



Analizador de Fraudes Eletrônicas e Verificador Metrológico Integrado para detecção de fraudes em medidores de energia elétrica

Tema: Recuperação de energia - Perdas não-técnicas

Autores: Ebersson Ricardo Patalo, Elayne Holanda Madruga, Flavio Luiz de Oliveira e Silva, Manoel Messias Vieira de Menezes Junior, Ricardo Ary Rufato Zaia, José Calazans Alves, Eduardo Gabriel Carvalho Marinho, Leandro Henrique Melo de Carvalho, Carlos Humberto Cardoso Rezende, Daniel Pereira de Carvalho, Carlos Augusto Bissochi Junior, José Rubens Macedo Junior

Co-Autores:

Empresa: Energisa Paraíba - Distribuidora de Energia S/A

Resumo

Este trabalho apresenta uma nova metodologia para identificação de fraudes eletrônicas em medidores de energia, através de um protótipo de equipamento desenvolvido pelo Grupo Energisa, em parceria com a Universidade Federal de Uberlândia e a MINIPA. Chamado de Analisador de Fraudes Eletrônicas e Verificador Metrológico Integrado (AFEVMI), o equipamento é compatível com todos os modelos de medidores e verifica tanto o erro metrológico quanto as fraudes eletrônicas, permanentes ou dinâmicas. Fraudes permanentes são identificadas através da função de verificação metrológica, em que se compara o medidor com um padrão metrológico calibrado, avaliando a precisão e integridade da medição. Fraudes dinâmicas, por sua vez, são detectadas pela análise das características elétricas do medidor. A instalação de circuitos externos altera essas características originais, permitindo identificar discrepâncias entre um medidor padrão e um fraudado. A metodologia foi testada em laboratório e em campo, apresentando uma assertividade de 100% na detecção de medidores fraudados. Com o desenvolvimento de um único equipamento com as funcionalidades de analisador de fraudes eletrônicas e verificador metrológico integrado, pretende-se aumentar a produtividade e assertividade dos eletricitistas na detecção de fraudes em medidores de energia.

1. Introdução

A deterioração das condições socioeconômicas do país tem ocasionado o aumento das perdas não técnicas de energia, concomitantemente com o aumento do nível de inadimplência. As perdas não técnicas, apuradas pela diferença entre as perdas totais e as perdas técnicas, têm origem principalmente nos furtos de energia (ligação clandestina, desvio direto da rede, adulterações de componentes eletrônicos do medidor, adulteração do mecanismo do medidor eletromecânico) e nas perdas administrativas (erros de leitura, erro no cadastro de consumidores, constante de faturamento e iluminação pública).

Diversos trabalhos foram desenvolvidos com o objetivo de reduzir o montante de perdas não técnicas das distribuidoras de energia elétrica. O trabalho desenvolvido por Foiatto (2009) propõe uma sistematização para o reconhecimento de irregularidades que caracterizam fraudes em medidores. Ela é baseada em um banco de dados hierarquicamente padronizado e em informações de verificação metrológicas para garantir a confiabilidade dos resultados. Martins (2018) apresentou um dispositivo, fruto de um projeto de

P&D ANEEL, com o objetivo de detectar desvios no padrão de entrada de unidades consumidoras. Este dispositivo utiliza um conjunto de sensores para realizar a detecção dos campos elétricos e magnéticos gerados pelos desvios. No trabalho desenvolvido em Amhenrior *et al.* (2017) foi construído um medidor de energia com detecção e reporte automático de fraude. O medidor desenvolvido é dividido em duas partes: a primeira é o medidor de energia propriamente dito, enquanto a segunda é composta por um sensor chamado transformador de corrente “sem fios”. O princípio de operação deste dispositivo é comparar a corrente medida pelo medidor com a corrente do transformador de corrente sem fios. Caso o valor de corrente seja divergente, a distribuidora pode ser comunicada por meio de uma rede de comunicação sem fios. O trabalho desenvolvido por Patil *et al.* (2017), por sua vez, apresenta um medidor capaz de detectar automaticamente circuitos de desvio no padrão de entrada das unidades consumidoras. O princípio de operação desse medidor consiste em se desconectar automaticamente a carga do medidor e verificar a presença da corrente de retorno. Caso exista a detecção da fraude, a distribuidora é comunicada por meio de SMS ou outra rede de comunicação.

Além de dispositivos para detecção das fraudes, pode ser encontrada uma ampla bibliografia com diferentes metodologias que utilizam o padrão de consumo da unidade consumidora para identificação de fraudes. Apesar da vasta literatura sobre o tema de fraudes de energia, pouco se foi encontrado referente ao desenvolvimento de soluções para detecção de fraudes eletrônicas dinâmicas, que podem estar ligadas ou desligadas de forma intermitente, normalmente acionadas por circuitos eletrônicos por controle remoto do usuário beneficiário da fraude, que é um dos principais focos desse trabalho.

Tradicionalmente, as fraudes em medidores de energia elétrica consistem em danificar o medidor ou alterar os circuitos responsáveis pela medição da tensão ou da corrente. Alguns exemplos são injeção de corrente contínua para danificar as bobinas de medição, substituição de componentes para alterar valor da tensão medida, *by-pass* do transdutor de corrente, entre outros. A Figura 1 ilustra exemplos de medidores com fraudes nos circuitos de medição dos canais de corrente e tensão.

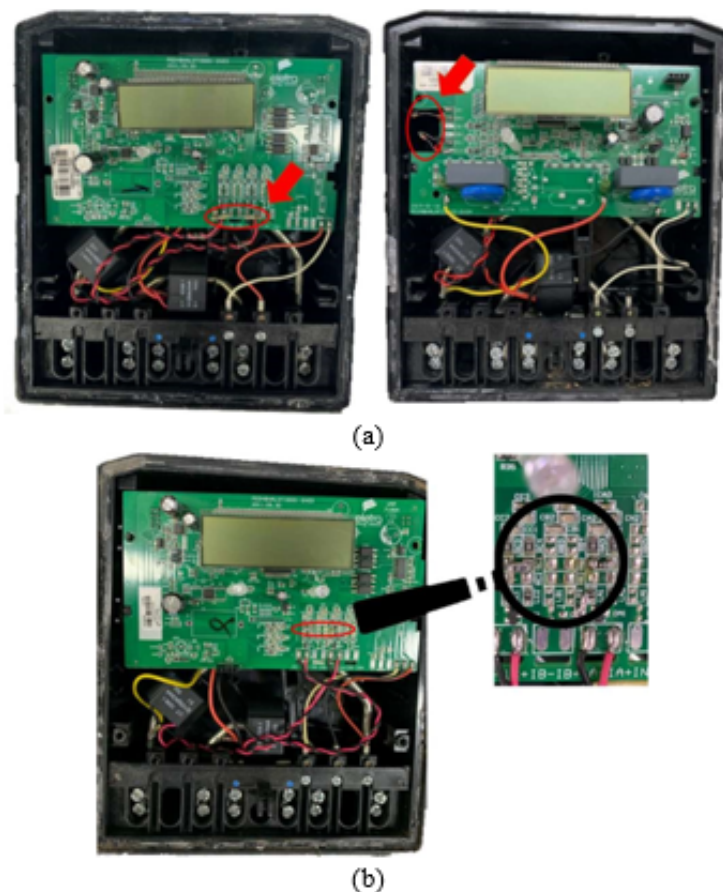


Figura 1 – (a) Medidores com resistências adicionadas ao canal de corrente. (b) Medidor com resistências do canal de tensão adulteradas.

Uma característica em comum que todas essas fraudes apresentam é que são permanentes, ou seja, não podem ser revertidas. Para esse tipo de fraude, nas inspeções, os eletricitistas utilizam o equipamento de verificação metrológica, que possui um padrão preciso e calibrado em laboratório; quando é injetada uma determinada corrente no medidor sob teste e conectada uma carga padronizada, é realizada uma comparação entre o valor medido no equipamento verificador metrológico, que possui a referência padrão de um medidor sem fraude, e o que está sendo medido no medidor sob teste. Se houver discrepância entre as medidas, o equipamento gera um alerta de suspeita de fraude e o eletricitista pode executar os procedimentos para notificação do cliente, retirada e substituição do medidor, com o medidor retirado sendo lacrado para confirmação de seu funcionamento “I – em laboratórios acreditados para ensaios em medidores de energia elétrica; ou II - no laboratório da distribuidora, desde que com pessoal tecnicamente habilitado e equipamentos calibrados conforme padrões do INMETRO ou órgão metrológico delegado, devendo o processo ser certificado na norma ABNT NBR ISO 9001.” (Resolução Normativa ANEEL nº 1000, 2021, art. 593).

Entretanto, para contornar a detecção dessas fraudes permanentes que são identificadas com os equipamentos verificadores metrológicos tradicionais de mercado, os fraudadores desenvolveram o que pode ser chamado de fraude dinâmica. Diferentemente das fraudes permanentes, este tipo de fraude utiliza circuitos eletrônicos ativos que, além de promoverem uma redução na leitura realizada, permitem habilitar e desabilitar a fraude dinamicamente, acionada, por exemplo, por um temporizador ou por controle remoto.

A Figura 2 mostra um medidor eletrônico removido de uma unidade consumidora com a instalação de circuitos externos ao medidor. Como pode ser observado, foram adicionadas duas placas eletrônicas, sendo uma fonte de alimentação e uma placa de comunicação por rádio frequência (RF) com relés eletromecâni-

cos integrados, utilizados para realizar o desvio nos canais de medição de corrente. Ou seja, quando a fraude dinâmica estivesse ligada, o medidor de energia estaria registrando um consumo menor e quando a fraude estivesse desligada o medidor de energia estaria registrando um consumo correto, igual a um medidor padrão sem fraudes.



Figura 2 - Medidor com um circuito externo inserido contendo dispositivos de comunicação remota. Nesta categoria de fraude, o equipamento verificador metrológico padrão não seria assertivo caso a fraude se encontrasse desabilitada durante a inspeção do medidor, pois com a fraude desligada a medição de consumo de energia do medidor não será discrepante em relação ao padrão de referência de um medidor sem fraude. Nessa situação, há um número de fraudes que não é possível detectar com os equipamentos existentes atualmente, e a identificação dessa fraude depende da habilidade e da experiência do eletricitista em verificar se houve abertura do invólucro do medidor, o que muitas vezes não é tarefa simples e perceptível em campo, ocasionando a possibilidade de algumas fraudes não serem detectadas com a precisão e a assertividade desejada no combate à fraude de energia, que prejudica todos os consumidores em geral. Por meio da pesquisa realizada nesse trabalho, foi comprovado que todo circuito eletrônico e especialmente os de medidores eletrônicos de energia elétrica possuem características próprias que são únicas para cada modelo de medidor dentro de certos aspectos das grandezas elétricas, tais como: potência consumida (perda interna), corrente, distorção harmônica (THD) de corrente, forma de onda, etc. Consequentemente, a adição de qualquer circuito externo ao circuito original irá modificar substancialmente e de maneira observável essas características intrínsecas do medidor de energia.

Diante do cenário apresentado, viu-se a oportunidade de desenvolver uma metodologia para detecção de fraudes eletrônicas dinâmicas e, a partir disso, construir um único equipamento que conseguisse de forma integrada identificar tanto as fraudes dinâmicas quanto as fraudes permanentes. Como o conceito para identificação de fraudes permanentes já era conhecido, através de equipamentos de verificação metrológica, o principal desenvolvimento foi realizar a incorporação das funcionalidades referentes à detecção das fraudes eletrônicas dinâmicas.

A metodologia de identificação de fraudes eletrônicas desenvolvida neste trabalho parte da premissa que um medidor eletrônico de energia elétrica pode ser identificado pelas informações contidas nas formas de onda da tensão e da corrente, uma vez que, com a adição de um circuito estranho ao medidor, haverá algum nível de modificação destas características e essas diferenças podem ser percebidas por meio de uma comparação de sinais elétricos e medição de grandezas. As seções seguintes detalham o desenvolvimento e os resultados obtidos ao longo deste trabalho.

2. Desenvolvimento

Para desenvolvimento deste trabalho, realizou-se, inicialmente, uma análise estatística visando a identificação dos tipos de fraudes internas comumente encontradas em medidores de energia elétrica. Para esse propósito, analisou-se um total de 495 medidores eletrônicos de energia elétrica contendo algum tipo de fraude ou reprovados em testes e inspeções da Energisa, estratificados entre 6 fabricantes e 19 modelos diferentes, conforme mostrado na Tabela 1. Também foram analisados medidores de referência, não fraudados.

Tabela 1 - Estratificação da amostra de medidores utilizados.

FABRICANTE	MODELO	QUANTIDADE	
		FRAUDADOS	NÃO FRAUDADOS
A	1	13	1
	2	5	0
	3	1	0
	4	1	0
	5	1	0
	6	0	1
	7	0	1
	8	0	1
	9	0	1
B	1	15	4
	2	224	6
	3	1	0
	4	7	1
	5	149	1
	6	0	3
	7	0	7
	8	0	1
C	1	7	2
	2	20	4
	3	0	1
D	1	4	3
	2	0	1
E	1	44	4
	2	0	1
	3	0	1
	4	0	1
	5	1	1
	6	0	1
	7	1	0
	8	1	0
F	1	0	2
	2	0	2
TOTAL		495	52

Dos medidores cujas fraudes foram observadas, foram identificados quatro tipos de fraudes recorrentes, a saber:

- ICE: Inserção de um circuito externo, geralmente um switch programável;
- ICE–CR: Inserção de circuito externo contendo algum dispositivo de comunicação remota;
- AR: Adulteração da resistência do canal de tensão/corrente;
- BCC: “By-pass” direto do canal de corrente.

A Figura 3 ilustra a composição numérica dos tipos de fraude encontrados. A Figura 4, por sua vez, apresenta um resumo estatístico dos tipos de fraudes internas encontradas na amostra de medidores.

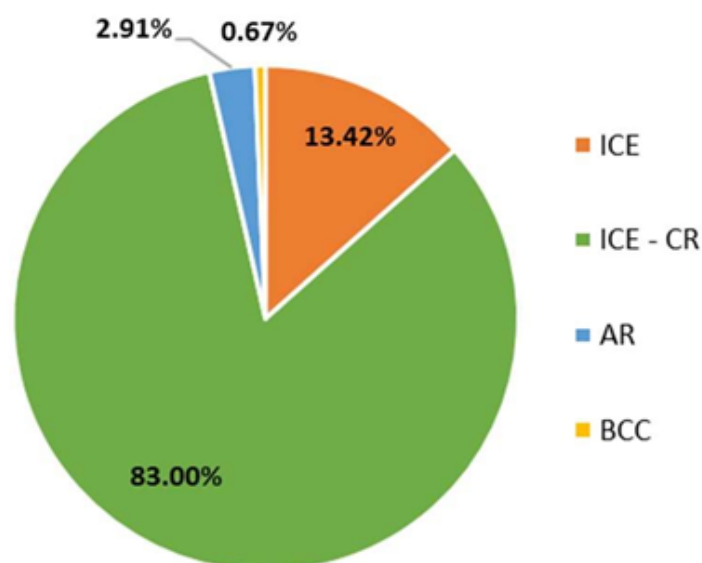


Figura 3 - Quantitativos do resultado dos tipos de fraude encontrados.

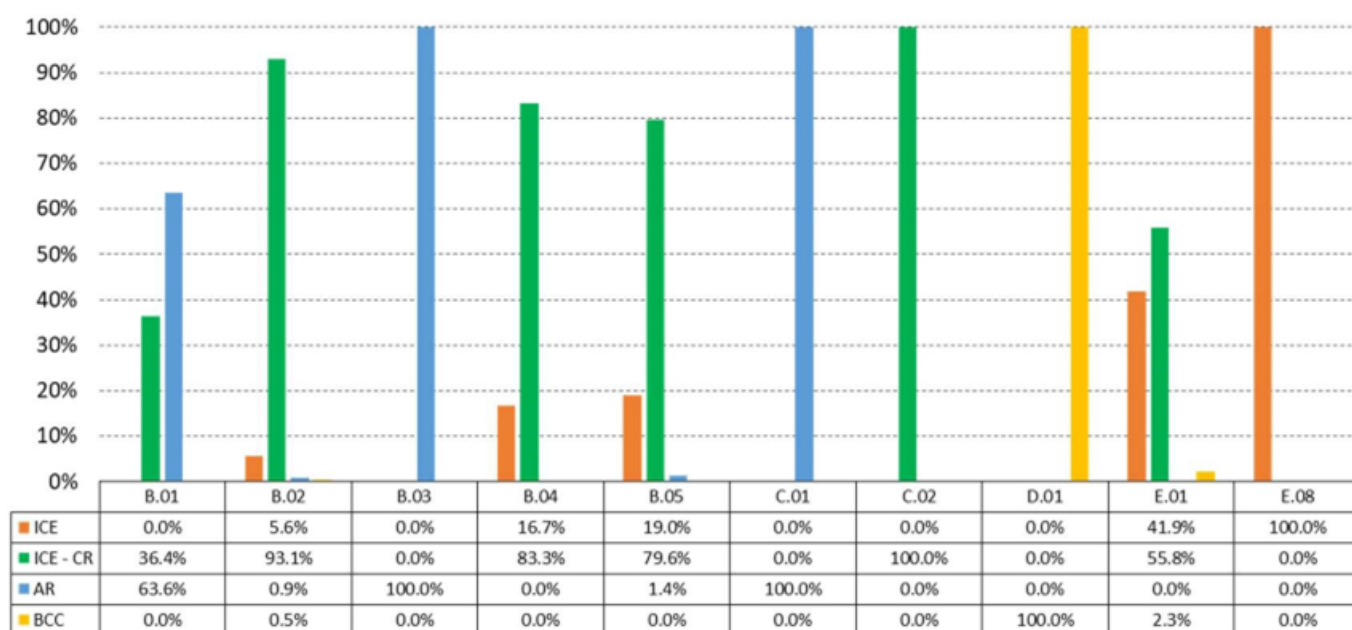


Figura 4 - Resumo estatístico do resultado dos tipos de fraude encontrados.

Durante o processo de levantamento dos tipos de fraude, verificou-se que a maioria das fraudes compreende a inserção de um circuito eletrônico (suprido por uma fonte de alimentação própria) dentro do próprio medidor, muitas vezes com acionamento remoto. Essas fraudes não possuíam equipamento capaz de identificá-las sem a abertura do medidor. O segundo maior tipo de fraude encontrado está relacionado à inserção de circuito de *by-pass*. A adulteração de resistências e o *by-pass* do canal de corrente foram encontrados em menor número, sendo estas fraudes possíveis de serem detectadas *in loco* no medidor sob teste pelo eletricista inspetor com a utilização da funcionalidade de verificador metrológico.

Após o levantamento estatístico dos tipos de fraudes encontradas, foram realizadas medições para avaliar e comparar as características elétricas dos medidores de referência e fraudados. A Figura 5 apresenta o *setup* de laboratório da Universidade Federal de Uberlândia (UFU) utilizado nestas medições. Para auxiliar

na análise, foi desenvolvido um *software* que permitiu comparar visualmente as formas de onda instantâneas de tensão e corrente entre medidores de referência e medidores fraudados. Além disso, o *software* desenvolvido é capaz de calcular parâmetros como amplitude de tensão e corrente eficaz, perda interna do medidor, assim como a distorção harmônica de corrente. A Figura 6 ilustra o exemplo de um resultado de comparação entre dois medidores, sendo um de referência e outro fraudado.

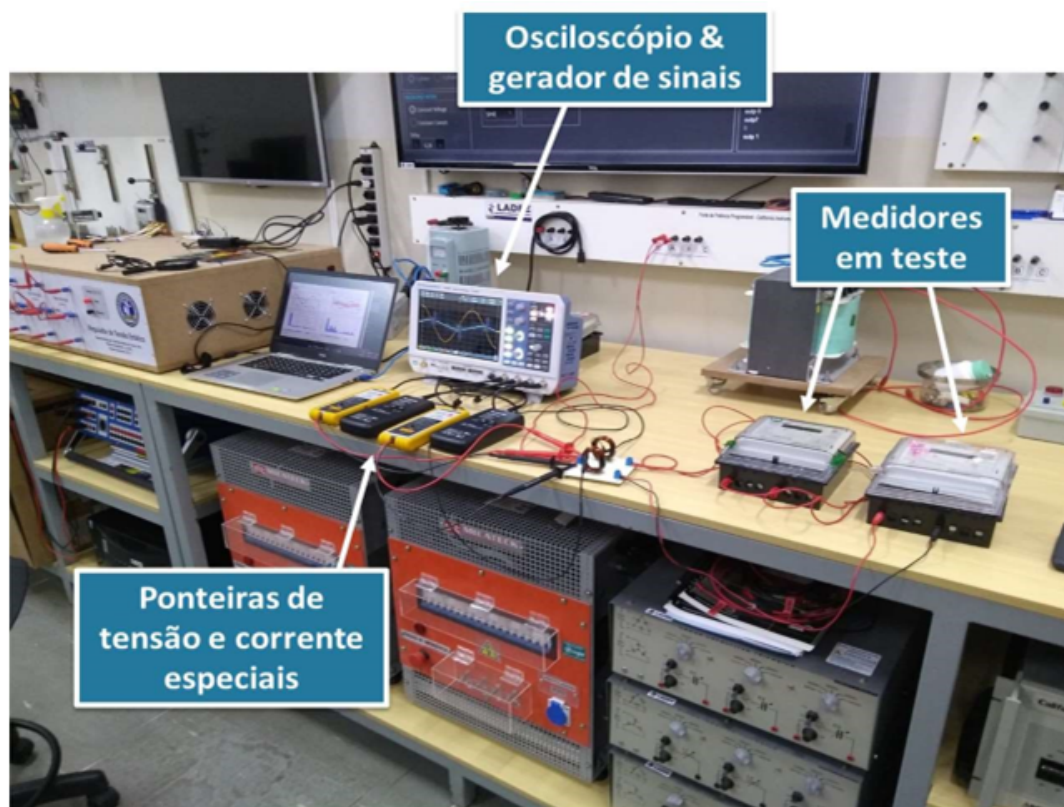


Figura 5 - *Setup* de laboratório utilizado para avaliação das características de alimentação de medidores eletrônicos de energia elétrica.

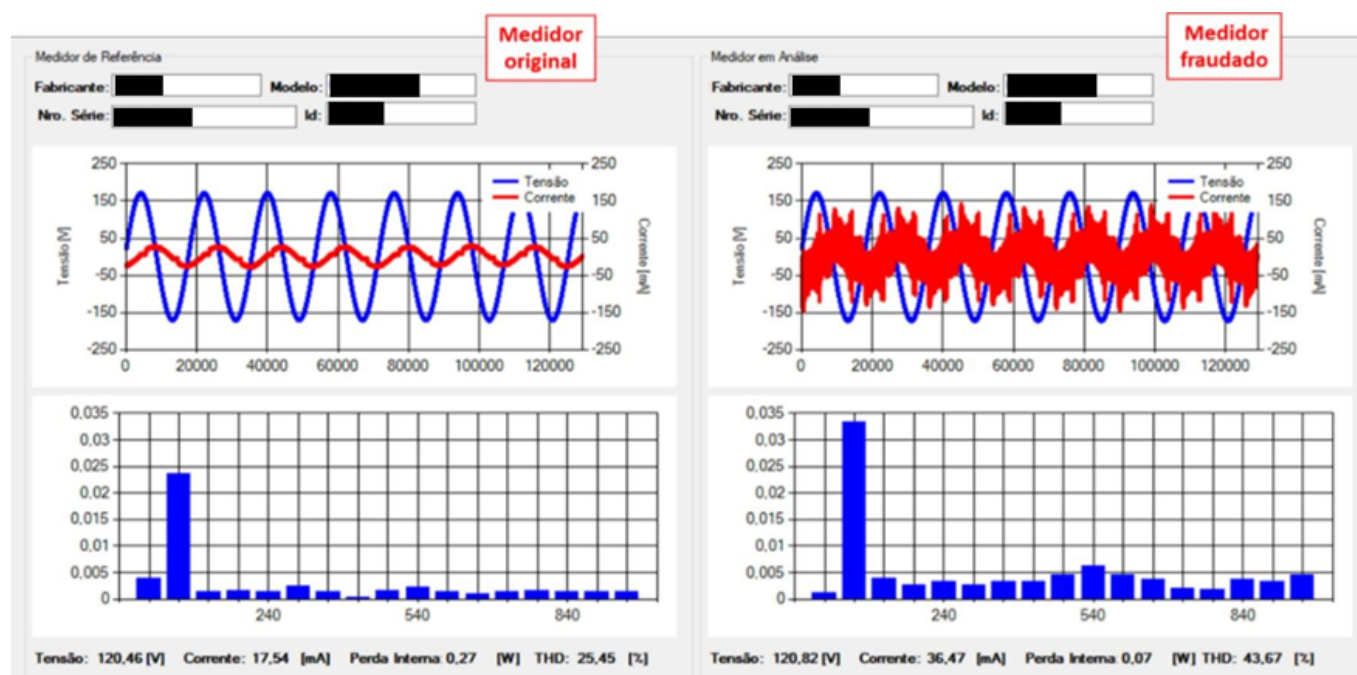


Figura 6 - Tela do *software* de laboratório utilizado para comparar medidores de referência e fraudados. Após a análise e a comparação das formas de onda da corrente nos canais de tensão entre os medidores, sem fraude e com fraude, identificou-se duas situações distintas. Na primeira situação foram adicionados ao medidor circuitos com fonte de entrada linear, com característica semelhante às fontes utilizadas na maioria dos medidores ensaiados. A forma de onda da corrente nos medidores fraudados é, com exceção da amplitude, muito semelhante àquela encontrada em medidores não fraudados. Os principais indicadores que podem ser utilizados para identificação da fraude nesta situação são: amplitude da corrente fundamental, distorção harmônica total de corrente, assim como a perda interna do medidor considerando apenas a frequência fundamental. Para quantificação da distorção harmônica total de corrente, considerou-se uma frequência máxima de 900 Hz (15ª harmônica).

Na segunda situação, a fonte de entrada do circuito de fraude é do tipo chaveada. Este tipo de fonte tem como característica ruídos em alta frequência provocados pelo chaveamento. Assim, diferentemente da primeira situação, a forma de onda da corrente observada nos medidores fraudados é bastante distinta daquela encontrada nos medidores não fraudados, permitindo que a fraude seja identificada por mera comparação das formas de onda. Além disso, observou-se uma variação expressiva nas amplitudes das harmônicas individuais de ordens superiores, distorção harmônica total, assim como uma alteração muito significativa na perda interna do medidor. Observou-se, também, perdas internas negativas e bem próximas à zero.

A partir dos resultados dos testes realizados foi proposta a metodologia para a identificação de fraudes dinâmicas em medidores eletrônicos. Esta metodologia é baseada na comparação entre os parâmetros das curvas de corrente dos canais de tensão obtidos de medidores de referência com as curvas do medidor sob teste. São calculados parâmetros para cada combinação possível dos canais de tensão. Isto é, para um medidor trifásico a 4 fios serão calculados os parâmetros para os canais AN, BN, CN, AB, BC e CA. Este conjunto de parâmetros característico para cada modelo de medidor foi denominado de DNA Digital do medidor. As curvas de corrente devem ser obtidas utilizando a tensão nominal do medidor, normalmente 120V para medições fase-neutro e 240V para medições fase-fase. A partir desses resultados positivos da pesquisa, iniciou-se o desenvolvimento do protótipo do equipamento eletrônico com a funcionalidade de detecção de fraudes eletrônicas dinâmicas.

A Figura 7 mostra o protótipo do equipamento analisador de fraudes eletrônicas e o *software* de gestão de banco de dados de DNA Digital em sua versão original da primeira fase da pesquisa e desenvolvimento. A Figura 8 mostra a comparação entre as curvas de corrente de um medidor de referência sem fraude e um medidor do mesmo modelo contendo a fraude em seu circuito eletrônico.



Figura 7 - Analisador de Fraudes e software de gestão da base de dados de DNA Digital.

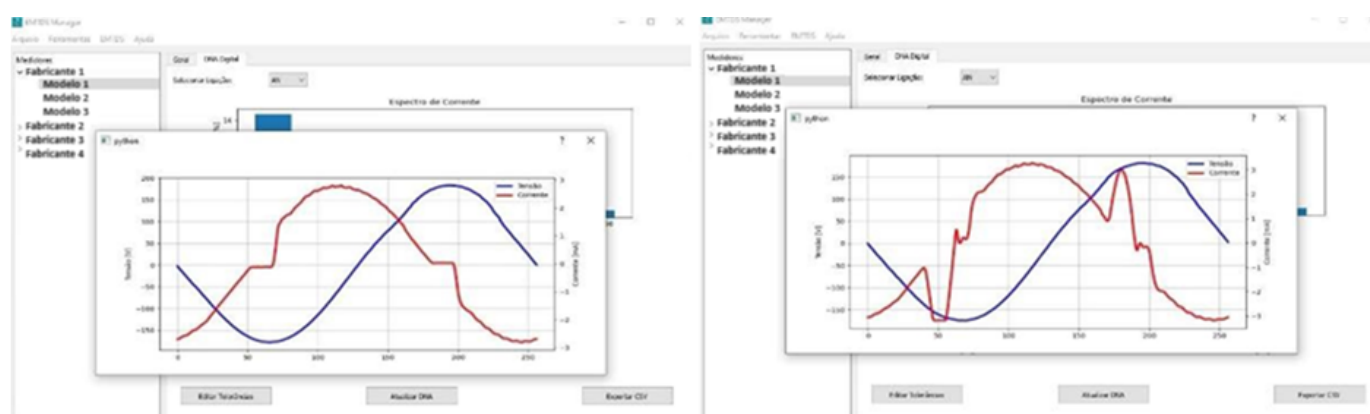


Figura 8 - Comparação entre as curvas de corrente de um medidor de referência e fraudado.

A eficácia da metodologia proposta para detecção de fraudes eletrônicas dinâmicas foi, primeiramente, testada em laboratório da UFU e, em seguida, foram realizados testes de campo com os eletricitas inspetores na Energisa Rondônia, utilizando os equipamentos para verificação de medidores eletrônicos, conforme visto na Figura 9. Nesse primeiro teste de campo foi possível obter vários depoimentos dos eletricitas como oportunidades de melhoria do equipamento no sentido de usabilidade e ergonomia.



Figura 9 - Fotos dos testes realizados pela equipe de eletricitas da Energisa Rondônia.

As sugestões de melhoria do primeiro teste foram priorizadas e implementadas em uma nova versão do protótipo do equipamento de detecção de fraudes eletrônicas, que foram novamente submetidas a novo ciclo de testes em laboratório da Energisa Rondônia. Nos testes de laboratório, foram avaliados 172 medidores de 8 modelos de 4 fabricantes diferentes. Desta amostra, a metodologia desenvolvida apresentou uma assertividade de 100% para os medidores fraudados e de 93% para medidores não fraudados (7% de falsos positivos).

Após a realização dos testes em laboratório, algumas unidades da nova versão do equipamento analisador de fraude eletrônica foram distribuídas para equipes de eletricitas da Energisa Rondônia para realização de uma campanha de inspeção em campo e em medidores escolhidos aleatoriamente, considerando aqueles que possuíam qualquer um dos 8 modelos de medidores analisados durante os testes de laboratório. Ao longo da campanha de inspeção, foram testados 76 medidores em campo e a metodologia foi capaz de identificar 100% dos medidores fraudados e 84% dos medidores não fraudados.

Por meio da análise dos dados para identificar os motivos para os falsos positivos de apontamento de suspeita de fraude em medidores não fraudados, foi possível constatar que as causas estão associadas a uma maior variabilidade das características dos circuitos eletrônicos de medidores com lotes de fabricação em anos diferentes dos lotes dos medidores testados em laboratório. Esse ponto foi considerado como prioritário na melhoria da precisão do equipamento integrado a ser desenvolvido na nova versão do equipamento.

Com os bons resultados provenientes dos testes com o equipamento analisador de fraudes eletrônicas em laboratório e em campo, decidiu-se desenvolver o equipamento Analisador de Fraudes Eletrônicas e Ver-

ificador Metrológico Integrado (AFEVMI). Dessa forma, seria possível ter as funcionalidades de detecção de fraudes dinâmicas e permanentes em um único equipamento.

A funcionalidade de verificação metrológica para identificar as fraudes permanentes utiliza a metodologia de comparação das medições do medidor sob análise com as de um medidor padrão calibrado que está referenciado no equipamento com alta precisão e é rastreável com os padrões metrológicos estabelecidos nas normas de medição. Assim, o equipamento verifica se o medidor sob teste está registrando corretamente o consumo de energia conforme a corrente injetada e o consumo medido pelo equipamento por meio de acionamento de botoeira de pulso ou sensor de leitura ótica. Após o tempo estabelecido para o teste, é feita a comparação entre as medidas registradas no equipamento e no medidor e, se houver discrepâncias, é indicado se há ou não indícios de adulteração no medidor. As características do verificador metrológico utilizadas no equipamento são: Classe de exatidão + incerteza de 0,2%; categoria de sobretensão CAT IV-300V; tensão de alimentação de 127 Vca $\pm 10\%$ / 60 Hz $\pm 1\%$ ou 220 Vca $\pm 10\%$ / 60 Hz $\pm 1\%$, com uma interface de operação por meio de uma tela que permite configurar os parâmetros como constante do medidor (ex. 0,05 W/h por pulso), número de pulsos para execução do ensaio de exatidão.

A funcionalidade do equipamento de detecção de fraudes eletrônicas dinâmicas utiliza o mesmo princípio metodológico da versão do protótipo da fase anterior da pesquisa, ou seja, o equipamento integrado fará a identificação da fraude por meio da comparação direta entre os parâmetros característicos (DNA Digital) de um modelo de medidor de referência com os parâmetros do medidor sob teste. Para realizar esta comparação, é utilizado o banco de dados local do equipamento com todos os DNA Digitais de um conjunto de modelos de medidores de referência que foram coletados em laboratório e armazenados em um software de gestão. Na Figura 10, é possível observar o protótipo que contempla as 2 funcionalidades e foi desenvolvido em parceria com a empresa MINIPA.



Figura 10 - Protótipo do Analisador de Fraudes Eletrônicas e Verificador Metrológico Integrado.

Para essa nova fase com versão do sistema integrado, também foi desenvolvido um novo software de gestão do DNA Digital, onde cada modelo de medidor é cadastrado e as informações de grandezas dos medidores de referência serão armazenadas em banco de dados. No software de gestão foi implementada uma metodologia estatística para calcular a mediana e o desvio padrão e armazenar o DNA Digital do modelo do medidor, a partir de várias medições realizadas em medidores de referência do mesmo modelo, mas com anos de fabricação diferentes. Isso endereça a resolução do problema de falsos positivos identificado na versão inicial do equipamento. Após o cálculo do desvio padrão das grandezas, será armazenada a margem de tolerância que forma o registro de DNA digital de cada modelo de medidor. Um registro de configuração do DNA Digital geral de vários modelos será gerado e carregado no equipamento AFEVMI, com controle de atualização pelo software de gestão. No software de gestão, são cadastrados os fabricantes, os modelos de medidores, os equipamentos integrados produzidos, calibrados e certificados. Além disso, há um controle de rastreabilidade de suas atualizações de firmware e DNA Digital.

Em laboratório, o usuário autorizado irá fazer o cadastro do modelo do medidor no software, realizar a alimentação do equipamento AFEVMI em uma tensão estabilizada e conectar os cabos do equipamento no medidor de referência que se quer realizar as medições. Com a medição coletada e validada na tela do equipamento pelo técnico de laboratório, este enviará o comando para armazenar as medidas no software de gestão, sendo gravadas as informações de usuário, equipamento, data e hora da medição, modelo do medidor e todas as grandezas características de tensão, corrente, perda interna e distorção harmônica. Cada medição realizada será associada a um modelo de medidor no software de gestão. Após a medição de todos os modelos de medidores disponíveis em laboratório, o técnico responsável irá fazer a geração do arquivo geral do DNA Digital dos modelos de medidores.

Após isso, todos os equipamentos AFEVMI devem ser atualizados com a versão mais recente do DNA Digital, o que pode ser feito de modo remoto e sincronizado, por meio de um comando, quando o equipamento for conectado a uma rede *Wi-Fi* autorizada. Serão registradas, no software, todas as atualizações realizadas pelos equipamentos e exibidos em relatório os equipamentos que estão atualizados com a última versão e os que precisam de atualização mais recente.

Com o equipamento atualizado em mãos, o eletricista inspetor pode realizar as inspeções em campo, obedecendo a todos os procedimentos de comunicação e segurança para desligar o medidor de energia do cliente. Para isso, ele irá desconectar os cabos de entrada da alimentação do medidor de energia e conectar de forma segura os cabos de alimentação das fases e neutro no conector especial do AFEVMI, fazendo a devida identificação dos cabos de entrada (fase/neutro) e saída (carga do cliente), obedecendo a sinalização da cor dos cabos do equipamento e sinalizações nos bornes do medidor.

Com o equipamento devidamente conectado e energizado, o eletricista irá selecionar o modelo do medidor a ser testado na interface do equipamento (tela sensível ao toque) e clicar no botão para iniciar o teste de detecção de fraude de forma automatizada. O equipamento irá selecionar automaticamente a combinação das fases do medidor e ligação das entradas e saídas por meio de relés e realizará inicialmente o teste de detecção de fraude eletrônica, que indicará na tela o resultado do teste como CONFORME ou NÃO CONFORME e, em seguida, irá realizar o teste de verificação metrológica, indicando o percentual do erro de medição encontrado.

3. Conclusão

Este trabalho apresentou o desenvolvimento de uma metodologia de comparação de DNA Digital e a criação de um equipamento integrado para analisar fraudes permanentes e dinâmicas em medidores de

energia elétrica. O equipamento é de fácil operação e agrega funcionalidades de precisão e exatidão na análise de fraudes eletrônicas em todos os modelos de medidores.

O trabalho proposto teve como objetivo, inicialmente, desenvolver uma metodologia para identificar fraudes dinâmicas, a fim de construir um equipamento capaz de incorporar essa metodologia e, posteriormente, realizar o desenvolvimento de um equipamento único, denominado Analisador de Fraudes Eletrônicas e Verificador Metrológico Integrado, com a capacidade de detectar todos os tipos de fraudes eletrônicas em medidores de energia.

A metodologia de detecção de fraudes eletrônicas dinâmicas se baseia na criação de um conjunto de parâmetros extraídos das curvas de tensão e corrente do medidor denominado DNA Digital. O DNA Digital é extraído de um medidor de referência não fraudado e compõe um banco de dados que é utilizado pelo Analisador de Fraude como referência de comparação para determinar se o medidor sob teste está CONFORME, ou seja, possui os parâmetros equivalentes ao modelo de medidor de referência, ou se está NÃO CONFORME, indicando suspeita de fraude por inserção de circuitos eletrônicos para fraudar o medidor.

Posteriormente, foi realizada a especificação para que fosse possível integrar ao equipamento de detecção de fraudes eletrônicas a funcionalidade de verificação metrológica, permitindo, assim, que o equipamento também identifique fraudes permanentes, através da comparação das medições do medidor sob análise com as de um padrão calibrado e preciso referenciado no equipamento com os padrões metrológicos estabelecidos nas normas de medição. Assim, o equipamento verifica se o medidor sob teste está registrando corretamente o consumo de energia conforme a corrente injetada e o consumo medido pelo equipamento por meio de acionamento de botoeira de pulso ou sensor de leitura ótica. Após o tempo estabelecido para o teste, é feita a comparação entre as medidas registradas no equipamento e no medidor e é apresentado o erro de medição encontrado.

A eficácia da metodologia de detecção de fraudes eletrônicas dinâmicas foi avaliada em testes de laboratório e comprovada durante uma campanha de inspeção em medidores reais em campo. Tanto nos testes em laboratório quanto nos testes em campo a metodologia proposta foi capaz de identificar 100% dos medidores fraudados e pelo menos 84% dos medidores sem fraude. O número de falsos positivos pode ser reduzido melhorando a precisão e exatidão do equipamento integrado e aprimorando os critérios de decisão utilizados para identificar um medidor fraudado com os parâmetros utilizados no DNA Digital de referência, considerando o modelo estatístico com medidas de modelos de medidores de lotes de fabricação diferentes. Esses resultados da melhoria da detecção de fraudes com o equipamento integrado serão divulgados oportunamente quando tivermos mais dados de testes em campo.

4. Referências bibliográficas

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA (ANEEL). **Resolução Normativa nº 1000, de 7 de dezembro de 2021**. Consolidação dos atos normativos da ANEEL de natureza normativa, exceto regimentos internos e normas de organização interna. Brasília, 2021. Disponível em: <https://www.aneel.gov.br>. Acesso em: 26 nov. 2024.

AMHENRIOR, H. E., EDEKO, F. O., OGUJOR, E. A., EMAGBETERE, J. O. **Design and Implementation of an Automatic Tamper Detection and Reporting Capability for a single-phase Energy Meter**. IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), 2017.

FOIATTO, Noara. **Sistematização do reconhecimento de irregularidades que caracterizam fraude em medidores de energia**. Dissertação de Mestrado, Universidade Federal do Rio Grande do Sul, 2009.

MARTINS, Anderson Vedoveto. **Medidor de energia elétrica não intrusivo para detecção de fraudes.** Dissertação de Mestrado, Universidade Estadual de Campinas, 2018.

PATIL, N. V., BONDAR, D. R., KANASE, R. S., BAMANE, P D. **Intelligent Energy Meter with Advanced Billing System and Electricity Theft Detection.** 2017. International Conference on Data Management, Analytics and Innovation (ICDMAI).