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 ~~stored alert~~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 the sensor data includes one or more of: vibration data, optical data, acoustic data, temperature data, orientation data, pressure data, altitude data, biometric data, humidity data, radioactivity data, and chemical data.~~

~~13. The method of claim 1, wherein the sensor includes a capacitive sensor, an altimeter, a gyroscope, an accelerometer, a temperature sensor, a strain sensor, a pressure sensor, a piezoelectric sensor, a weight sensor, an optical sensor, an acoustic sensor, a smoke detector, a radioactivity sensor, a chemical sensor, a biosensor, a magnetic sensor, an electromagnetic field sensor, and a humidity sensor.~~

~~14. The method of claim 1, wherein a wireless node of the wireless sensing system is attached to the asset, 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 the wireless node.~~

~~15~~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.

~~16~~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.

~~, at the wireless sensing system, a signal from a recently-activated wireless node of the network of wireless nodes; and~~

~~add, to a database and according to a classification of the recently-activated wireless node, an identifier of the recently-activated wireless node to indicate that the recently-activated wireless node has joined the network of wireless nodes~~.

~~17~~14. The wireless sensing system of claim ~~16~~13, the non-transitory memory storing further machine-readable instructions that, when executed by the processor, further cause the processor to:

~~receive, via the wireless sensing system, sensor data from a sensor associated with an asset, the sensor data representing a tampering event of the asset;~~

~~determine whether the tampering event was authorized;~~

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

in response to ~~one or both of: (1)~~ the tampering event occurring outside of the authorized area, transmit the notification.~~is unauthorized, and (2) the tampering event is not~~

~~performed within the authorized area, transmit a notification indicating the tampering event to a mobile device wirelessly connected to the wireless sensing system.~~

~~18. The wireless sensing system of claim 17, wherein the sensor includes a capacitive sensor, an altimeter, a gyroscope, an accelerometer, a temperature sensor, a strain sensor, a pressure sensor, a piezoelectric sensor, a weight sensor, an optical sensor, an acoustic sensor, a smoke detector, a radioactivity sensor, a chemical sensor, a biosensor, a magnetic sensor, an electromagnetic field sensor, and a humidity sensor.~~

~~19. The wireless sensing system of claim 17, wherein the sensor data includes one or more of: vibration data, optical data, acoustic data, temperature data, orientation data, pressure data, altitude data, biometric data, humidity data, radioactivity data, and chemical data.~~

~~20. The wireless sensing system of claim 17, wherein said determine, based on the sensor data, whether the tampering event was authorized comprises further machine-readable instructions that, when executed by the processor, cause the processor to:~~

~~communicate, by a node of the wireless sensing system, the node attached to the~~

~~asset, with a user device associated with an authorized user; and~~

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

~~21~~15. The wireless sensing system of claim ~~17~~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.

~~22. The wireless sensing system er of claim 17, wherein said receive sensor data, said determine whether the tampering event was authorized, said determine whether the tampering event occurred within the authorized area, and said transmit a notification are performed by a wireless node of the wireless sensing system, wherein the memory storing further machine-readable instructions that, when executed by the processor, further causes the processor to:~~

~~store, by the wireless sensing system, information describing the tampering event.~~

~~23. The wireless sensing system of claim 17, wherein a wireless node of the network of wireless nodes is attached to the asset, and wherein the receiving sensor data, said determine whether the tampering event was authorized, said determine whether the tampering event occurred at an authorized area, and said transmit the notification of the tampering event to a device registered with the wireless sensing system, are all performed by the wireless node.~~

~~24. The wireless sensing system of claim 16, a classification defining a communication capability of the recently-activated wireless node and being one of a plurality of classifications each defining different communication capabilities of a wireless communication interface of each wireless node in the network of wireless nodes.~~

~~25. A method for operating a wireless sensing system including: a first tape node attached to a first parcel, the first tape node having a first type of wireless communication interface and a second type of wireless communication interface having a longer range than the first type of wireless communication interface, and a second tape node capable of communicating with the first tape node, the method comprising:~~

~~establishing, by a server, a wireless communication connection with the second type of wireless communication interface of the first tape node; and~~

~~designating, by the server, the first tape node as a master node of the second tape node.~~

~~26. The method of claim 25, the wireless sensing system further including a third tape node operable to communicate with the first tape node and the second tape node, the method further comprising:~~

~~creating a hierarchical structure for a communications network, comprising at least the first, second, and third tape nodes defined by one or more factors; and~~

~~assigning the first, second, and third tape nodes to various levels of the communications network based on a classification for each of the first, second, and third nodes, according to the one or more factors.~~

~~27. The method of claim 26, wherein creating the hierarchical structure of the communications network further includes utilizing one or more of a neural network, artificial intelligence method, and a machine learning computing systems.~~

~~28. The method of claim 26, wherein the second and third tape nodes are each attached to opposing doors of a storage container, the method further comprising:~~

~~measuring, by one of the second and third tape nodes, a change in distance between the second and third tape nodes; and~~

~~transmitting, by one of the second and third tape nodes, an alert that a tampering event is occurring, in response to the change in distance between the second and third tape nodes satisfying a threshold.~~

~~29. The method of claim 26, wherein the wireless sensing system further comprises one or more sensors, wherein the one or more sensors are at least a vibration sensor for detecting tampering that causes an increase of vibration compared to background vibration levels.~~

~~30~~17. A wireless sensing system having a primary electronic logging device (ELD) and a secondary ELD, ~~comprising:~~

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.

~~31. The wireless sensing system of claim 30, wherein the memory further causes the secondary ELD to determine whether the tampering event can be resolved locally.~~

~~32~~18. The wireless sensing system of claim ~~30~~17, wherein the non-transitory computer readable instructions ~~memory~~ 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.

~~33~~19. The wireless sensing system of claim ~~32~~18, wherein transmitting the notification further includes transmitting to a client device, the notification alerting an authorized user of the client device.

~~34. The wireless sensing system of claim 30, wherein the memory further causes the processor to transmit a request for assistance from the primary ELD.~~

~~35. The wireless sensing system of claim 30, wherein the tampering event may be one of an improper asset, unfit asset, missing asset, and misrouted asset.~~

~~36. The wireless sensing system of claim 30, wherein the primary ELD is proximate to the secondary ELD, both of which are within a same vehicle.~~

~~37~~20. The wireless sensing system of claim ~~30~~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.

~~38~~21. The wireless sensing system of claim ~~37~~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.

~~39. The wireless sensing system of claim 37, wherein the tampering event cannot be resolved locally, further comprising the memory including further computer-readable instructions that, when executed by the processor, further cause the secondary ELD to send the primary ELD a request for an outside contingency plan.~~

~~40~~22. The wireless sensing system of claim ~~30~~17, wherein the primary ELD is the tape node designed to wirelessly communicate using Bluetooth, LoRa, Cellular, and GPS.

~~41~~23. The wireless sensing system of claim ~~30~~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.

~~42~~24. The wireless sensing system of claim ~~30~~17, wherein the tampering event occurred on a storage container.