CLAIMS

What is claimed is:

1. A method comprising:

receiving, by a wireless sensing system, sensor data from a sensor associated with an asset, the sensor data representing a tampering event of the asset; wherein the tampering event represents one or both of (1) a distance between a first tape node and a second tape node increasing past a threshold distance, and (2) a tear being detected in circuitry of a single tape node;

determining, by the wireless sensing system, whether the tampering event was authorized;

determining, by the wireless sensing system, whether the tampering event occurred at an authorized area; and

in response to one or both of: (1) the tampering event being unauthorized, and (2) the tampering event being performed within an unauthorized area, transmitting a notification of the tampering event to a mobile device wirelessly connected to the wireless sensing system.

2. The method of claim 1, wherein the tampering event occurred within an area of a storage container.

3. The method of claim 1, wherein determining, by the wireless sensing system, whether the tampering event is authorized comprises:

communicating, by a node of the wireless sensing system, the node attached to the asset, with a plurality of nodes attached to corresponding asset of a plurality of assets, the plurality of nodes tracking the plurality of assets;

receiving, by the node of the wireless sensing system, inventory of the plurality of nodes; and

transmitting, by the node of the wireless sensing system, an alert to other nodes attached to other assets in proximity of the asset, wherein the alert causes the other nodes to set a flag, indicative of the tampering event, at each of the plurality of nodes, the alert is a notification that a tampering event may have occurred.

4. The method of claim 3, wherein the flag, within each of the plurality of nodes,

is scannable by a user device.

5. The method of claim 1, wherein determining, by the wireless sensing system, whether the tampering event is authorized comprises:

communicating, by a node of the wireless sensing system, the node attached to the asset, with a user device associated with an authorized user; and

receiving, by the node of the wireless sensing system, an authorization key of the user device.

6. The method of claim 5, further comprising logging the received sensor data for the tampering event to a historical record of tampering records, each logged tampering event includes a set of corresponding sensor data.

7. The method of claim 5, wherein the user device is a smart phone, the method further comprising:

determining that the tampering event is authorized in response to receiving, by the node of the wireless sensing system, the authorization key of the user device.

8. The method of claim 5, wherein the user device is a badge that includes an RFID chip, the method further comprising:

determining that the tampering event is authorized in response to receiving, by the node of the wireless sensing system, the authorization key of the user device.

9. The method of claim 5, further comprising:

receiving, by the node of the wireless sensing system, from the user device, a wireless signal that sets a period of time that a tampering event shall not trigger the wireless sensing system.

10. The method of claim 1, wherein determining, by the wireless sensing system, whether the tampering event occurred within an authorized area comprises:

receiving, from a local node of the wireless sensing system that is attached to the asset, a current location of the asset; and

determining whether the current location of the asset is within the authorized area.

11. The method of claim 10, wherein the local node of the wireless sensing system determines the current location of the asset is within the authorized area, the method further comprising:

disabling, by the local node, some functionality of the local node to save battery life of the local node.

12. The method of claim 1, wherein a server is associated with the wireless sensing system, and wherein the receiving sensor data, the determining whether the tampering event was authorized, the determining whether the tampering event occurred at an authorized area, and the transmitting the notification of the tampering event to a device registered with the wireless sensing system, are all performed by a server of the wireless sensing system.

13. A wireless sensing system having a network of wireless nodes, comprising,

at least one processor; and

non-transitory memory communicatively coupled with the at least one processor and storing machine-readable instructions that, when executed by the processor, cause the processor to:

receive sensor data from a sensor associated with an asset, the sensor data representing a tampering event of the asset, wherein the tampering event represents one or both of (1) a distance between a first tape node and a second tape node increasing past a threshold distance, and (2) a tear being detected in circuitry of a single tape node;

determine whether the tampering event was authorized; and

in response to the tampering event being unauthorized, transmit a notification of the tampering event to a mobile device wireless connected to the wireless sensing system.

14. The wireless sensing system of claim 13, the non-transitory memory storing further machine-readable instructions that, when executed by the processor, further cause the processor to:

determine whether the tampering event occurred within an authorized area; and

in response to the tampering event occurring outside of the authorized area, transmit the notification.

15. The wireless sensing system of claim 14, wherein said determine, by the wireless sensing system, whether the tampering event occurred within an authorized area comprises:

receive, via the wireless sensing system and from a local node attached to the asset, a

current location of the asset; and

determine whether the current location of the asset is within the authorized area.

16. The wireless sensing system of claim 13, the non-transitory memory storing further machine-readable instructions that, when executed by the processor, further cause the processor to: scan for one or more wireless nodes; store scan results indicating current wireless nodes responding to the scan; compare the scan results to a logistics schedule; and transmit a logistics alert when the scan results do not correspond to the logistics schedule.

17. A wireless sensing system having a primary electronic logging device (ELD) and a secondary ELD,

the secondary ELD comprising:

at least one processor; and

a memory communicatively coupled with the at least one processor and storing machine-readable instructions that, when executed by the processor, cause the processor to:

receive tape node data from a tape node associated with an asset proximate to the secondary ELD, the tape node data representing a tampering event performed on the asset;

compare the tape node data to a list of predetermined events, stored within the memory, the list of predetermined events includes one or more predetermined events and corresponding elements of tape node data associated with each of the one or more predetermined events;

determine, based on the comparison of the tape node data to a list of predetermined events, that the tampering event does not match a predetermined event within the list of predetermined events; and

execute, in response to the determination that the tampering event does not match a predetermined event, a particular contingency plan, based on the tampering event.

18. The wireless sensing system of claim 17, wherein the non-transitory computer readable instructions further causes the processor to:

when the tampering event is not a predetermined event, retrieve, from a plurality of wireless nodes associated with the asset, data relating to the tampering event;

broadcast data, according to the particular contingency plan, to the plurality of wireless nodes associated with the asset; and

transmit a notification, to the primary ELD of the wireless sensing system, to notify a management system of the wireless sensing system, the notification alerting the management system of the wireless sensing system that the tampering event has occurred.

19. The wireless sensing system of claim 18, wherein transmitting the notification further includes transmitting to a client device, the notification alerting an authorized user of the client device.

20. The wireless sensing system of claim 17, wherein said execute the particular contingency plan further comprises the memory including further non-transitory computer-

readable instructions that, when executed by the processor, further cause the secondary ELD to:

identify the contingency plan as a particular contingency plan, from a set of contingency plans, satisfying a threshold, comprising:

compare the tampering event to a set of contingency plans stored in the memory;

determine, based on the comparison of the tampering event with the contingency plan satisfying a threshold, a particular contingency plan; and

execute instructions contained within the particular contingency plan.

21. The wireless sensing system of claim 20, the wireless sensing system further includes a peripheral wireless network node that is associated with a missing asset, wirelessly connected to the secondary ELD, and proximate to the asset, wherein the tampering event is a missing asset, and the particular contingency plan includes instructions for wireless sensing system to re-broadcast ping packets to the peripheral wireless network node associated with the missing asset using a different communications protocol.

22. The wireless sensing system of claim 17, wherein the primary ELD is the tape node designed to wirelessly communicate using Bluetooth, LoRa, Cellular, and GPS.

23. The wireless sensing system of claim 17, wherein the primary ELD is another tape node than the tape node and the primary ELD has increased storage capacity, battery, and processing power than the tape node.

24. The wireless sensing system of claim 17, wherein the tampering event occurred on a storage container.