

DOI: 10.24850/j-tyca-2020-04-08

Notes

## **Indicative and preventive measures against tampering of water consumption meters**

### **Medidas indicativas y preventivas contra la manipulación fraudulenta de medidores de agua**

Stefan Ziemendorff<sup>1</sup>, ORCID: <https://orcid.org/0000-0001-9253-4250>

<sup>1</sup>Consultor de la cooperación alemana al desarrollo, Deutsche Gesellschaft für Internationale Zusammenarbeit, Eschborn, Alemania, [sziemendorff@gmail.com](mailto:sziemendorff@gmail.com)

Correspondence author: Stefan Ziemendorff, [sziemendorff@gmail.com](mailto:sziemendorff@gmail.com)

#### **Abstract**

The tampering of water consumption meters is a problem of increasing importance in many countries, resulting in economic losses for the water utilities. In the present article the great variety of tampering of meters are analyzed, defining the vulnerable points of them. Then it proceeds to analyze and compare the existing indicative and preventive measures to protect the meters, arriving at the conclusion that according to each

legal situation there are measures that allow avoiding their tampering, vandalization and theft in an effective way. Finally, it is recommended for each legal situation what these measures are.

**Keywords:** Tampering of water meters, water meter security devices, security seals.

## Resumen

La manipulación fraudulenta de medidores de agua potable es un problema de importancia creciente en muchos países, lo cual provoca pérdidas económicas para las entidades prestadoras. En el presente artículo se analizan las formas de manipulación de medidores, señalando sus puntos vulnerables. Luego se procede a analizar y comparar las medidas indicativas y preventivas existentes para proteger los medidores, llegando a la conclusión de que acorde con cada situación legal, hay medidas que de manera eficaz permiten evitar su manipulación, vandalización y robo. Por último, se recomienda para cada situación legal cuáles son las medidas a tomar.

**Palabras clave:** manipulación de medidores de agua, dispositivos de seguridad de medidores de agua, sellos de seguridad.

Received: 12/07/2018

Accepted: 02/10/2019

## Introduction

Due to the growing shortage of drinking water, many utilities have taken measures to reduce their water losses, both physical losses and so-called apparent or commercial losses. Although progress has been made by reducing physical losses by controlling pressures and leaks, reducing commercial losses, increasing the levels of micromediation, there is a component that seems to be constantly increasing: water theft. This occurs through illegal installations and the tampering of meters. This paper refers on the latter and the ways to fight it.

Although this topic is treated extensively in newspapers throughout Latin America, there is very little data on the true size of the problem. As an example, it can be mentioned that in the city of Lima, Peru, almost 8 000 cases of stolen, tampered or vandalized meters were recorded in the first four months of 2019 (García, 2019).

This paper refers only to velocity meters (single-jet and multi-jet), which are used in most Latin American localities due to their low cost. The objective of this study is to find out what are the most effective ways to protect these meters against different types of tampering. To this end, the procedure was as follows:

- First step: Operators of meter test benches of Peruvian utilities have been interviewed (see acknowledgments) about the forms of tampering they have found.
- Second step: These forms of tampering have been classified according to the points of the meters that are violated.
- Third step: It was analyzed how preventive and indicative measures protect meters at their vulnerable points.

Below are the results for the three steps followed.

## Results

### **Ways of tampering velocity meters and the vulnerable points of the meters**

The tampering of meters is done in different ways, varying the patterns, depending on the meter model installed, the legal situation and the security measures taken by the operators. One form to classify the ways

of tampering is according to their visibility, the first group being the one where the tampering is evident to the naked eye, the second group that can be noticed only with a careful review of the meter and the third group that does not leave visible evidence. Some frequent forms are shown in Figure 1.



**Figure 1.** Ways of tampering: A) Vandalized glass; B) perforated glass; C) separate register; D) helices stopped with a wire; E) gear teeth removed; F) magnetic transmission braked with a token; G) cut propellers; H) stopping with a magnet.

**Group 1 (Permanent and visible physical tampering):** Its purpose is that the meter cannot be read. They are detected at the latest during the meter reading. The forms are:

1. **Self-theft of the meter:** It consists of the user subtracting his meter permanently, pretending that it was stolen. Because in some places the theft of meters is really massive, it is extremely difficult to distinguish self-theft from real theft.
2. **Theft of the register:** It consists of extracting the register, leaving the cast. It occurs frequently if the meter is anchored on the floor.
3. **Vandalization:** It consists in destroying the meter, hitting it, affecting its operation or avoiding the reading (Figure 1, A).
4. **Scratching or painting of the glass:** This form allows the meter to work, but prevents it from being read.

**Group 2 (permanent physical tampering, only visible when checking the meter):** This group consists of altering the meter in a way that it records less than the actual consumption, altering its internal functioning. It is frequent where tampering is not sanctioned. They are not obvious, and can be found mostly only by uninstalling, disassembling and checking the meter. The forms are:

1. **Perforation of the glass:** It consists of drilling a hole in the glass to access the register to destroy it or to temporarily introduce objects that paralyze the consumption count (Figure 1, B).
2. **Drilling of register from the side:** It is similar to the previous form of tampering, but with the difference that it is done from the sides with a hot metal object or with drills. It is more difficult to detect at the time of reading.
3. **Perforation of the turbine cast:** Meter models with plastic casts can be perforated with hot metal objects to access the helices, at

points that are not visible to the reader, being able to paralyze them temporarily or permanently, without taking out the meter. Although metallic casts could also be perforated (with a drill), it is much more difficult, exposes the tamperer to be discovered and it is almost impossible to perform it at an invisible point.

- 4. Internal alteration of the helices:** It consists of disassembling the meter to modify the turbine helices so that they move at a slower speed (Figure 1, G).
- 5. Alteration of the transmission mechanism of the turbine to the register:** The magnetic transmission is interrupted or stopped with the introduction of small objects, such as metal or plastic tokens, between the turbine and the register (Figure 1, F).
- 6. Internal alteration of the gears of the register:** It consists of removing the register from the meter and removing teeth from the different gears, thus causing the recorded consumption to be lower, depending on the percentage of the teeth removed (Figure 1, E).
- 7. Paralysis of the helices:** It consists of paralyzing the helices by introducing pins or glue from the entrance or exit of the water (Figure 1, D), previously uninstalling the meter.
- 8. Boiling the meter:** It consists of uninstalling the meter and heating it so that its plastic parts deform or melt, altering or paralyzing the registration (Goodwin, Kaggwa, & Malebo, 2013).

**Group 3 (non visible temporary tampering, even by checking the meter):** These forms of tampering also have the purpose of under-

registration of the meter, but do not physically modify it, which makes it impossible to detect the tampering with its revision. The forms are:

- 1. Meter reversal:** The meter is turned over so that instead of increasing, the reading decreases as consumption continues.
- 2. Temporary removal of the meter:** In periods of high consumption, the meter is removed or replaced by a “phantom meter”; after this period, it is reinstalled.
- 3. Temporary separation of the register:** It consists of removing only the register from the meter, but not the complete meter, and putting it back before reading dates (Figure 1, C).
- 4. Reverse reading:** in this case a pressurized air flow is used to reverse the register. To do this, the meter is removed, the register is reversed and it is reinstalled.
- 5. Inclination of the meter:** Some users tip the meter to one side to under-register, although, depending on the model of the meter, the effect of this is little, not reaching 10% of under-registration in most meters, that is, it is still registered 90% of consumption (Arregui, Cabrera, Cobacho, & García-Serra, 2005).
- 6. Temporary introduction of wires:** It consists of a wire being introduced from the property, without being able to see the tamperer in the act of tampering. It also allows regulating the consumption record so that it does not go to zero, avoiding suspicion. In addition, the wire can be removed on reading dates.
- 7. Temporary application of magnets:** The magnetic transmission from the turbine to the register is braked with powerful magnets.



They are applied to the side of the meter, from where they can be quickly removed, which makes detection difficult (Figure 1, H).

With these forms of tampering the vulnerable points of the meters have been identified (Table 1).

**Table 1.** Vulnerabilities of velocity meters identified from the different forms of tampering.

Form of tampering		Vulnerability	
Group 1: Permanent and visible physical tampering	1	Meter (self)-theft	Meter removal
	2	Theft of the register	Meter or register removal
	3	Vandalization	Glass destruction, scratching
	4	Scratching / Painting of the glass	
Group 2: Permanent physical tampering , only visible by uninstalling and checking the meter	1	Perforation of the glass	Register perforation
	2	Perforation of the register from the side	
	3	Perforation of the meter cast	Cast perforation
	4	Alteration of the helices	Meter or register removal
	5	Alteration transmission turbine - register	
	6	Alteration of gears of the register	
	7	Stopping the helices	
	8	Meter boiling	Meter removal
Group 3: Temporary	1	Meter reversal	
	2	Temporary removal of the meter	

tampering not visible even checking the meter	3	Temporary removal of the register	Register removal
	4	Retrocession of registered consumption	Meter removal
	5	Inclination of the meter	Inclination
	6	Temporary stopping helices with wires	Wire through pipe
	7	Temporary stopping with magnets	Magnetism

The eight vulnerabilities identified are shown in Figure 2.



**Figure 2.** Vulnerabilities of velocity meters.

## Indicative measures

**Indicative measures** are those that evidence that the meter has been tampered without authorization. They do not prevent or hinder the tampering much, but their usefulness lies in the following points:

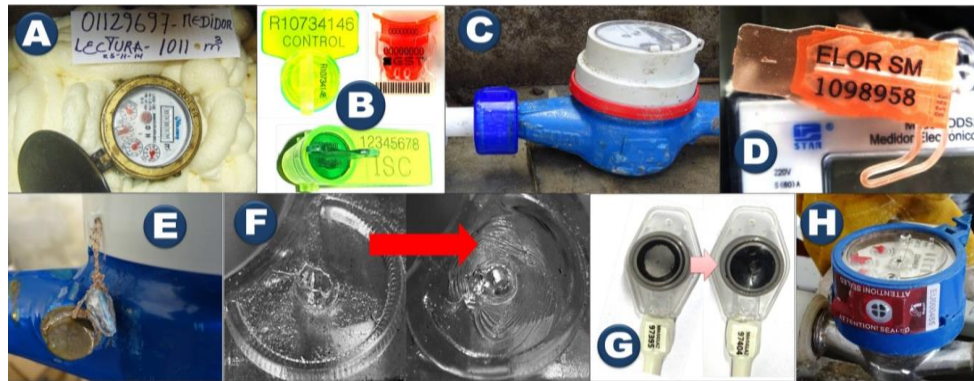
- a) Depending on the regulations, the violation of security seals can be sanctioned as an infraction or crime.
- b) Even if a broken seal is not accepted as evidence, it may result in the meter review or the application of other measures.
- c) The visible presence of the seals or other indicative measure may be dissuasive for a user tempted to tamper his meter.

Indicative measures can be classified into three:

1. Vulnerabilities where indicative measures may show that a specific vulnerability was exploited to tamper the meter.
2. Vulnerabilities that do not require indicative measures.
3. Vulnerabilities where it is impossible to take indicative measures.

**The first group** consists of feasible and useful indicative measures:

- 1. Against the possibility of perforating the register from the side** (Vulnerability 2): Although there are no security seals for this, there is an indicative measure that consists of filling the meter box with expansive foam and taking a picture of the box ( Figure 3, A). Since this foam always forms unique patterns, it is impossible to return it to its previous state once the meter has been tampered. Otherwise, it can only be detected by carefully checking the meter for which it is often necessary to uninstall it.



Figure

**Figure 3.** Indicative measures: A) filling the registration box with expansive foam (Courtesy SEDACUSCO); B) transparent seals; C) seal on the meter locknut; D) seal on a meter; E - Lead seal; F - Heat indicator, before and after heating; G - Magnetism indicator seal, before and after being magnetized; H - Meter with magnetism indicator seal.

**2. Against the possibility of perforating the cast (Vulnerability 3):** There are no seals for this, the expansive foam method being equally effective to indicate this type of tampering.

**3. Against the withdrawal of the meter (Vulnerability 4):** There are several methods in use, such as the expansive foam and a seal that secures the locknuts that fix the meter (Figure 3, C). The latter allows the meter to be removed only after breaking the seal that cannot be replaced without leaving evidence. A third method is with the use of sealing wire, secured with a seal (Figure 3, B). For the reader to realize it is necessary to move the wire because the cut part can be glued or hidden so that it is not noticed (Ríos, 2013).

**4. Against the removal of the register** (Vulnerability 5): The main use of security seals with wire sealant is to avoid the removal of the register. They serve to detect if the register was separated from the meter, which, even if the fact that the seal is broken cannot be sanctioned, is useful to realize that it is necessary to disassemble the meter and check if helices, gears, etc. were altered. Likewise, filling the meter box with expansive foam could provide evidence.

**5. Against the inclination of the meter** (Vulnerability 6): An inclined meter cannot be easily detected, when the user, before the reading date, returns the meter to its normal position. For this form of tampering the seal on the locknut is not useful (Figure 3, C), but two other measures:

- a) The installation of security seals that serves to identify if the meter was uninstalled. For this it is necessary that the sealing wire, which fixes the security seal, is firmly attached so that the meter can be moved only after the wire has been cut or the seal has been broken.
- b) The filling of the box with expansive foam.

**6. Against the use of magnets** (Vulnerability 8): A measure is the use of magnetism indicator seals. They are placed in the same meter and if they are subjected to magnetism they irreversibly indicate that there was a magnet nearby (Figure 3, G and H).

**The 2nd group**, which does not require indicative measures, consists of:

**1. Against the vulnerability of the glass** (Vulnerability 1): The destruction or perforation of the glass is self-evident at the time of

reading, although perforations of diameters smaller than one millimeter have been found, which are difficult to detect.

**The 3rd group** (impossible to take indicative measures), refers to the point:

**1. Against the accessibility to the turbine through the tube** (Vulnerability 7): A measure has not been found that evidences that the meter has been tampered, by introducing a paralyzing object from the site, this is without touching the meter. However, there is a preventive measure consisting of an anti-wire device (see below).

The indicative security measures are shown in Table 2.

**Table 2.** Indicative measures of tampering according to the meter vulnerabilities.

Vulnerabilities		Indicative measures			
		Expansion foam	Sealing wire /Security seals	Security device on the locknut	Magnetism indicator seal
<b>1</b>	<b>Glass destruction, scratching</b>	Not necessary	Not necessary	Not necessary	Not necessary
<b>2</b>	<b>Register perforation</b>	Feasible	Not feasible	Not feasible	Not feasible
<b>3</b>	<b>Cast perforation</b>	Feasible	Not feasible	Not feasible	Not feasible
<b>4</b>	<b>Meter removal</b>	Feasible	Feasible	Feasible	Not feasible
<b>5</b>	<b>Register removal</b>	Feasible	Feasible	Not feasible	Not feasible

<b>6</b>	<b>Inclination</b>	Feasible	Feasible	Not feasible	Not feasible
<b>7</b>	<b>Wire through pipe</b>	Not feasible	Not feasible	Not feasible	Not feasible
<b>8</b>	<b>Magnetism</b>	Not feasible	Not feasible	Not feasible	Feasible

Additionally, some specifications about the different methods are necessary to ensure that they can fulfill their function:

**About the use of expansive foam:** The measure is low cost (USD 2 to 3), but there is still no experience that the modification of the pattern, which leaves the foam, is accepted as legal proof of tampering. In any case, it is necessary to have a photo to make the contrast with the current state.

**About the use of security seals:** The wide variety of these is due to the fact that tamperers continually invent new methods for tampering these seals. Therefore, it is recommended:

1. The serial numbers of the seals must be registered, associated with the meter and be accessible to inspectors and readers in order to be verified. It has been observed that many utilities in Peru do not proceed in this way, allowing replacing the broken seal with another, without being detected.
2. Lead seals (Figure 3, E), do not provide much security because they are easy to handle with cuts or heat, imitable or artificially aged so that they are taken as originals (Ríos, 2013).

3. The security seals should preferably be transparent so that a possible tampering inside can be noticed.
4. Seals that are multi-body (such as male and female) must have the numbering on all parts or be physically attached, so as not to allow the removal and replacement of a part, for example, with stolen parts of seals from other meters (Figure 3, D; the seal is numbered in its 2 parts that were also joined).
5. One of the ways to violate plastic seals is with the use of heat that allows the removal of apparently fixed parts. Therefore it is recommended that they have heat indicators (Figure 3, F).

**About the use of magnetism indicator seals:** In a trial that was carried out in Tarapoto, Peru (Ziemendorff, 2017), it turned out that for these seals to fulfill their function they have to be very close to the magnet. It was tested with a 48.7 cm<sup>3</sup> magnet, in this case the seal (Figure 3, G) reacted at a distance of 6.5 cm, and in the case of another seal just at a distance of 3.5 cm. This implies that if the user recognizes the seal, he can attach the magnet to the other side of the meter (whose outside diameters exceed 6.5 cm) without the danger of being detected. Therefore, for the seals to work, the following measures are recommended:

- a) Get more sensitive indicator stamps. We do not know if these exist in the market.



- b) Use seals on opposite sides of the meter. To be effective they must react to magnetism at a minimum distance of 4 to 5 centimeters (according to the diameter of the meter).
- c) Place the seals in the middle of the glass. For this they must be adhered in such a way that it is impossible to be removed without leaving a trace (like the one in Figure 3, H).

## **Preventive measures incorporated into the design of the meter**

**Preventive measures** have the main purpose of making it impossible or difficult to tamper the meter. These can be classified into two types: those that are incorporated into the same meter and those that are additional devices. In case these are violated, which implies a much greater effort; they leave physical evidence, so they can also be indicative at the same time. The measures incorporated in the meter, depending on their vulnerabilities, can be classified into three:

1. Measures that have already been incorporated into the design. This mainly refers to meters observed in Peru.

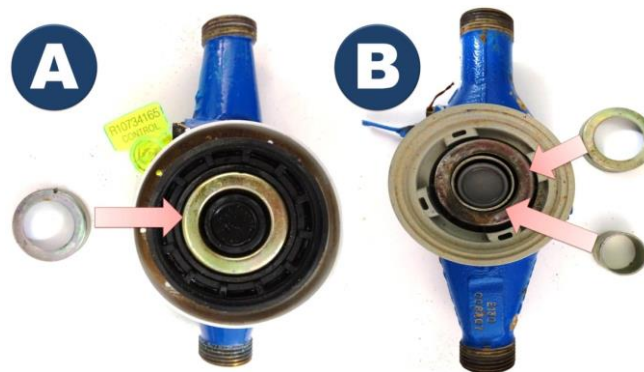
2. Measures that are technically feasible to incorporate. It refers to measures that have not been observed, but which theoretically could be part of the meters.
3. Measures that are not technically feasible to incorporate.

In the first group, forms have been found that prevent or hinder the following violations:

- 1. Against the perforation of the register from the side** (Vulnerability 2): Some meter models have, between the plastic housing of the register and the register itself, a metal tape, which prevents it from being perforated with hot pointed objects.
- 2. Against the possibility of perforating the cast** (Vulnerability 3): The vast majority of meter models have a metal cast that prevents it from being perforated with hot pointed objects. In those with a plastic cast, no metal tapes or plates equivalent to those mentioned above have been found.
- 3. Against the withdrawal of the meter** (Vulnerability 4): There are meters that have differentiated input and output threads, making it impossible to invert them. However, they are vulnerable against forms of tampering that involve the removal of the meter (reversal etc.). Therefore it is not an important advantage.
- 4. Against the withdrawal of the register** (Vulnerability 5): Almost all meters allow the removal of the register, but only by breaking some type of security seal. However, it has been found that several models allow the register to be opened in such a way that the seal remains intact. Apart from that, a model has been found whose

register is fixed with screws that can only be removed with violence or with a special key (González, Val, Rocha, & Segundo, 2010).

**5. Against the use of magnets** (Vulnerability 8): Many meters have been provided with antimagnetic shields, consisting of nickel and iron alloy rings (Figure 4).



**Figure 4.** (A) Simple antimagnetic shield (B) Double shield.

To evaluate the effectiveness of these shields, three different magnets were attached to four different  $\frac{1}{2}$  meters, in the standard test flows (Table 3). The tests were performed in Tarapoto, Peru (Ziemendorff, 2017).

**Table 3.** Results of tests with antimagnetic shields.

Magnet	Flow	Single Jet	Single Jet	Multi Jet	Multi Jet
--------	------	------------	------------	-----------	-----------

	rate	Without magnetic shield	With simple magnetic shield	With simple magnetic shield	With double magnetic shield
1	4.7 cm <sup>3</sup>	Q1	Standstill	No effect	No effect
		Q2	Standstill	No effect	No effect
		Q3	Standstill	No effect	No effect
2	23.1 cm <sup>3</sup>	Q1	Standstill	No effect	Standstill
		Q2	Standstill	No effect	No effect
		Q3	Standstill	No effect	No effect
3	48.7 cm <sup>3</sup>	Q1	Standstill	Under registration 5%	Standstill
		Q2	Standstill	No effect	Under registration 10%
		Q3	Standstill	No effect	No effect

As shown - the shields are effective. Unlike the unprotected meter, which is paralyzed with a small magnet in all flows, meters with antimagnetic protection are almost unaffected. The small sub-registers in the minimum and transient flows do not allow the tamperer to recover his investment in the magnet. The 48.7 cm<sup>3</sup> magnet (cost: USD 50), is the largest commercialized in Peru. Its handling was difficult and even dangerous due to its magnetic force. Therefore, it is assumed that larger magnets, apart from their higher cost, are already unmanageable for the tampering of meters.

In the second group of measures, among those which could be theoretically incorporated in the design of the meter itself, but which have not been observed, are the following:

- 1. Against the vulnerability of the glass (Vulnerability 1):** The glass of the meter is vulnerable due to the fact that it is manufactured with materials that are easily scratched, perforated or destroyed. It is feasible that they can be replaced by high-resistant transparent materials, such as metal glass.
- 2. Against the accessibility of the turbine through the tube (Vulnerability 7):** An anti-wire device can be fixed at the meter outlet to prevent the user from accessing the turbine from his property.

In the third group of measures, it has been found that it is not possible to prepare the meter against the following vulnerabilities:

- 1. Against the withdrawal of the meter (Vulnerability 4).**
- 2. Against the inclination of the meter (Vulnerability 6):** It is reiterated that not all meters are affected by the inclination.

The measures incorporated in the meter are summarized in Table 4.

**Table 4.** Preventive measures incorporated into the meter.

Vulnerabilities		Preventive built-in measures
1	Glass destruction, scratching	Possible (Metallic glass?)
2	Register perforation	Metallic tape

3	Cast perforation	Iron cast
4	Meter removal	Need for an additional security device
5	Register removal	Special screws
6	Inclination	Some meters are not affected
7	Wire through pipe	Possible (build-in anti-wire device)
8	Magnetism	Antimagnetic shields

## Preventive security devices

Preventive measures with security devices are intended to protect the meter, avoiding or making the tampering much more difficult. They also serve as an indicator in case of destruction of the device and the meter. In Peru, several devices have been found in use, which —contrary to indicative measures— have preference among operators due to the difficulty of sanctioning of tampering. The devices analyzed below represent an extension to previous evaluations (Ziemendorff, Vázquez, & Ruesta, 2015) (Figure 5).



**Figure 5.** Preventive devices: A) "Gauss" anchor; B) seals for the locknut; C) coating with cement; D) grids in the meter box; E) anti-wire cone; F) "Copa" anchor; G) anchor "Argolla"; H) anchor "Pulpo"; I) Anchor "Casco"; J) anchorage "Seguridad Total".

Based on the aforementioned vulnerabilities, the preventive security devices identified are:

- 1. Against the vulnerability of the glass (Vulnerability 1):** The only devices that have been found to protect the glass from scratching, perforating or hitting are the "Seguridad Total" and "Casco" devices (Figure 5, I and J). The first was developed by the Peruvian utility EPS GRAU (Ziemendorff *et al.*, 2015). The protection consists of a safety glass, reinforced with an acrylic glass. The other device was developed for the utility Sedapal (Servicio de Agua Potable y Alcantarillado de Lima) (Peru) and is called "Casco". Its mode of protection of the glass, consists of a thick metal helmet that prevents

access to the window, but also to reading. Therefore it has to be opened for reading with a special key.

- 2. Against the possibility of perforating the register from the side** (Vulnerability 2): The same two devices are the only ones that prevent this type of tampering, protecting the sides of the meter with a metal cast. The “Copa” and “Pulpo” devices could fulfill the same function, however they leave that part of the register without protection, where are the hinges of the meter cover fit (Figure 5, F and H; the arrows indicate the vulnerable part).
- 3. Against the possibility of perforating the cast** (Vulnerability 3): It only occurs in plastic cast meters, for which, due to its low use, no devices have been developed. The only form of protection is the coating of the meter with a cementitious mass, which presents practical problems (see below).
- 4. Against the withdrawal of the meter** (Vulnerability 4): Being this form of tampering frequent, all the devices analyzed, with the exception of the anti-wire device, fulfill this function.
- 5. Against the withdrawal of the register** (Vulnerability 5): The “Gauss” and “Argolla” devices do not fulfill this function, nor the seals mounted on the locknut, nor the anti-wire device (Figure 5, A, B, E, G), while the other do (Figure 5, F, H, I, J). In case of the grids (D) are so narrow that they not allowing the hands to be put in the meter box they also comply with it.
- 6. Against the inclination of the meter** (Vulnerability 6): The “Gauss” device, the seals on the locknut, the grids and the anti-wire



device do not fulfill this function (Figure 5, A, B, D, E), while others do comply (Figure 5, F, G, H, I, J).

**7. Against the accessibility of the turbine through the tube**

(Vulnerability 7): There is a device, which is mounted at the water outlet of the meter, called an anti-wire device (Figure 5, E). This lets the water pass, but not intrusive object to the meter. Theoretically, it is also feasible to mount a non-return valve, however its cost is much higher (USD 0.2 vs. USD 9 approx.).

**8. Against the use of magnets** (Vulnerability 8):

The only devices that provide effective security to the meter against the use of magnets, even if it does not have a built-in antimagnetic shield, are the “Casco” and “Seguridad Total” devices . This is because they increase the distance by which the magnet can be attached to the meter, and because they contain iron, which has an effect similar to the shields. Tests were performed using the same meters and magnets mentioned, putting both devices on top. The tests were carried out in Tarapoto, Peru (Ziemendorff, 2017) with the result that both devices only allow a small under-registration in meters without antimagnetic protection at the minimum flow rate and with the largest magnet (Table 5).

**Table 5.** Results of the tests of the antimagnetic protection provided by the “Seguridad Total” and “Casco” devices.

Magnet	Flow	Single Jet	Single Jet	Multi Jet	Multi Jet
--------	------	------------	------------	-----------	-----------

		rate	Without magnetic shield	With simple magnetic shield	With simple magnetic shield	With double magnetic shield
1	4.7 cm <sup>3</sup>	Q1	No effect	No effect	No effect	No effect
		Q2	No effect	No effect	No effect	No effect
		Q3	No effect	No effect	No effect	No effect
2	23.1 cm <sup>3</sup>	Q1	No effect	No effect	No effect	No effect
		Q2	No effect	No effect	No effect	No effect
		Q3	No effect	No effect	No effect	No effect
3	48.7 cm <sup>3</sup>	Q1	Under registration 15-25%	No effect	No effect	No effect
		Q2	No effect	No effect	No effect	No effect
		Q3	No effect	No effect	No effect	No effect

An under-registration of this magnitude does not justify the acquisition of a magnet by the fraudulent user. In summary, preventive measures with safety devices against meter tampering are in Table 6.

**Table 6.** Preventive measures with security devices against the tampering of meters according to their vulnerabilities.

Vulnerabilities	Preventive security devices					
	Device Gauss/ Locknut	Cement covering	Iron grid at meter box	Device Argolla	Devices Copa or Pulpo	Devices "Casco" or "Seguridad"

		seals					Total"
1	Glass destruction, scratching	Do not protect	Do not protect	Do not protect	Do not protect	Do not protect	Protect
2	Register perforation	Do not protect	Protect	Do not protect	Do not protect	Do not protect	Protect
3	Cast perforation	Do not protect	Protect	Do not protect	Do not protect	Do not protect	Do not protect
4	Meter removal	Protect	Protect	Protect	Protect	Protect	Protect
5	Register removal	Do not protect	Protect	Protect	Do not protect	Protect	Protect
6	Inclination	Do not protect	Protect	Protect	Protect	Protect	Protect
7	Wire through pipe	Do not protect	Do not protect	Do not protect	Protect	Do not protect	Do not protect
8	Magnetism	Do not protect	Do not protect	Do not protect	Do not protect	Do not protect	Protect

Additionally it is necessary to make some specifications about the different preventive measures:

**About the use of the "Gauss" anchor and the security seals that are installed in the meter locknut:** As shown in Table 6, these devices have the sole function of preventing or hindering the removal of the meter. Its installation can be a valid strategy in combination with meters with metal cast and antimagnetic shields, security seals and the anti-wire device in places where a user with a tampered meter is effectively sanctioned. Otherwise, one of the preventive devices "Casco"

or "Seguridad Total" is suggested. The easiest device to violate is the plastic one, which is why its use is not recommended in places where it is impossible to sanction if the seal is broken.

**About the coating of the meter with a cementitious mass:**

As shown in Table 6, this measure is quite effective in protecting the meter. However, its application revealed serious inconveniences, especially when there is a need to temporarily remove the meter. The removal is not only difficult, but also damages the accessories of the meter and may cause leakages.

**About the use of grids in the meter box:** Since the installation of the grids is expensive (more than USD 15) and provides little protection to the meter, all anchors presented are better options. In addition, the grids make it difficult to cut-off (suspend) the service.

**About the "Argolla", "Copa" and "Pulpo" anchors:** It is recommended to discard the "Argolla" anchor by allowing the register's removal from the meter. The anchors "Copa" and "Pulpo" can be a valid alternative as they protect meters that have antimagnetic shields and metallic casts. If the meters also have a protection against perforation of the register (such as the mentioned metal tape), they can be used as such, otherwise it is advisable to eliminate the vulnerability they present (Figure 5, F and H, red arrow), which consists of allowing access to register between the hinges of the meter cover. If all the aforementioned factors are actually given, the meter is still vulnerable

by the glass, so it is suggested to use the “Casco” or “Seguridad Total” devices if its visible violation cannot be sanctioned.

**About the use of the “Seguridad Total” and “Casco” devices:** Both devices (Figure 5, I and J) have been developed in Peru with the purpose of protecting the meter completely, but in places where no meter with plastic casts was used, so they were not designed to protect against this vulnerability. However, it is feasible to adapt them for this type of meter, although it would increase its cost, which is currently around USD 7 (with installation USD 10). For most meters (metal cast) they provide complete security if an anti-wire device is added (see next paragraph). The main difference between the two types of devices is the use of a special key for the “Casco” device, which represents an advantage because the meter can be removed and replaced without the need to disassemble the anchor. The technical specifications can be consulted in a tender of the operator of Lima, Peru (Sedapal, 2008). The disadvantage is that for Reading the meter it has to be opened with the same key, which also makes the key its main weakness. Therefore, if the use of the key cannot be restricted to a few people, the use of the “Seguridad Total” device is recommended (its design can be consulted by the author of this text). Both devices are anchored with quick-setting cement, with an operator seal on it, to evidence if the device were moved to tamper the meter.

**About the use of anti-wire device:** This device has the sole function of protecting the meter against the introduction of paralyzing objects such as wires through the pipe from the property-side. This function is

not fulfilled by another preventive or indicative device. It is a perfect complement to the other measures for cases where this vulnerability exists - that is that there are no obstacles between the interior installations of the user and the register that prevent the introduction of wires. The pressure loss due to the installation of the device is minimal - if it is fixed on a single jet meter below 0.45 bar and without it below 0.2 bar at flow rate  $Q_3$ . Unlike the plastic device in the photo (Figure 5, E) it is suggested that it be made of metal to prevent it from being perforated with hot objects.

## Discussion

In almost all locations in Latin America the meters are placed on public roads, accessible to whoever wants. This, although it facilitates its reading, presents a drawback: the simple fact that a meter is tampered or shows signs of having been tampered with (security seal broken for instance), cannot be easily attributed to the user who benefits from the tampering, unless he is seen in the act of tampering.

The difficulty of sanctioning the tampering leads to impunity, therefore, efforts have been undertaken to allow administrative or legal

sanctions, even in those cases where there is only evidence of the tampering, being able to attribute it in some way to the beneficiary of the tampering. In the case of Peru, for example, the regulations state that a tampered meter can be charged to the user if it occurs for the second time in five years.

Therefore, before choosing any of the presented alternatives, it is necessary to analyze whether it is feasible or not to apply effective sanctions for the tampering of the meter or of the security seals. It is important to make this differentiation because there are several forms of tampering leaving the seals broken, but that do not leave physical evidence on the meter (such as the application of magnets). In this case the indicative measures only indicate that immediate preventive measures should be taken.

Likewise, in case of not being able to effectively sanction the tampering, preventive measures must necessarily be applied. Regardless of the legal situation, it is important to take into account all the vulnerabilities of the meter, since, as shown (Ziemendorff *et al.*, 2015), the application of measures that only protect some of the vulnerabilities have the effect that the tampering pattern changes, without decreasing its quantity.

## Conclusions

1. Velocity meters have up to eight vulnerable points, where they can be tampered to avoid the correct measurement of water consumption.
2. There are different ways to detect and avoid these forms of tampering through indicative and preventive measures.
3. Indicative and preventive measures can be combined in such a way that adequate integral security is provided to the meter.
4. The specific application of these measures depends mainly on the possibility of sanctioning or not of the tampering of the meter or of the indicators (such as seals).

## **Recommendations**

1. To provide complete security, where there is difficulty with the effective sanctioning of tampering, the installation of “Casco” or “Seguridad Total” devices is suggested, being the first best when the use of special keys can be restricted. Both devices must be



complemented with an anti-wire device in the aforementioned cases. The use of plastic cast meters is not recommended.

2. To provide security to meters in places where there is the ease of sanctioning tampering, but as evidence only the physically tampered meter counts, it is recommended:
  - a) Use meters with antimagnetic protection, metal cast and whose register is protected against perforation from the side, combined with an anchor that does not allow the removal or inclination of the meter, and with an anti-wire device for the cases already described.
  - b) If the meters do not have these characteristics, it is better to use on of the "Casco" or "Seguridad Total" devices.
3. Where there is the possibility of sanctioning only with the indications of tampering, there are wide possibilities, such as:
  - a) Expansive foam combined with a magnetism indicator seal (if the meter does not have an antimagnetic shield) and the anti-wire device. Only then it is possible to use plastic cast meters without leaving vulnerabilities.
  - b) The meter can be secured against withdrawal, inclination and against removal of the register with seal wire and seals if the meter has a metal cast and has a register protection from the side. Magnetism indicator seals may be used additionally if the meter does not have an antimagnetic shield, also an anti-wire device.
  - c) It is equally feasible to use any strategy mentioned for the other legal situations, applying preventive measures although these are of higher cost.

## Acknowledgments

The author thanks Javier Marina and Luis Burel of EMAPA San Martín, Sain Mestanza and Candelario Chuquizuta of EMUSAP Amazonas, Fernando Carrasco and Gustavo Lindao of EPS Grau, who have carried out the tests described in their test benches; also to the companies Security Seals and A&G Industries and finally to the Swiss Cooperation (SECO) and the German development cooperation, GIZ / PROAGUA II, specifically to the AKUT Partner consultants, José Giménez, Oscar Perfecto, Raúl Cáceres, Julián Gonzales, Frank Vidalón, Melisa Pantoja and finally to Christoph Platzer for his contributions.

## References

- Arregui, F., Cabrera Jr., E., Cobacho, R., & García-Serra, J. (September, 2005). Key factors affecting water meter accuracy. *Proceedings Leakage 2005 Conference*, Halifax, Canada.
- García, E. (2019). Sedapal: robo de medidores de agua aumentó 92% en primeros cuatro meses del 2019 versus 2018. *Diario Gestión*, 20.05.2019.
- González, F., Val, R., Rocha, J., & Segundo, J. (2010). *Manual de selección, instalación y mantenimiento a medidores de agua fría*. Ciudad de México, México: Universidad Nacional Autónoma de México.

- Goodwin, R., Kaggwa, R., & Malebo, A. (2013). *Utility management series for small towns. Volume 6: Reduction of illegal water*. Nairobi, Kenia: The United Nations Human Settlements Programme (UN-Habitat).
- Ríos, S. (2013). *Guía para la detección de fraudes en suministros de energía eléctrica en medición directa*. Pereira, Colombia: Universidad Tecnológica de Pereira.
- Sedapal, Servicio de Agua Potable y Alcantarillado de Lima. (2008). *Licitación pública N° 0020-2008. Suministro de dispositivos de seguridad para medidores*. Lima: Servicio de Agua Potable y Alcantarillado de Lima.
- Ziemendorff, S., Vázquez, W., & Ruesta, H. (2015). La seguridad de medidores de agua potable contra robo, vandalización y manipulación. *Revista INDES*, 3(2), 5-15.
- Ziemendorff, S. (2017). *Informe: seguridad de medidores contra robo, manipulación y vandalización. La seguridad de medidores contra imanes*. Informe interno. Tarapoto, Perú: Secretaría de Estado de Suiza para la Economía (SECO), Gesellschaft für Internationale Zusammenarbeit- Agencia alemana para la Cooperación Internacional (GIZ), AKUT Partner.