are usually known as, for example, tamper seals, security seals, tamper evident security seals, security tapes, tamper evident tapes, plastic zip ties, or padlocks, which for the purpose of simplicity are herein referred to as “security seals” or “security devices.” In general, these security seals or devices are designed to be visually inspected and easily recognized if tampered with or broken. As an example, security seals or devices are utilized in commercial aircraft to help ensure that any items placed onto the aircraft have been cleared by the relevant security personnel, and once cleared, those items are sealed to make sure that they cannot be tampered with before, during and post flight.

Unfortunately, while useful, these types of security seals or devices require the relevant security personal or crew member to walk through the vehicle and visually, and possibly physically, inspect each security seal or device individually to see if it has been tampered. As a result, this leads to downtime of the vehicle and increased manual labor costs related to the physical inspection of all of the security seals or devices on the vehicle. Therefore, there is a need for a system and method that addresses the limitations of the known security seals and devices.

SUMMARY

An aspect of the disclosure provides a wireless tamper sensor comprising a transmitter; a receiver; a multi-layer probe having predetermined electrical characteristics; a processing device in signal communication with the multi-layer probe; and a power supply in signal communication with the transmitter and the processing device. The processing device includes a processor; and a computer-readable medium accessible to the processor, the computer-readable medium

storing instructions that are executable by the processor to initiate a tamper state of the wireless tamper sensor to untampered responsive to the wireless tamper sensor being armed by a user; detect a physical trigger on the multi-layer probe; set the tamper state to tampered in response to detecting the physical trigger; receive a wake command from an external device, wherein the user utilizes the external device to arm the wireless tamper sensor with the wake command; authenticate the wake command; and setting the tamper state to untampered responsive to the wake command being authenticated.

Another aspect of the disclosure provides a method for detecting tampering on a wireless tamper device. The method comprises arming the wireless tamper device by a user, wherein arming includes initiating a tamper state of the wireless tamper device to untampered; detecting a physical trigger on a multi-layer probe; setting the tamper state to tampered in response to detecting the physical trigger; receiving a wake command from an external device, wherein the user utilizes the external device to arm the wireless tamper device with the wake command; authenticating the wake command; and setting the tamper state to untampered responsive to the wake command being authenticated.

A wireless tamper device ("WTD") is disclosed. The WTD includes a transmitter, multi-layer probe, processing device, and power supply. The processing device is in signal communication with the multi-layer probe and the power supply is

CLAIMS

1. A wireless tamper sensor comprising:

a transmitter;

a receiver;

a multi-layer probe having predetermined electrical characteristics;

a processing device in signal communication with the multi-layer probe; and

a power supply in signal communication with the transmitter and the processing device, wherein the processing device includes:

a processor; and

a computer-readable medium accessible to the processor, the computer-readable medium storing instructions that are executable by the processor to:

initiate a tamper state of the wireless tamper sensor to untampered responsive to the wireless tamper sensor being armed by a user;

detect a physical trigger on the multi-layer probe;

set the tamper state to tampered in response to detecting the physical trigger;

receive a wake command from an external device, wherein the user utilizes the external device to arm the wireless tamper sensor with the wake command;

authenticate the wake command; and

setting the tamper state to untampered responsive to the wake command being authenticated.

2. The wireless tamper sensor of claim 1, further comprising an encapsulating material that encloses at least a portion of the wireless tamper sensor.

3. The wireless tamper sensor of claim 1, further comprising a trigger switch, wherein the trigger switch is configured to be armed by the user, and wherein the instructions are further executable by the processor to set the tamper state to untampered responsive to the trigger switch being activated.

4. The wireless tamper sensor of claim 1, wherein the multi-layer probe is an antenna having an antenna length, and wherein the physical trigger is a reduction of the antenna length.

5. The wireless tamper sensor of claim 1, wherein detecting the physical trigger on the multi-layer probe includes determining that the multi-layer probe has new electrical characteristics as a result of the physical trigger.

6. The wireless tamper sensor of claim 5, wherein the physical trigger is a separating of a layer of material within the multi-layer probe.

7. The wireless tamper sensor of claim 1, further comprising a sensor in signal communication with the processing device, wherein the sensor senses the physical trigger on the multi-layer probe.

8. The wireless tamper sensor of claim 1, wherein the instructions are further executable by the processor to transmit a tamper state signal in response to detecting the physical trigger, wherein the tamper state signal indicates that the tamper state is either tampered or untampered.

9. The wireless tamper sensor of claim 8, wherein the instructions are further executable by the processor to:

receive a status command from the external device;

authenticate the status command; and

transmit the tamper state signal in response to receiving the status command, wherein the tamper state signal indicates that the tamper state is either tampered or untampered.

10. The wireless tamper sensor of claim 1, further comprising an accelerometer, wherein detecting the physical trigger includes detecting a movement or vibration with the accelerometer.

11. The wireless tamper sensor of claim 10, wherein the instructions are further executable by the processor to:

receive a reset signal from the external device; and

reset the tamper state to untampered in response to receiving the reset signal.

12. The wireless tamper sensor of claim 1, wherein the processing device includes a field programmable-gate array.

13. A method for detecting tampering on a wireless tamper device, the method comprising:

arming the wireless tamper device by a user, wherein arming includes initiating a tamper state of the wireless tamper device to untampered;

detecting a physical trigger on a multi-layer probe;

setting the tamper state to tampered in response to detecting the physical trigger;

receiving a wake command from an external device, wherein the user utilizes the external device to arm the wireless tamper device with the wake command;

authenticating the wake command; and

setting the tamper state to untampered responsive to the wake command being authenticated.

14. The method of claim 13, further comprising transmitting a tamper state signal in response to detecting the physical trigger, wherein the tamper state signal indicates that the tamper state is tampered.

15. The method of claim 13, further comprising:

receiving a status command from the external device;

authenticate the status command; and

transmitting a tamper state signal in response to receiving the status command.

16. The method of claim 15, wherein detecting the physical trigger includes determining that the multi-layer probe has been broken or substantially altered.

17. The method of claim 16, wherein the multi-layer probe is an antenna.

18. The method of claim 14, wherein detecting the physical trigger includes detecting a movement or vibration with an accelerometer.

19. The method of claim 18, further comprising:

receiving a reset signal from the external device; and

resetting the tamper state to untampered.