CLAIMS

What we claim is:

1. A device for detection of unsanctioned implantation of a powerline communication module in a connected product, the device comprising:

   a controller;

   a signal generator and a current sensor, the signal generator is configured to generate a signal and a current sensor is configured to measure the electric current evolved from the generated signal;

   an AC-out connector configured to connect the device to the product;

   an AC-in connector configured to connect the device to the mains; and

   an analog front-end unit (AFE) configured to couple the signal generator and the current sensor to the AC-out connector.

2. The device of claim 1, further comprising an on/off switch, configured to control on-off state of the connected product.

3. The device of any one of claims 1-2, wherein the device further comprises a power line filter, configured to create a low noise and/or high impedance environment at an AC-out side of the device; wherein the power line filter is configured to operate at the frequency range of about 10KHz – 30MHz.

4. The device according to any one of claims 1-3, further comprising: a local database, a processing unit, a user interface (a command and control unit), a power supply, a network connection, or any combination thereof.

5. The device according to any one of claims 1-4, wherein the signal generator is configured to generate an output signal at a frequency range of about 10KHz – 30MHz.

6. The device according to any one of claims 1-5, wherein the current sensor is configured to measure current at a frequency range of an input signal at about 10KHz – 30MHz.

7. The device according to any one of claims 1-6, wherein coupling frequency of the input/output signal coupled by the AFE is in the range of about 10KHz – 30MHz.

8. The device of claim 1, wherein the measured electric current evolved from the generated signal is used to determine the impedance fingerprint of the product and/or

   wherein the fingerprint of the product is obtained at an off-state of the product and/or at an on-state of the product.

9. The device according to any one of claims 1-8, configured to execute a method for detection of unsanctioned implantation of a powerline communication module in the connected product, the method comprising comparing the impedance fingerprint of the connected product to a corresponding reference impedance fingerprint obtained from a corresponding trusted unmodified product.

10. A method for detection of unsanctioned implantation of a powerline communication module in a product, the method comprising:

    - obtaining an impedance fingerprint of an AC circuit of the product; and
    - comparing the impedance fingerprint of the product to an AC impedance circuit fingerprint of a trusted unmodified corresponding product (golden fingerprint);

    wherein a difference in values of the compared fingerprints is indicative of an unsanctioned implantation of a powerline communication module in the product.

11. The method of claim 10, wherein obtaining the impedance fingerprint comprises applying a signal on the product's AC circuit and measuring the evolved electric current and to create the impedance fingerprint; and/or

    wherein the frequency range of the signal is in the range of about 10KHz – 30MHz; and/or

    wherein the fingerprints are obtained at an off-state and/or an on-state of the product.

12. The method of any one of claims 10-11, wherein the golden fingerprint and/or the product fingerprint are created by applying a signal on the AC circuit of the trusted unmodified product and measuring the evolved electric current to create the golden fingerprint; and/or

    wherein the fingerprints are created on a server; or

    wherein the fingerprints are created in the device; and/or.

    wherein the golden fingerprint is obtained from a database.

13. The method of any one of claims 10-12, wherein the method further comprises storing the impedance fingerprint and/or the golden fingerprint on a database; and/or

    wherein the database is a local database of a detection device configured to be connected to the product and apply the signal on the product's AC circuit and measure the evolved electric current; or

    wherein the database is a network database connected to a server and/or

    wherein the creation of the fingerprint(s) is done on a server; or

    wherein the creation of the fingerprint(s) is performed by the device.

14. The method of any one of claims 10-13, wherein comparing between the fingerprints comprises loading the golden fingerprints, loading the impedance fingerprints of the product under test and comparing between the golden fingerprint and the impedance fingerprint of the product under test; and/or

    wherein the comparison process is performed in a server or by a detection device; and/or

    wherein comparing between the fingerprints further comprises saving and/or displaying the test results; and/or

    wherein the fingerprints are loaded from a network database connected to the server and/or from a local database within the detection device; and/or

    wherein the test results are saved on a local database and/or the network database; and/or

wherein the test results are displayed on a detection device and/or a network server.

15. A system for detection of unsanctioned implantation of a powerline communication module in a product under test, the system comprising:

a server and a database; and

a detection device comprising:

a controller;

a signal generator and a current sensor, the signal generator is configured to generate a signal and a current sensor is configured to measure the electric current evolved from the generated signal;

an AC-out connector configured to connect the device to the product;

an AC-in connector configured to connect the device to the mains; and

an analog front-end unit (AFE) configured to couple the signal generator and the current sensor to the AC-out connector.