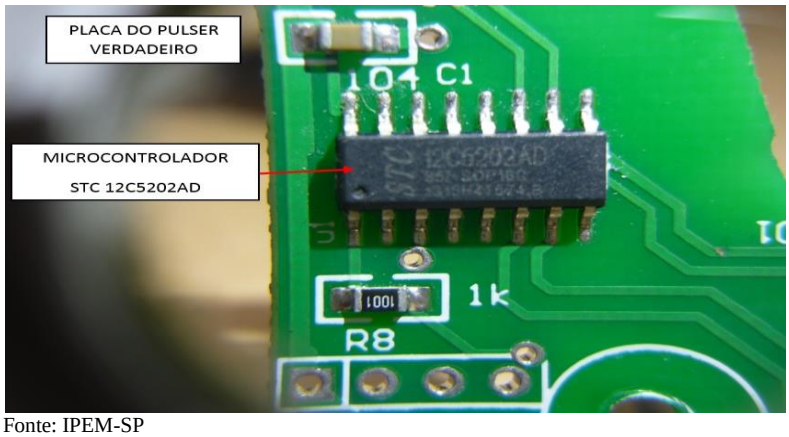
Figura A84 – PCI original e alterada.



Fonte: IPEM-SP

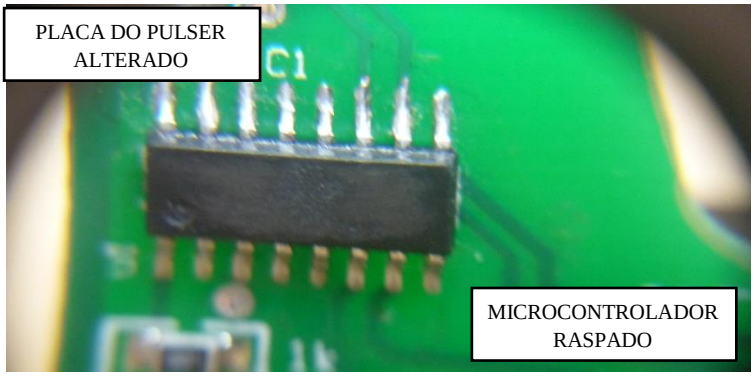
A-5.6.2 A única diferença reside no microcontrolador utilizado, conforme mostrado nas figuras A85 e A86. Observa-se que o microcontrolador utilizado na PCI fraudada está raspado para dificultar sua identificação.

Figura A85 – Detalhe do microcontrolador original de fábrica da PCI original.



Fonte: IPEM-SP

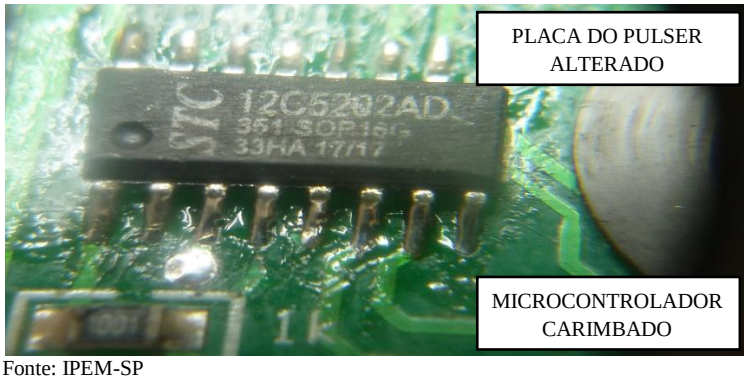
Figura A86 - Detalhe do microcontrolador adulterado (raspado) da placa original.



Fonte: IPEM-SP

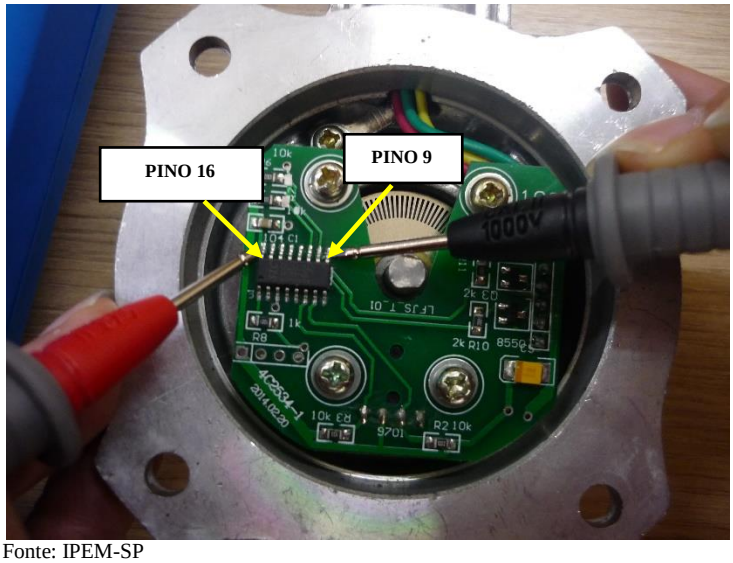
A-5.6.3 Em algumas implementações da fraude, após a raspagem também é aplicado um ‘carimbo’ sobre o componente para que se pareça com um componente original de fábrica (ver figura A87).

Figura A87 - Detalhe do microcontrolador adulterado (raspado e carimbado) da placa original.



Fonte: IPEM-SP

Figura A88 - Detalhe dos pinos a serem medidos.



Fonte: IPEM-SP

A-5.6.4 Para confirmação da existência da fraude no *pulser* é necessário o uso do multímetro, conforme mostrado na figura A88. As pontas de prova do multímetro são conectadas entre o pino 9 e 16 do microcontrolador para execução de um teste de continuidade. Se o teste for positivo fica confirmada a presença de fraude.

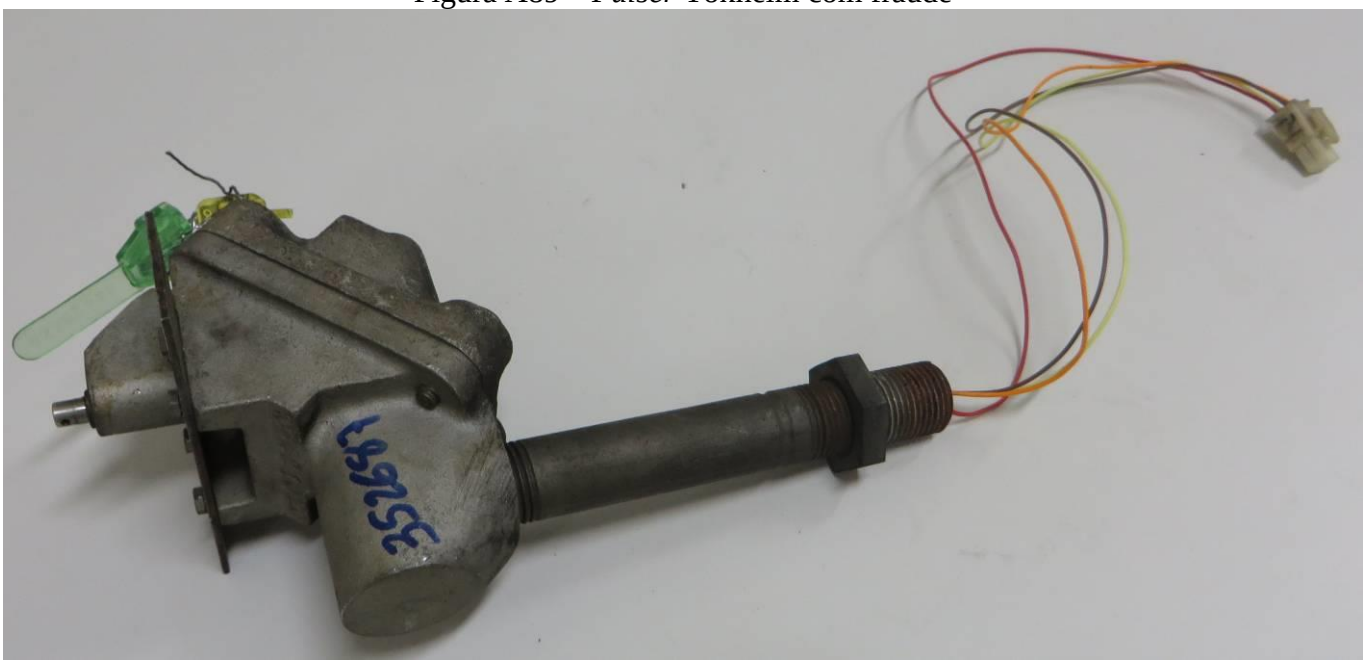
A-5.6.5 As sequências de ativação da fraude, podem ser feitas por sequência de liga e desliga, ou de liga e desliga e espera por um determinado tempo para ligar, ou ainda por mais de uma destas sequencias e mais a espera de determinado tempo para a ativação. Isso depende muito da programação que foi inserida no microcontrolador. Para desativar a fraude, basta desligar e ligar a bomba que o equipamento funcionará normalmente (sem erros).

A-5.6.6 Neste tipo de fraude, o volume abastecido é menor do que o resultado da medição apresentado no *display* da bomba em questão. O erro percentual da medida é por volta entre -6% a -12% para cada abastecimento.

A-5.7 Modelo 5 – *Pulser* Tokheim com Fraude no Fio

A-5.7.1 A figura A89 a seguir apresenta um *pulser* Tokheim onde é implementada uma fraude no cabo que conduz o sinal original do *pulser*. É necessário desmontar a tubulação metálica acoplada ao *pulser* para evidenciar uma parte do cabo que se encontra envolvida por material isolante (figura A90).

Figura A89 – *Pulser* Tokheim com fraude



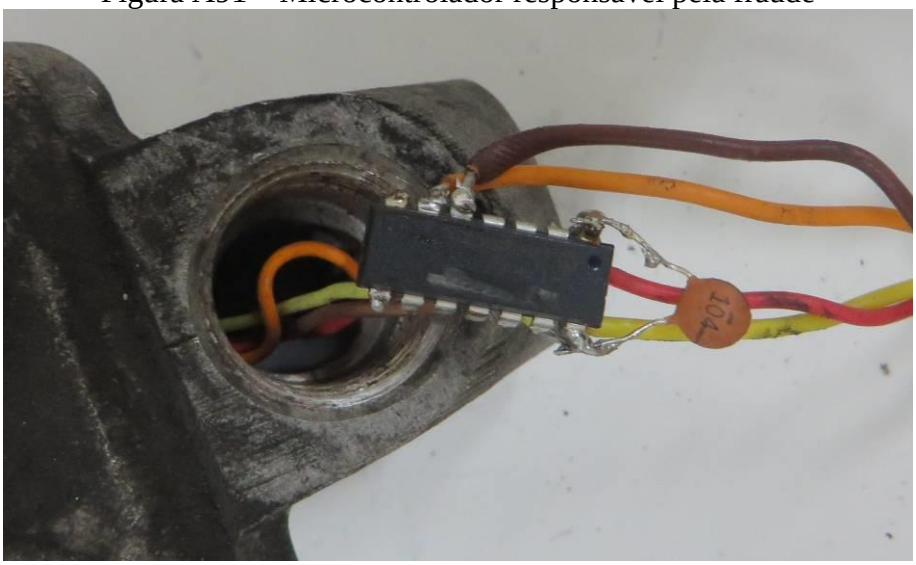
Fonte: Disme/Sinst

Figura A90 – Desmontando a tubulação metálica encontra-se parte da fiação envolvida em material isolante

Fonte: Disme/Sinst

A-5.7.2 Ao se retirar o isolante, evidencia-se o microcontrolador que efetua a fraude (figura A91).

Figura A91 – Microcontrolador responsável pela fraude

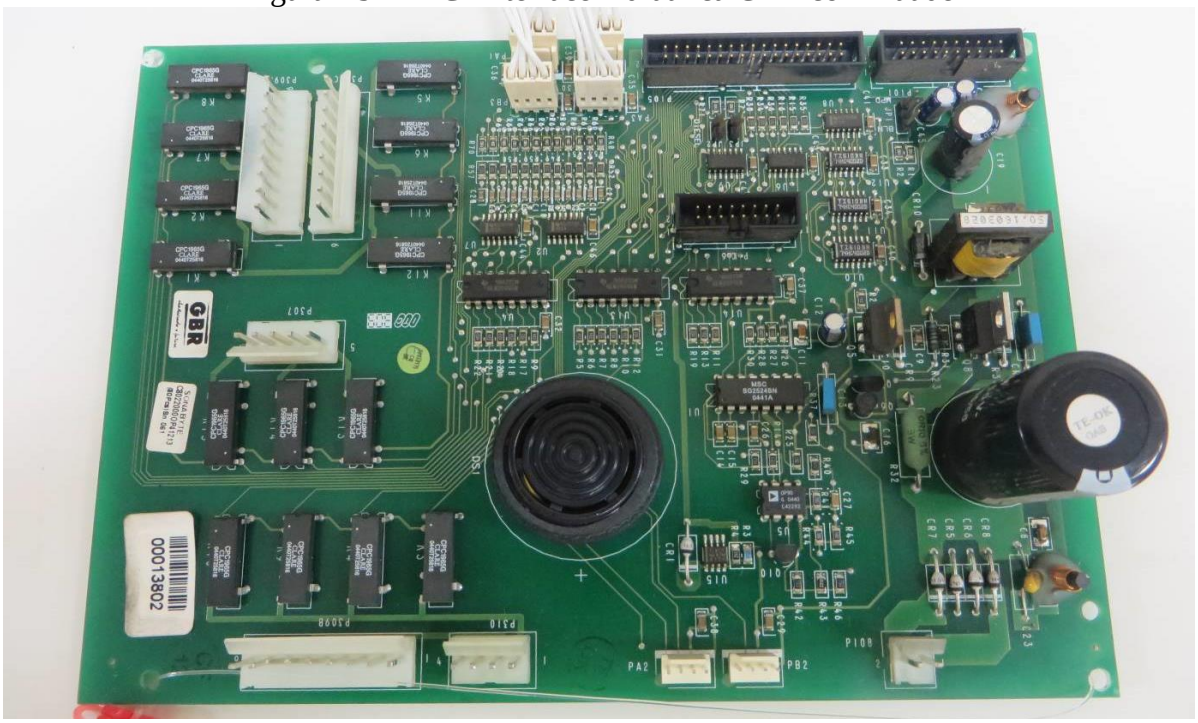


Fonte: Disme/Sinst

A-5.8 Modelo 6 – PCI de Interface Hidráulica com Fraude no Cabo de Comunicação do *Pulser* com a BMC, marca GBR modelo ENCORE/EVOLUTION

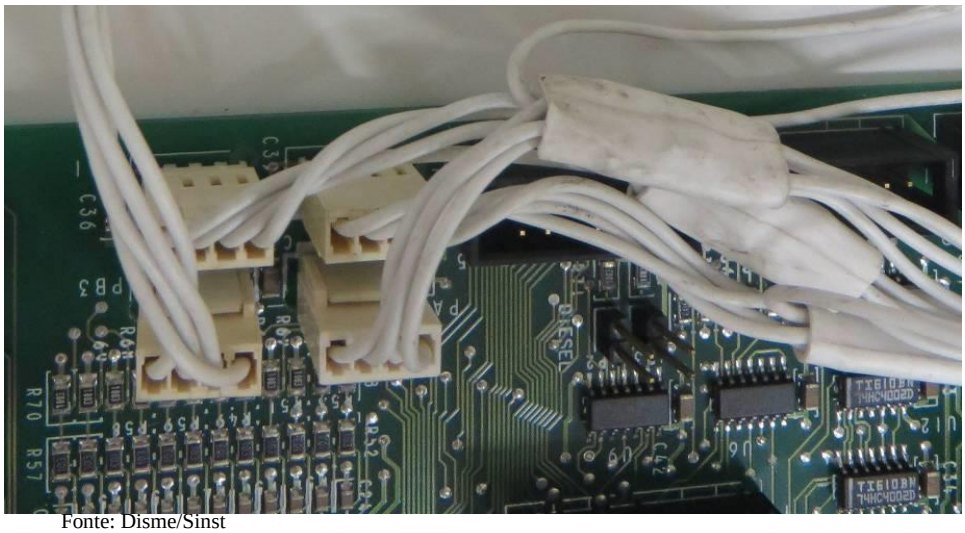
A-5.8.1 A figura A92 a seguir apresenta uma PCI original interface hidráulica marca GBR, modelo da bomba ENCORE/EVOLUTION, onde é implementada uma fraude no cabo que conduz o sinal do *pulser*.

Figura A92 – PCI interface hidráulica GBR com fraude



Fonte: Disme/Sinst

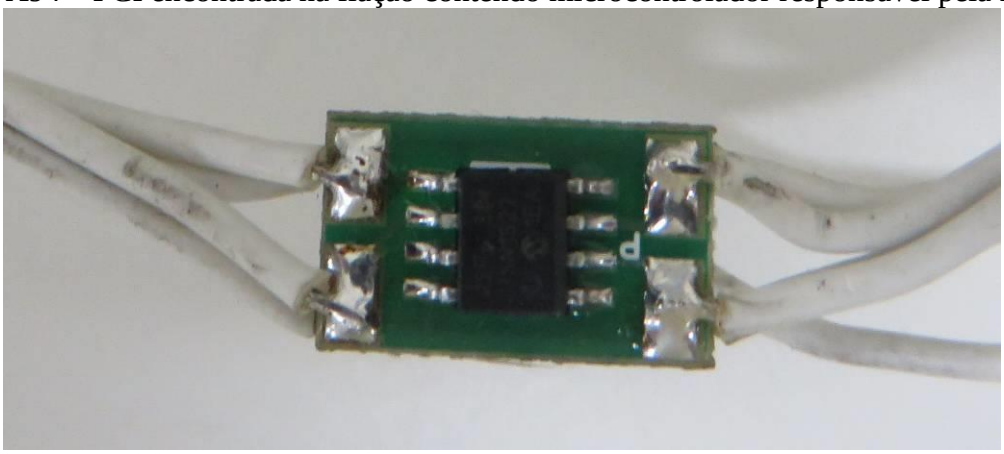
Figura A93 – Parte da fiação envolvida em material isolante.



Fonte: Disme/Sinst

A-5.8.2 Ao se retirar o isolante termo retrátil (figura A93), evidencia-se uma pequena placa contendo o microcontrolador que efetua a fraude (figura A94).

Figura A94 – PCI encontrada na fiação contendo microcontrolador responsável pela fraude.

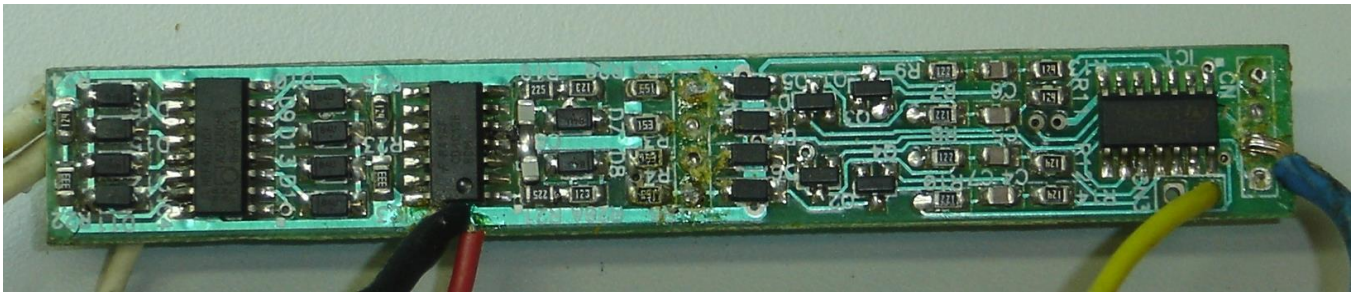


Fonte: Disme/Sinst

A-5.9 Modelo 7 – Placas Inseridas nos Cabos de Comunicação do *Pulser*

A-5.9.1 A figura A95 apresenta a placa encontrada nos cabos do *pulser*.

Figura A95 – PCI encontrada na fiação de *pulser* contendo componentes responsáveis por fraude.



Fonte: Disme/Sinst

A-5.9.2 Esta placa foi encontrada escondida dentro de tubulação metálica da bomba por onde passava a fiação. A tubulação apresentava massa epóxi em suas extremidades e a placa encontrava-se protegida por material isolante (figuras A96 e A97).

Figura A96 – Tubulação metálica onde a placa foi encontrada. As extremidades da tubulação encontravam-se protegidas com massa epóxi

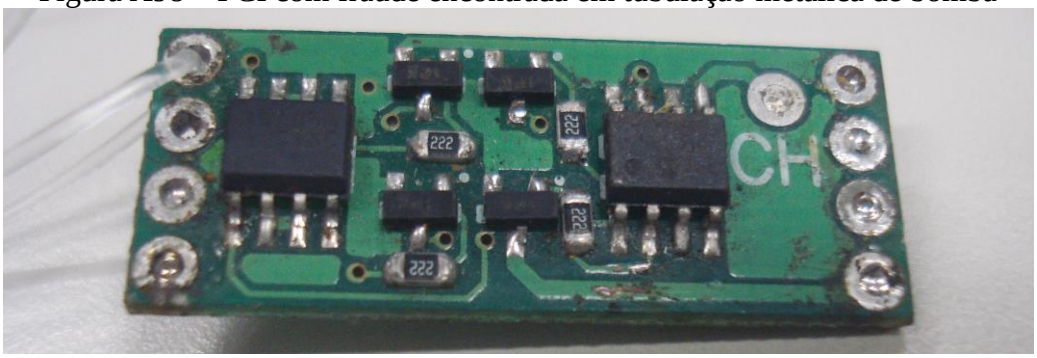
Fonte: Disme/Sinst

Figura A97 – PCI responsável pela fraude protegida com material isolante encontrada na tubulação metálica

Fonte: Disme/Sinst

A-5.9.3 Os tipos de placas encontradas nas tubulações metálicas das bombas podem variar. Na figura A98 é apresentado outro tipo de placa.

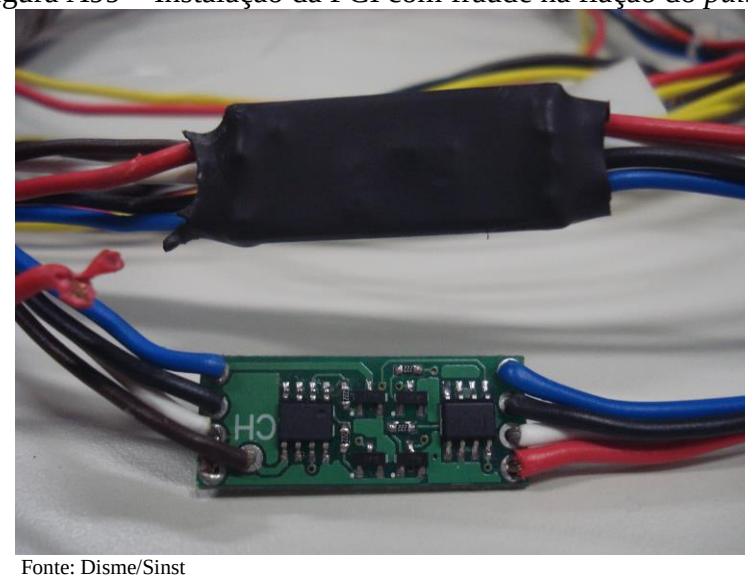
Figura A98 – PCI com fraude encontrada em tubulação metálica de bomba



Fonte: Disme/Sinst

A-5.9.4 A figura A99 mostra a forma como esta placa estava instalada na fiação do *pulser* da bomba.

Figura A99 – Instalação da PCI com fraude na fiação do *pulser*



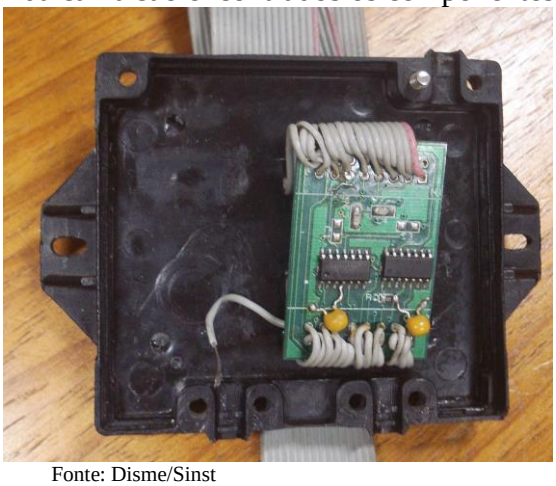
Fonte: Disme/Sinst

A-5.9.5 As figuras A100, A101 e A102 apresentam outra forma de inserção de placas fraudadas nos cabos de comunicação do *pulser*. Neste caso, as placas encontravam-se na fiação existente entre a placa de interface hidráulica e a CPU.

Figura A100 – Dispositivo inserido entre a placa de interface hidráulica e a CPU da bomba

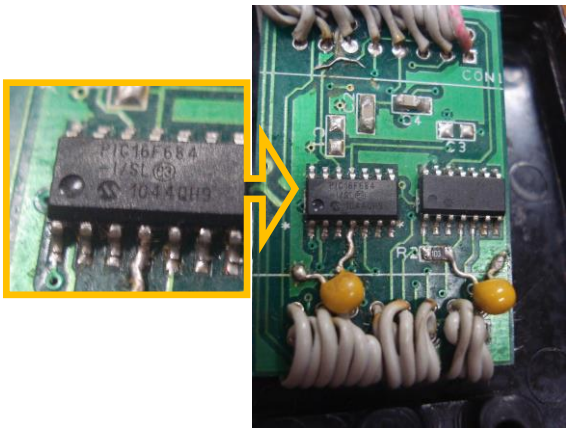
Fonte: Disme/Sinst

Figura A101 – No interior da caixa são encontrados os componentes responsáveis pela fraude



Fonte: Disme/Sinst

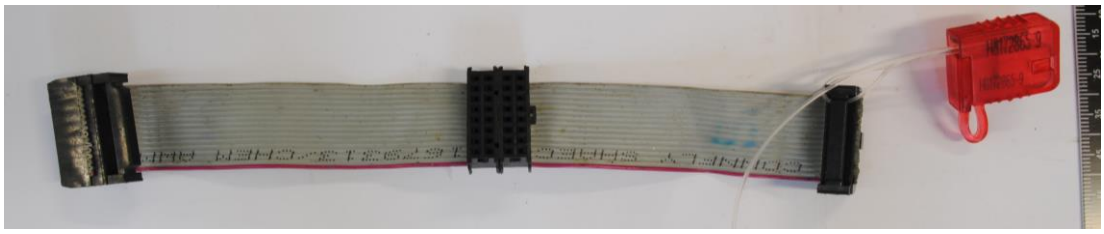
Figura A102 – Detalhe dos microcontroladores responsáveis pela fraude



Fonte: Disme/Sinst

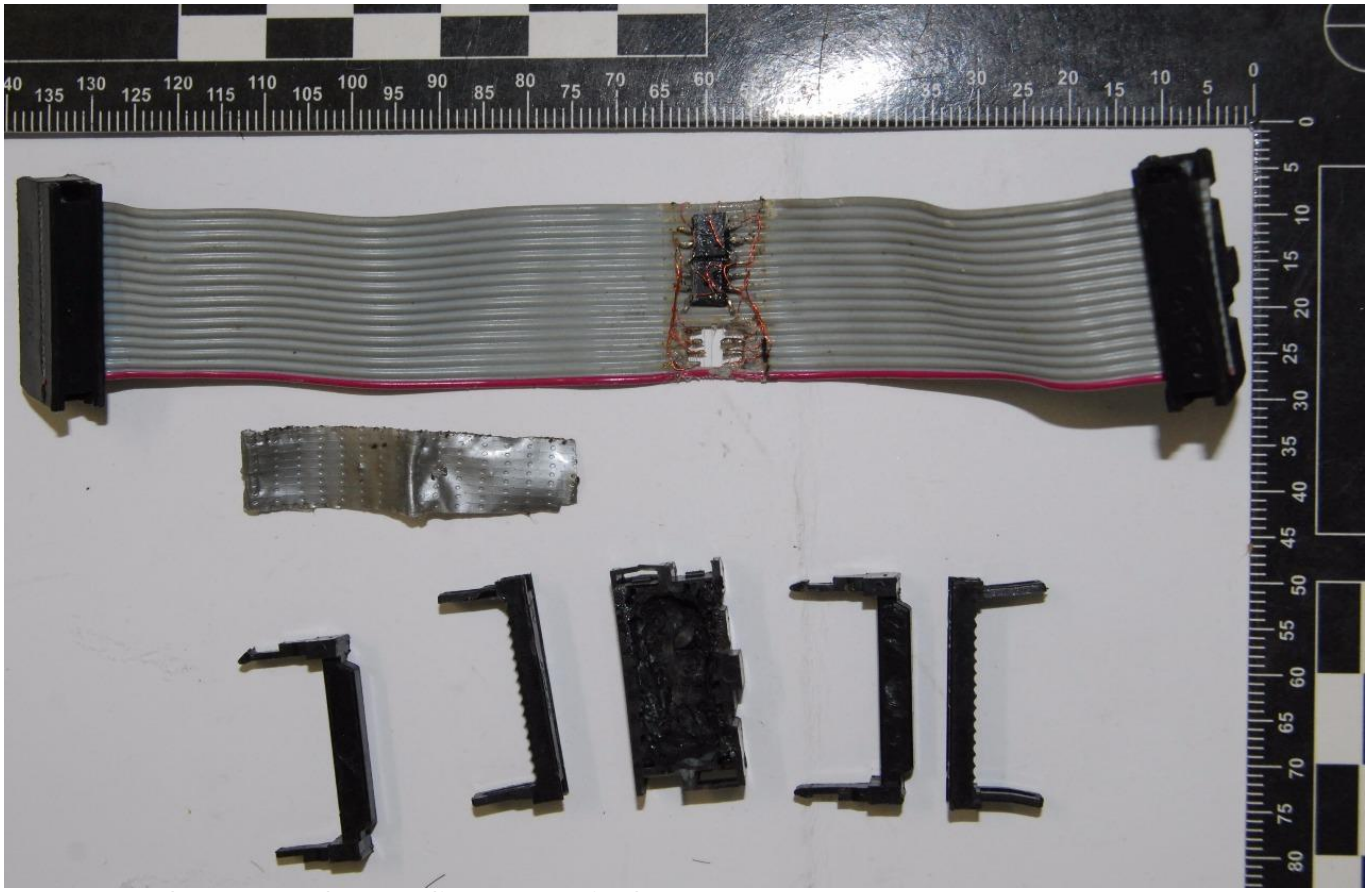
A-5.9.6 As figuras A103 e A104 a seguir demonstram uma variante da fraude anterior, onde no lugar da caixa para acomodar os componentes responsáveis pela fraude, optou-se por utilizar um par de conectores alinhados lado a lado no meio do cabo flat, simulando uma interligação a outra placa não utilizada. Os cabos originais desta bomba não possuem este conector. Seu acionamento se dá por uma sequência de cortes rápidos (da ordem de milissegundos) na alimentação elétrica da bomba. Já sua desativação acontece quando ocorre um desligamento da energia da bomba (falta de energia).

Figura A103 – Cabo de conexão entre CPU e interface hidráulica, com inserção de conector para esconder a fraude.



Fonte: Superintendência de Policia Técnico-Científica – Seção de Informática Forense - GO

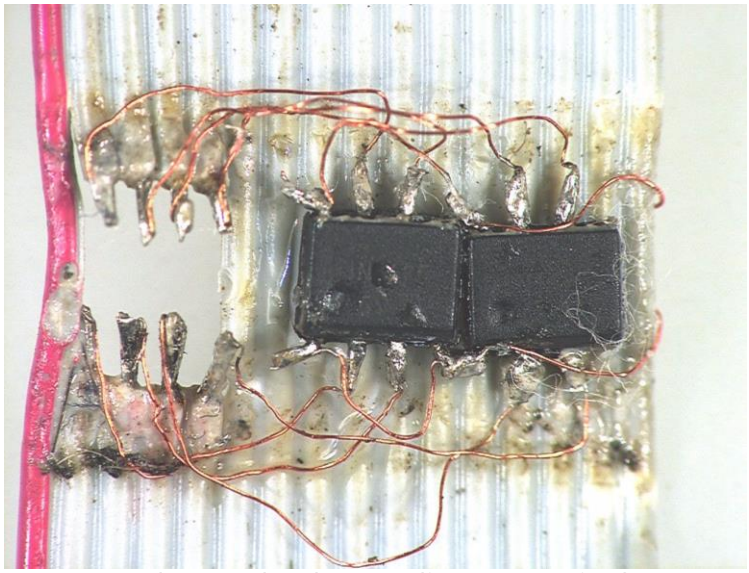
Figura A104 – Cabo de conexão entre CPU e interface hidráulica, microcontroladores escondidos.



Fonte: Superintendência de Policia Técnico-Científica – Seção de Informática Forense GO

A-5.9.7 A figura A105 mostra detalhes da ligação dos microcontroladores, utilizados na fraude, ao cabo flat.

Figura A105– Detalhes da ligação dos microcontroladores ao cabo flat.



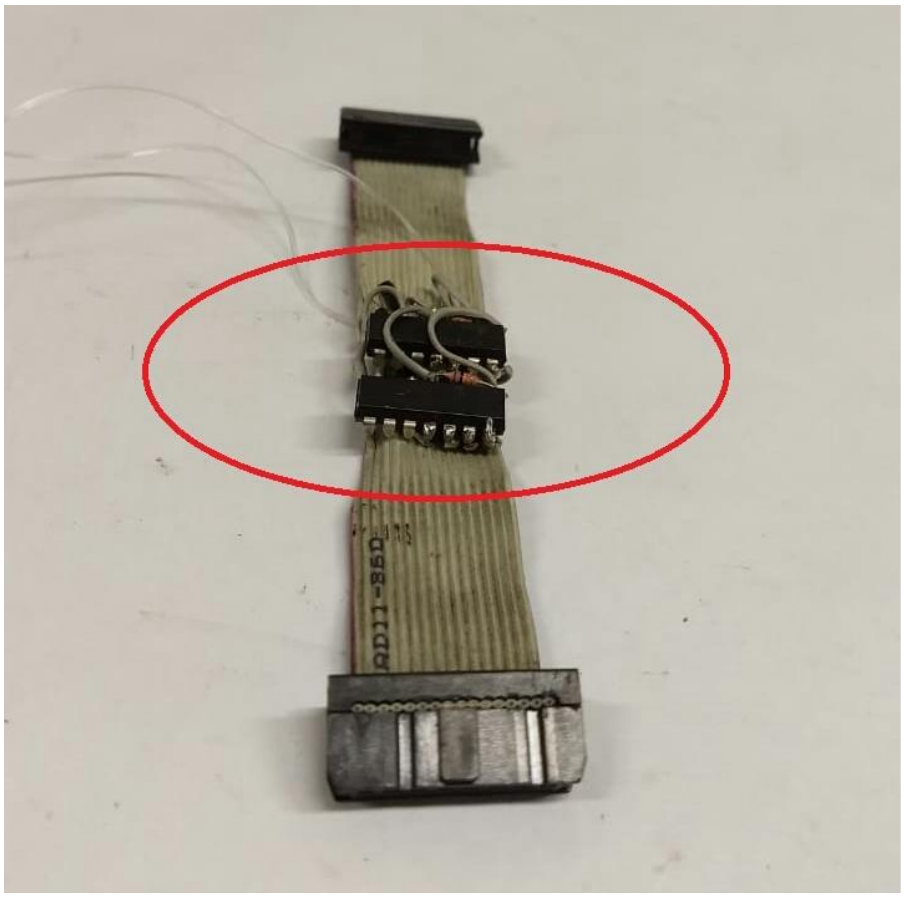
Fonte: Superintendência de Polícia Técnico-Científica – Seção de Informática Forense GO

A-5.9.7 As figuras A106 e A107 mostram uma outra forma de fraude com inserção de microncontrolador(es) no cabo flat.

Figura A106 – Detalhe do material termo retrátil usado para esconder o microcontrolador no cabo flat

Fonte: Disme/Sinst

Figura A107 – Detalhe do microcontrolador embutido no cabo flat

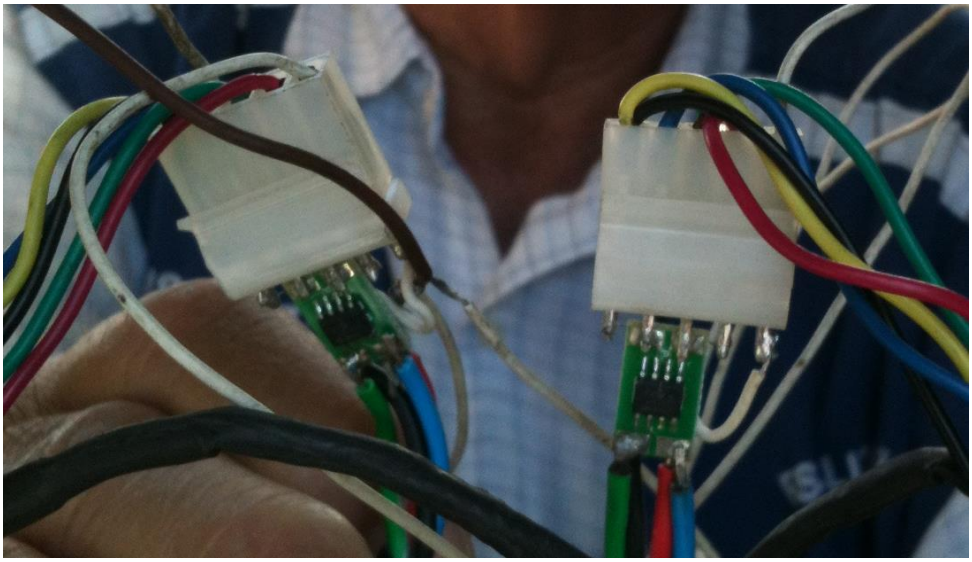


Fonte: Disme/Sinst

A-5.10 Modelo 8 – Placas Inseridas nos Cabos de Comunicação do *Pulser*

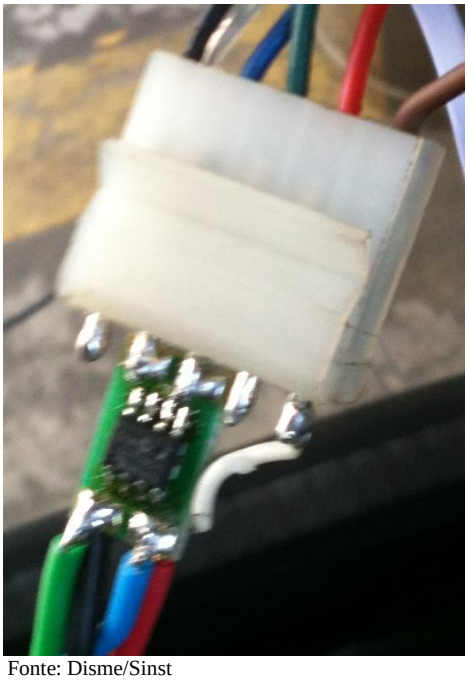
A-5.10.1 As figuras A108 e A109 apresentam as placas eletrônicas encontradas nos cabos de comunicação do *pulser*.

Figura A108 – Placas com microcontroladores que implementam fraude no cabo de comunicação



Fonte: Disme/Sinst

Figura A109 – Detalhe da placa com microcontrolador responsável pela fraude



Fonte: Disme/Sinst

A-6 FRAUDES EM PLACAS CONTROLADORAS DE *PULSER* (modelos 1 e 2)

A-6.1 Modelo 1 – Fraude em placa controladora de *pulser* inserida em placa de interface hidráulica

A-6.1.1 A tabela 13 a seguir apresenta as características dessa fraude.

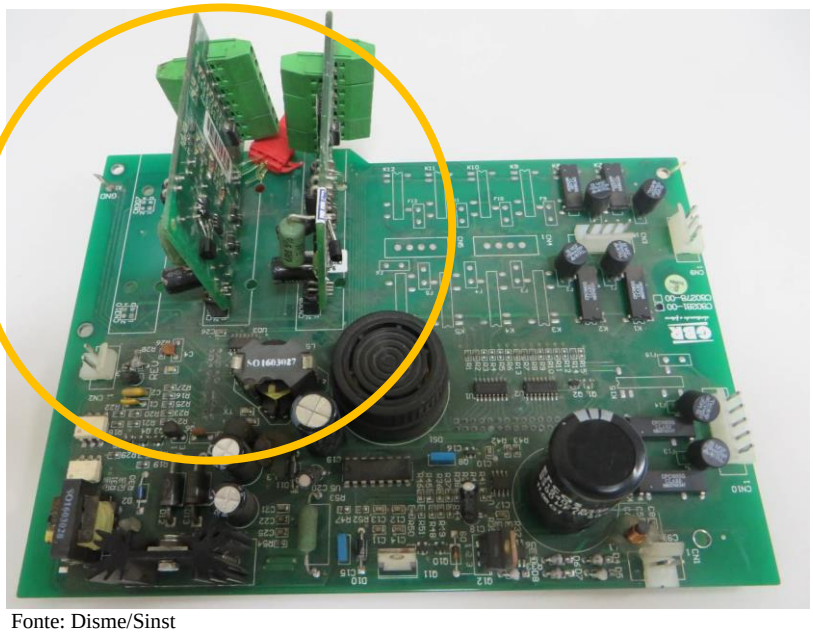
Tabela 13 – Características da fraude apresentada nas figuras A110 e A111

Componentes da fraude	PCI controladora de *pulser* original Microcontroladores Regulador de tensão Receptor comercial de RF Contator (contactora)
Operação	O microcontrolador incrementa a quantidade de pulsos originais gerados em um abastecimento.
Forma de acionamento/inibição	Uma sequência de comandos liga/desliga, normalmente enviados por controle remoto. O microcontrolador é programado para identificar uma sequência específica de interrupções da energia da bomba (sequência liga/desliga). Quando a sequência correta é detectada, a fraude é ativada. A inibição da fraude é feita pela interrupção do fornecimento de energia da bomba. Quando a bomba for novamente energizada a fraude estará desativada. Por este motivo recomenda-se realizar os ensaios metrológicos imediatamente ao chegar ao posto e não permitir o desligamento das bombas. O sistema de ativação da fraude inclui ainda um receptor comercial de RF e um contator (contactora) conectado ao circuito de alimentação da bomba, os quais implementam a sequência liga/desliga de acionamento da fraude.
Efeito	O resultado apresentado no *display* da bomba é maior do que o volume abastecido. O erro percentual da medida é fixo em -3,5% para cada abastecimento.

Fonte: Disme/Sinst

A-6.1.2 A figura A110 a seguir, apresenta uma placa interface hidráulica onde são acopladas as placas controladoras de *pulser*.

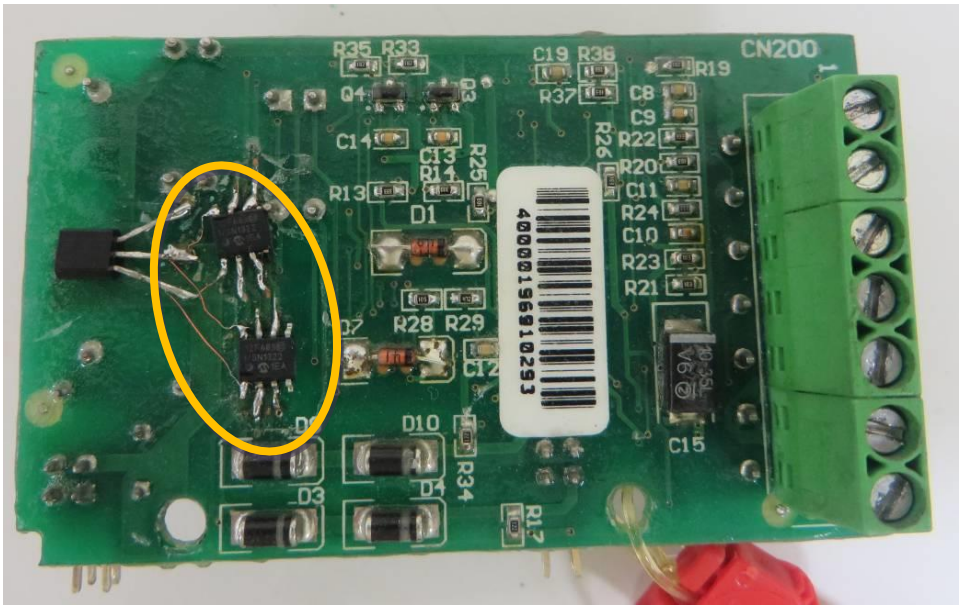
Figura A110 – PCI interface hidráulica com placas controladoras de *pulser* acopladas (em destaque)



Fonte: Disme/Sinst

A-6.1.3 A fraude é evidenciada na placa controladora de *pulser* com a inserção dos microcontroladores responsáveis pela fraude. O regulador de tensão encontra-se presente apenas para estabilização da tensão de alimentação dos microcontroladores (figura A111).

Figura A111 – Placa controladora de pulsos com fraude. Em destaque: microcontroladores responsáveis pela fraude.



Fonte: Disme/Sinst

A-6.2 Modelo 2 – Placa controladora de *pulser* falsa com componentes adicionais

A-6.2.1 A tabela 14 a seguir apresenta as características dessa fraude.

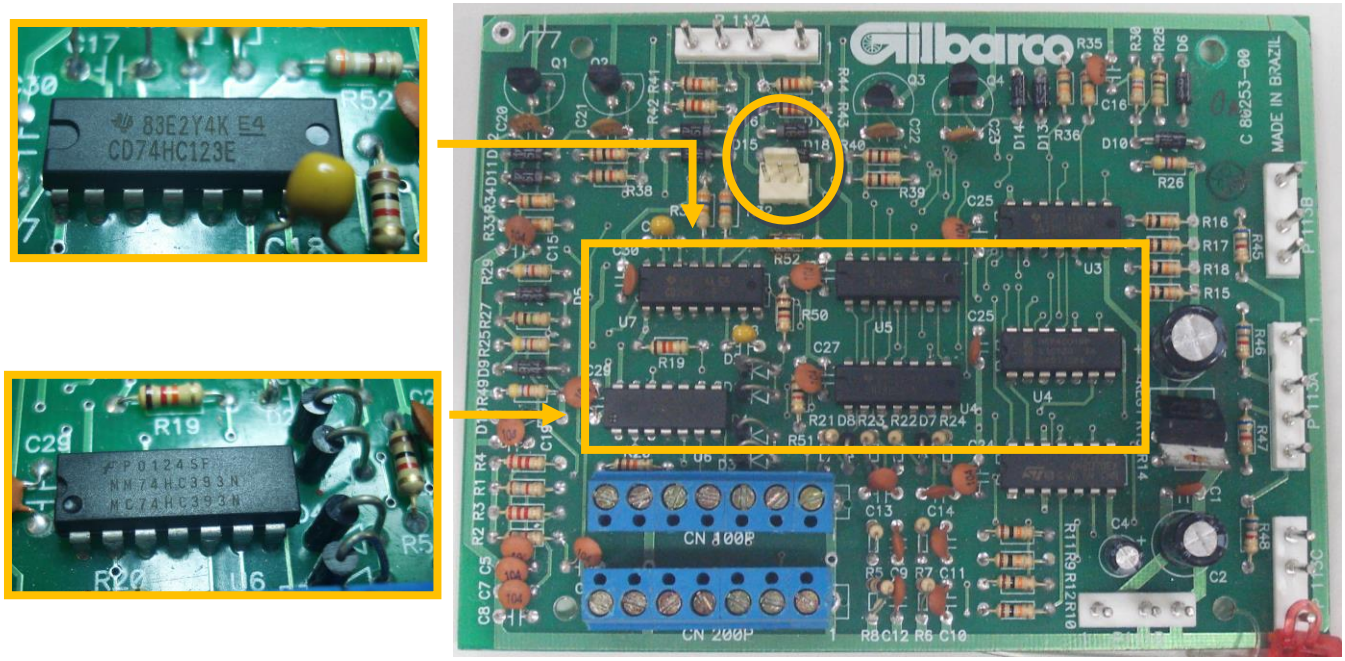
Tabela 14 – Características da fraude apresentada na figura A112

Componentes da fraude	Placa controladora de *pulser* falsa
Operação	Os componentes em destaque na Figura A112 formam o circuito responsável pelo incremento da quantidade de pulsos gerados em um abastecimento.
Forma de acionamento/inibição	Aplicação de uma tensão de 12V a um conector específico da placa (em destaque na figura A112). Quando a tensão é retirada, a fraude é inibida. Até o momento não é conhecida a forma de acionamento externo. Este acionamento/inibição poderia se dar através de controle remoto, de forma semelhante aos casos anteriores, ou através de um interruptor instalado no instrumento.
Efeito	O resultado apresentado no *display* da bomba é maior o que o volume abastecido. O erro percentual da medida é fixo em 8,3% para cada abastecimento.

Fonte: Disme/Sinst

A-6.2.2 A PCI apresentada a seguir (figura A112) constitui uma fraude semelhante à que foi apresentada no subitem A-2.2.

Figura A112 – Placa controladora de pulsos falsa que implementa fraude. Em destaque: conector utilizado para acionamento da fraude; componentes responsáveis pela fraude.



Fonte: Disme/Sinst

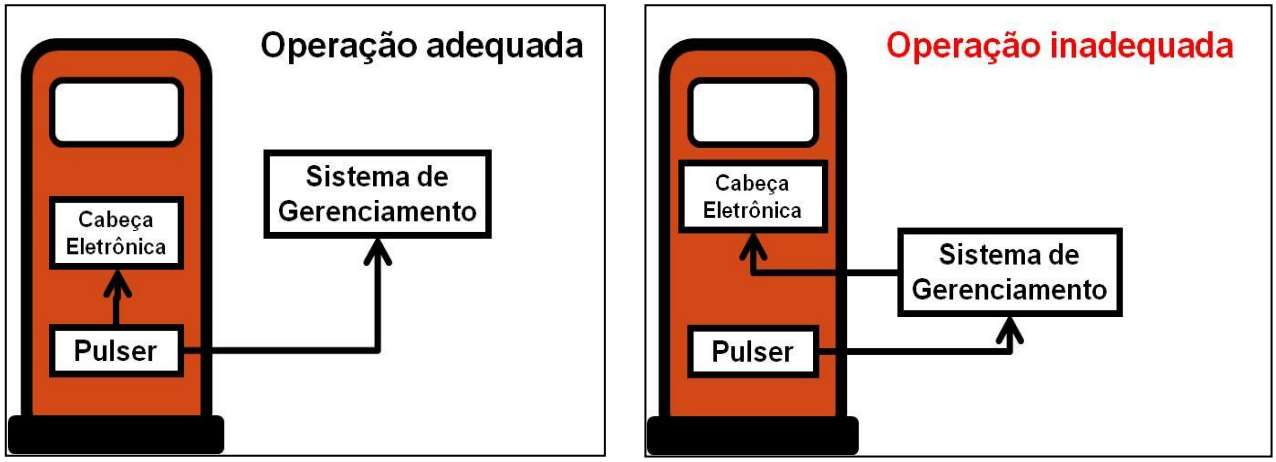
A-7 FRAUDES UTILIZANDO SISTEMAS DE GERENCIAMENTO E OUTRAS

A-7.1 Fraude em Sistema de Gerenciamento da Carddy

A-7.1.1 A fraude apresentada a seguir é implementada em um sistema de gerenciamento da marca Carddy, modelo BESS-01. O sistema de gerenciamento teve aprovação do Inmetro através da Portaria Inmetro/Dimel nº 133/2007 e as características do equipamento apreendido permitem a operação de modo fraudulento. Atualmente, a Portaria Inmetro/Dimel nº 133/2007 encontra-se revogada.

A-7.1.2 Para a finalidade de gerenciar a venda de combustíveis, o sistema da Carddy toma a informação de fornecimento de combustível diretamente do *pulser*. Em seu uso fraudulento, o sistema é modificado de tal forma que o sinal do *pulser* é interrompido e conduzido para o sistema de gerenciamento. O sinal do *pulser*, adulterado no sistema de gerenciamento, é devolvido à bomba para processamento da quantidade de combustível fornecido pela mesma (Figura A113 b). Como consequência, a bomba irá indicar uma quantidade de combustível maior do que aquela que foi efetivamente abastecida.

Figura A113 – Diagrama de conexão de sistema de gerenciamento: (a) o sinal do *pulser* não sofre intervenção e é apenas utilizado para captar informações sobre os abastecimentos; (b) o sinal do *pulser* sofre modificação no sistema de gerenciamento e é conduzido de volta à bomba para processamento da medição adulterada.



(a) **(b)**

Fonte: Disme/Sinst

A-7.1.3 A tabela 15 a seguir apresenta as características dessa fraude.

Tabela 15 – Características da fraude apresentada nas figuras A114 a A124

Componentes da fraude	Adulteração da conexão direta do *pulser* (figura A114) Sistema de gerenciamento Carddy fraudulento e seus diversos componentes (Figuras A115 a A124)
Operação	A placa apresentada na figura A123 faz parte da fraude e é encontrada na caixa do sistema fraudado (figura A119). Esta placa contém um microcontrolador que é o responsável pelo incremento da quantidade de pulsos gerados em um abastecimento.
Forma de acionamento/inibição	São quatro as formas possíveis: 1) Através do módulo com GSM (figura A124), por meio de ligação de telefone celular, que aciona o transmissor de radiocontrole. Pode ser feito acionamento ou inibição da fraude. 2) Através de controle remoto. Pode ser feito acionamento ou inibição da fraude. 3) A fraude pode ser inibida através da interrupção da energia do sistema de gerenciamento. Quando o sistema é novamente energizado, a bomba apresenta comportamento metrológico normal. 4) Botão de emergência presente na caixa do sistema fraudado (Figura A118). Ele é utilizado apenas para inibir a fraude, com envio de sinal de radiocontrole.
Efeito	O resultado apresentado no *display* da bomba é maior do que o volume abastecido. O erro percentual da medida é fixo em -10% para cada abastecimento.

Fonte: Disme/Sinst

A-7.1.4 Em geral, o sistema de gerenciamento instalado em postos de combustíveis é encontrado distante das bombas. O mesmo se dá com o sistema fraudado a placa da bomba. Mesmo assim, na própria bomba é possível identificar se há a presença de um sistema de gerenciamento deste tipo observando-se a conexão do *pulser* com a placa CPU, barreira intrínseca ou interface hidráulica, de acordo com cada projeto de BMC.

A-7.1.5 A figura A114 apresenta uma conexão normal. O *pulser* é conectado diretamente à placa da bomba. Neste caso, não há indicação da presença de um sistema de gerenciamento como aqui descrito.

Figura A114 – Conexão direta de *pulser* à placa da bomba

Fonte: Disme/Sinst

A-7.1.6 Uma conexão semelhante à apresentada na figura A115 é representativa de uma operação inadequada conforme indicado na figura A113(b) e, portanto, é uma indicação da presença de um sistema de gerenciamento que deve ser inspecionado.

Figura A115 – Conexão utilizada no sistema de gerenciamento Carddy com fraude. O *pulser* não é conectado diretamente à placa. Em destaque: parte da fiação que segue para o sistema de gerenciamento

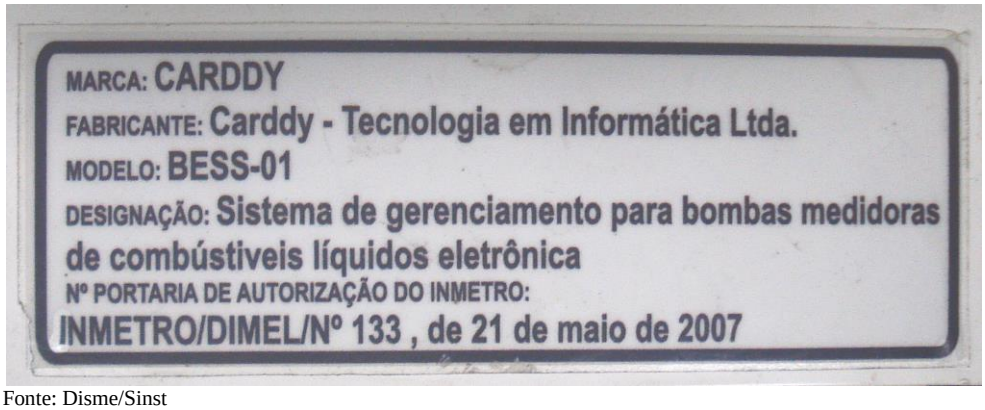
Fonte: Disme/Sinst

A-7.1.7 Uma vez que seja identificada conexão no *pulser* semelhante à Figura A115, o sistema de gerenciamento deve ser localizado e verificado. Nas figuras a seguir (A116 a A124) são apresentadas imagens que permitem a identificação do sistema de gerenciamento fraudado e seus componentes.

Figura A116 – Caixa do sistema de gerenciamento Carddy com fraude.
Observação: a forma e o tipo da caixa podem ser diferentes.

Fonte: Disme/Sinst

Figura A117 – Etiqueta de identificação do sistema de gerenciamento

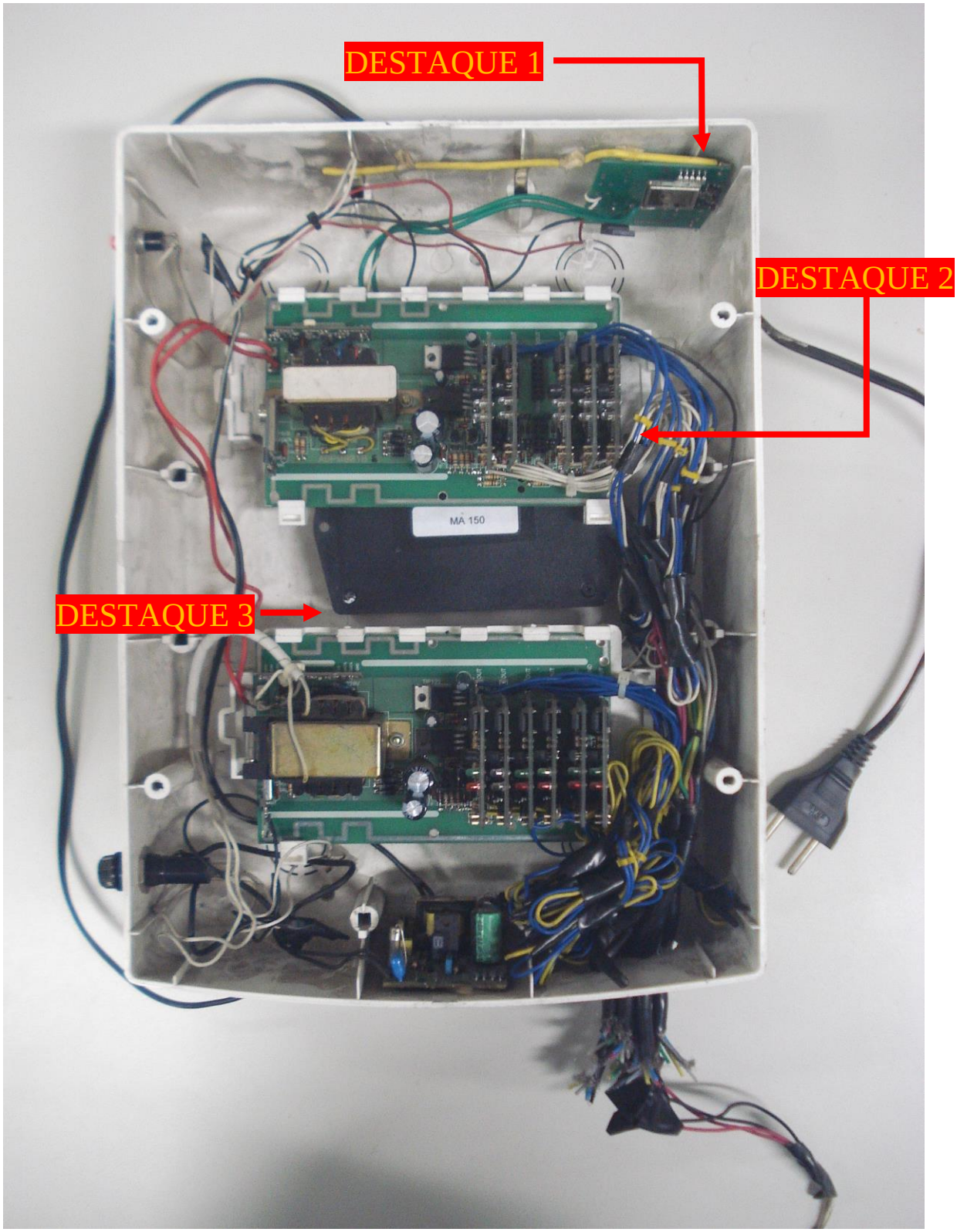


Fonte: Disme/Sinst

Figura A118 – Botão externo de emergência para desativação da fraude

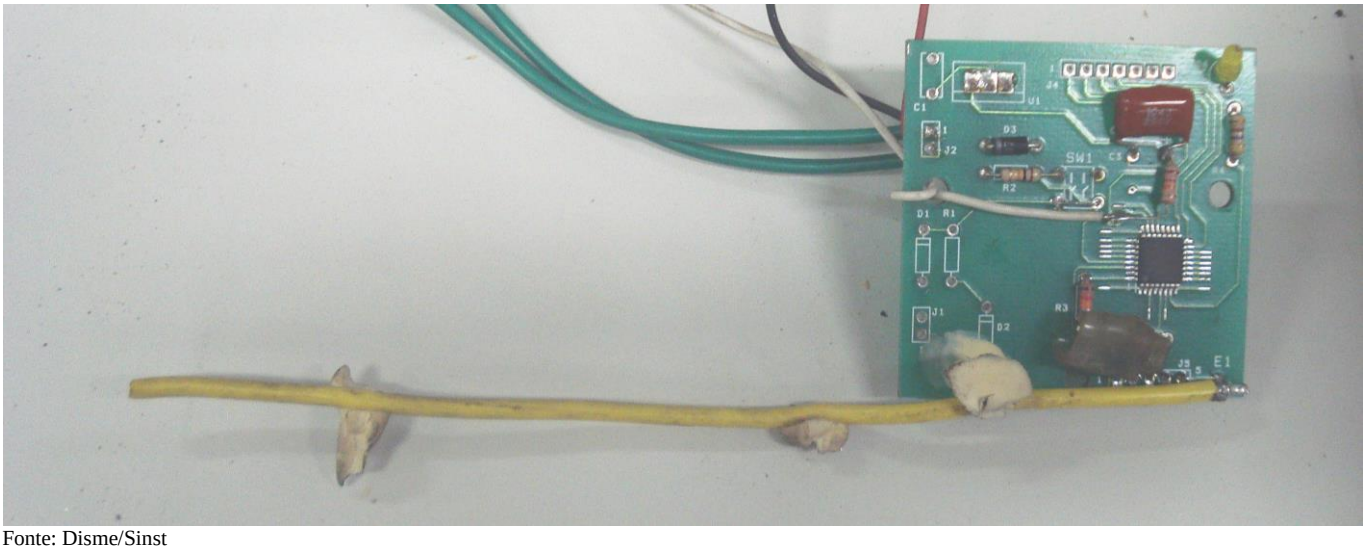
Fonte: Disme/Sinst

Figura A119 – Visão geral dos componentes integrantes do sistema de gerenciamento fraudado.



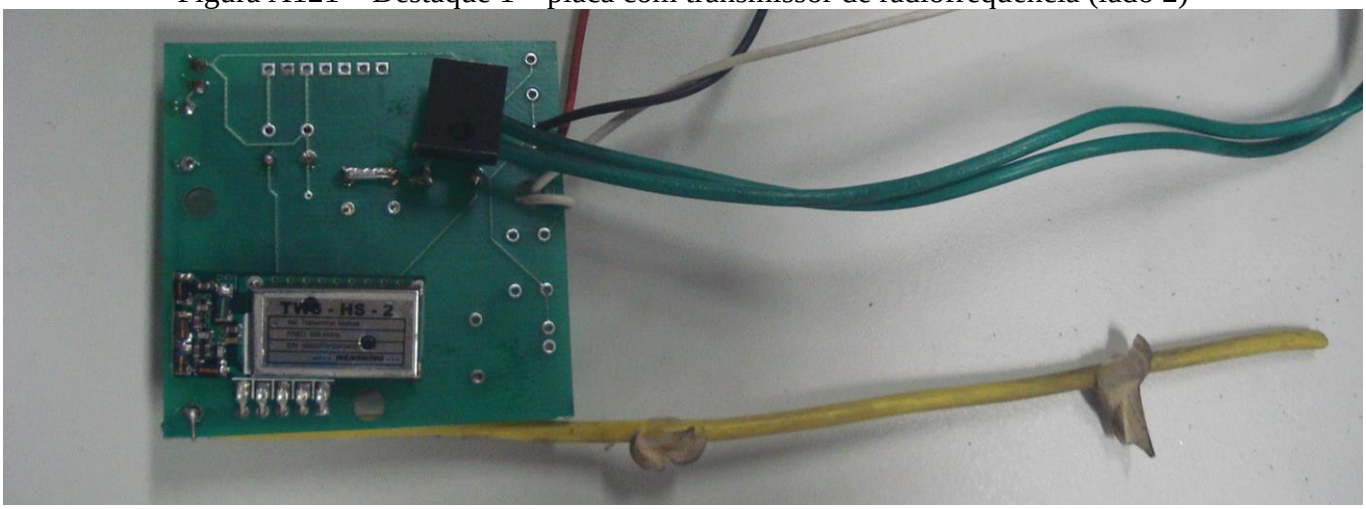
Fonte: Disme/Sinst

Figura A120 – Destaque 1 – placa com transmissor de radiofrequência (lado 1)



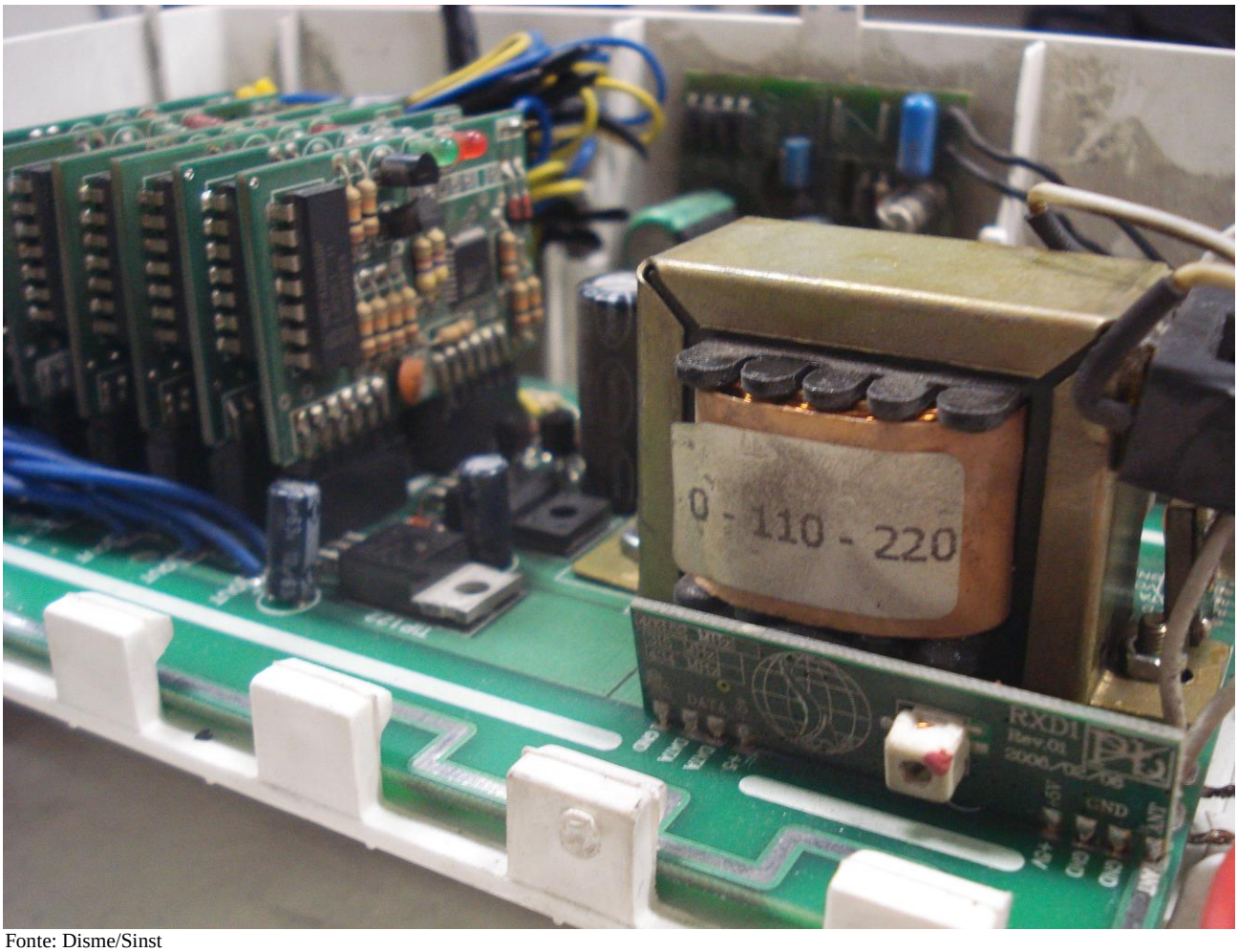
Fonte: Disme/Sinst

Figura A121 – Destaque 1 – placa com transmissor de radiofrequência (lado 2)



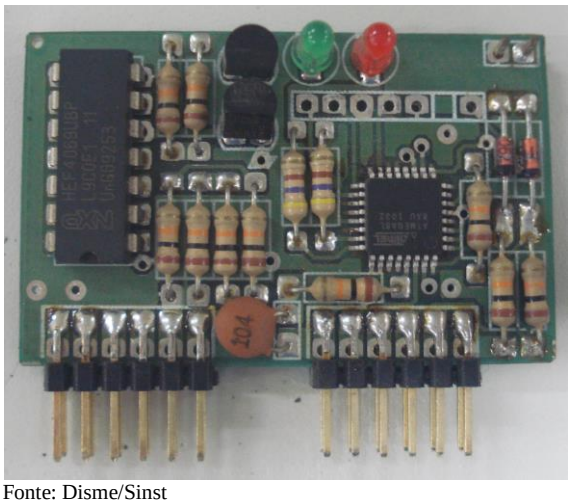
Fonte: Disme/Sinst

Figura A122 – Destaque 2 – placa receptora de radiofrequência com módulos de adulteração de medição de combustível encaixados



Fonte: Disme/Sinst

Figura A123 – Destaque 2 – módulo de adulteração de medição de combustível. Cada módulo efetua a fraude em um bico de abastecimento.



Fonte: Disme/Sinst

Figura A124 – Destaque 3 – módulo com GSM e seus componentes internos. Este módulo é utilizado para acionamento/desativação da fraude através de uma chamada telefônica de celular.

Fonte: Disme/Sinst

A-7.2 Fraude utilizando placa falsa instalada entre a CPU e a Interface Hidráulica

A-7.2.1 Nessa fraude foi instalada uma placa falsa que não existe em nenhuma BMC. Essa placa falsa (figura A125) foi usada com uma conexão entre a placa de Interface Hidráulica e a CPU.

Figura A125 – Placa falsa encontrada em uma Bomba Gilbarco PRO 2 e GBR 111

Fonte:IPEM-SP

A-7.2.2 O acionamento da fraude é feito por controle remoto.