(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2013 (07.02.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/019595 A2

(51) International Patent Classification:
G06F 21/02 (2006.01)

(21) International Application Number:
PCT/US2012/048477

(22) International Filing Date:
27 July 2012 (27.07.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2747342 29 July 2011 (29.07.2011) CA

(71) Applicant *(for all designated States except US)*: **ITRON, INC.** [US/US]; 2111 N. Molter Road, Liberty Lake, Washington 99019 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JOHNSON, Matthew** [US/US]; 3531 West Excell Lane, Spokane, Washington 99208 (US). **OSTERLOH, Christopher, L.** [US/US]; 9106 Wilton Bridge Road, Waseca, Minnesota 56093 (US).

(74) Agent: **MOOSE, Richard, M.**; Dority & Manning, P.A., P O Box 1449, Greenville, South Carolina 29602-1449 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

WO 2013/019595 A2

(54) Title: PROVIDING SECURITY TRACEABILITY OF CHANGES IN ENDPOINT PROGRAMMING THROUGH AUDITING

(57) Abstract: The present subject matter is directed to methodologies, devices and systems for providing enhanced tamper detection in AMR/AMI systems. A consumption sensing meter has associated therewith an endpoint device. The endpoint device is configured to increment a tamper counter upon detection of various events including, such as, metrology and non-metrology programming events. A count of detected tamper events is conveyed to a head end device within the system is compared with a known count representing authorized programming events and an alarm is generated if the reported count and known count do not match.

TITLE: PROVIDING SECURITY TRACEABILITY OF CHANGES IN ENDPOINT PROGRAMMING THROUGH AUDITING

FIELD OF THE SUBJECT MATTER

[0001] The present subject matter relates to information exchange in a wireless network of devices capable of exchanging information. More particularly, the present subject matter relates to improvements in tamper detection within a network of metrology devices with AMI capabilities.

BACKGROUND OF THE SUBJECT MATTER

[0002] A number of parameters programmed into utility meter endpoints affect the calculation of consumption and thus the amount billed to the customer and the revenue collected by the utility. Other programmed parameters may affect the performance of the endpoint and, if misprogrammed, can even reduce the battery life of battery-powered endpoints. Therefore, it would be advantageous to insure that no unauthorized changes are made to its meters that will affect either performance or revenue.

[0003] While there are many ways of controlling information and access to the equipment required for programming, there are still ways for rouge programming to occur (whether through an intentional act or otherwise inadvertently). Some utilities choose to use event logging and monitoring to identify actual or potential security issues in their IT infrastructure. Such approach allows the central correlation of events created by multiple systems to see if events across the IT infrastructure match as they should or if instead they indicate that a possible security event has occurred.

[0004] To facilitate such event logging architecture, all elements of the involved solution that generate relevant events must report those events up to the event logging system, and intermediate nodes (such as Handheld (HH), Mobile Collection (MC) and Fixed Network systems) must in turn pass such information up to and through their respective head-end systems to the event logging servers.

[0005] While programming devices and servers have records of the intended programming and results which are passed up in various file formats, such as XML, the messaging capability of endpoints is sometimes to an extent relatively limited. Event reporting fits most closely with the status reporting that is embodied in tampers.

[0006] Traditional tamper reporting in consumption messages, such as the standard consumption message (SCM), are generally relatively limited to a few (4) bits split into two 2 bit fields. Contemporary metering scenarios also tend to require more tamper/status information than traditional meters to support the needs of conservation, security, and system integrity functions within an AMI system. There are fundamentally too few bits in such scenario to support event reporting. Under a network, it might be possible to map reprogramming into one of the bits that times out, that is, clears itself, after a span of time, since the network is always listening to the endpoints, but such an approach is problematic for HH and MC systems when, for example, the endpoint is read once a month or less frequently.

[0007] The following patent documents are examples of prior publications relating to meter communications: US Patent No. 4,614,945 to Brunius, et al., entitled "Automatic/remote RF instrument reading method and apparatus;" US Patent No. 5,673,252 to Johnson, et al., entitled "Communications protocol for remote data generating stations; US Patent No. 6,218,995 to Higgins, et al., entitled "Telemetry antenna system;" US Patent No. 6,262,685 to Welch, et al., entitled "Passive radiator;" US Patent No. 7,079,962 to Cornwall, et al., entitled "Automated utility meter reading system with variable bandwidth receiver;" and US Patent No. 7,830,874 to Cornwall, et al., entitled "Versatile radio packeting for automatic meter reading systems."

[0008] In view of such concerns, it would be advantageous, therefore, to provide additional methodologies for examining a wider range of possible tamper instances; however, to date, no integrated technology has provided all of the advantages and capabilities for tamper detection and analysis as hereinafter described.

SUMMARY OF THE SUBJECT MATTER

[0009] In view of the recognized features encountered in the prior art and addressed by the present subject matter, improved methodology and apparatus are provided for providing enhanced tamper detection functionalities within an AMR/AMI environment. In accordance with the present subject matter, such improvements may be provided by way of a flexible data structure and associated data analysis within a network of metrology devices with AMI capabilities.

[0010] The present subject matter relates to methods for providing enhanced tamper detection functionalities in an advanced metering infrastructure. One present exemplary method provides a data structure including at least one field configured to convey a tamper count. In such methods, the tamper count may be compared to a known count and an alarm may be issued when the tamper count fails to match the known count.

[0011] In selected embodiments, the known count may correspond to a count of authorized programming events and, in particular embodiments, to a count of authorized metrology programming events.

[0012] Per some exemplary embodiments, the at least one field may correspond to at least one byte. In particular embodiments, at least one second field configured to convey a second tamper count may be provided.

[0013] In some present exemplary method embodiments, the tamper count may be incremented in response to programming events for an associated meter. In certain such embodiments, the programming events may comprise metrology programming events.

[0014] In certain of such exemplary method embodiments, the subject data structure may include separate counts for metrology-related and non-metrology related programming.

[0015] In other present alternative exemplary embodiments, the method comparing step may include comparing the tamper count with a record of associated work orders.

[0016] In addition to methodologies, the present subject matter equally relates to various and corresponding systems (such as AMR systems) and to various

embodiments of metrology devices and associated technologies, such as endpoint devices.

[0017] The present subject matter in some present exemplary embodiments may relate to an automatic meter reading (AMR) system including a consumption sensing meter having an associated endpoint device and a head end device. In such exemplary embodiments, the endpoint device may be configured to transmit signals using a data structure including at least one field configured to convey a tamper count, while an associated head end device may be configured to receive the signals and to compare the tamper count to a known count. In such embodiments, such head end device may be further configured to issue an alarm when the tamper count fails to match the known count.

[0018] In various alternative embodiments of such present systems, the tamper count may be incremented in response to programming events for the meter. In some of such alternatives, the programming events may comprise metrology programming events.

[0019] In other exemplary embodiments, the system may also include a portable programming device configured to receive the signals and to transmit the tamper count to the associated head end device. In particular such embodiments, the portable programming device may be a handheld device.

[0020] In certain other exemplary embodiments, the known count may correspond to a count of authorized programming events, and, in particular to a count of authorized metrology programming events. In selected of such embodiments, the at least one field may correspond to at least one byte. In yet further embodiments, the endpoint may be further configured to transmit signals using a data structure including at least one second field configured to convey a second tamper count.

[0021] In other present exemplary system embodiments, such data structure may include separate counts for metrology-related and non-metrology related programming.

[0022] In still further present alternative exemplary system embodiments, such head end device may be configured to compare such tamper count with a record of associated work orders.

[0023] In yet still further exemplary embodiments, the present subject matter relates to a metrology device including a consumption sensing meter and an associated endpoint device. In such exemplary embodiments, the endpoint device may be configured to transmit signals using a data structure including at least one field configured to convey a tamper count while the endpoint device may be configured to respond to programming events by incrementing the tamper count.

[0024] In particular such exemplary embodiments, the endpoint device may be configured to respond to metrology programming events.

[0025] In still further exemplary embodiments, the endpoint device may be configured to transmit signals using a data structure including at least one second field configured to convey a second tamper count. In certain of such further exemplary embodiments, such data structure may include separate counts for metrology-related and non-metrology related programming.

[0026] In still further alternative present exemplary embodiments, such metrology device may further be associated with a head end device configured to receive such tamper count, to compare such tamper count with associated work order data, and to issue an alarm for further investigation if such comparison does not match.

[0027] Additional objects and advantages of the present subject matter are set forth in, or will be apparent to, those of ordinary skill in the art from the detailed description herein. Also, it should be further appreciated that modifications and variations to the specifically illustrated, referred and discussed features, elements, and steps hereof may be practiced in various embodiments and uses of the subject matter without departing from the spirit and scope of the subject matter. Variations may include, but are not limited to, substitution of equivalent means, features, or steps for those illustrated, referenced, or discussed, and the functional, operational, or positional reversal of various parts, features, steps, or the like.

[0028] Still further, it is to be understood that different embodiments, as well as different presently preferred embodiments, of the present subject matter may include various combinations or configurations of presently disclosed features, steps, or elements, or their equivalents (including combinations of features, parts, or steps or configurations thereof not expressly shown in the figures or stated in the detailed description of such figures). Additional embodiments of the present

subject matter, not necessarily expressed in the summarized section, may include and incorporate various combinations of aspects of features, components, or steps referenced in the summarized objects above, and/or other features, components, or steps as otherwise discussed in this application. Those of ordinary skill in the art will better appreciate the features and aspects of such embodiments, and others, upon review of the remainder of the specification.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] A full and enabling disclosure of the present subject matter, including the best mode thereof, directed to one of ordinary skill in the art, is set forth in the specification, which makes reference to the appended figures, in which:

[0030] Figure 1 illustrates the format of an exemplary legacy SCM consumption message;

[0031] Figure 2 illustrates an exemplary format of an exemplary SCM+ message format in accordance with the present disclosure;

[0032] Figure 3 illustrates an exemplary tamper field mapping of bytes within the exemplary SCM+ message format illustrated in present Figure 2 such as may be used in an exemplary gas endpoint in accordance with the present disclosure;

[0033] Figure 4 is a diagram illustrating an exemplary architecture of a system constructed in accordance with present technology; and

[0034] Figure 5 is a flow chart of an exemplary method for determining the presence of programming tampering within an endpoint, in accordance with the present disclosure.

[0035] Repeat use of reference characters throughout the present specification and appended drawings is intended to represent same or analogous features, elements, or steps of the present subject matter.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0036] As discussed in the Summary section, the present subject matter is particularly concerned with methodologies for providing enhanced communications functionalities within an AMR/AMI environment, and, more particularly, with

providing methods for detection of various forms of endpoint tampering. and corresponding apparatus and device subject matter. With initial reference to Figure 1, there is illustrated the format generally 100 of a legacy standard consumption message (SCM). Traditional tamper reporting in consumption messages, such as the SCM message, have been typically limited, for example, to a few (4) bits split into two 2 bit fields. Contemporary metering scenarios, on the other hand, often can lead to a desire for more tamper/status information than available through traditional meters in order, for example, to desirably support the needs of conservation, security and system integrity functions within an AMI system. In legacy consumption messages such as illustrated in Figure 1, the two bit fields illustrated as tamper counter fields, i.e., field #5 and field #7, can be used as 2 bit counters or status flags. Of course, providing only 2 bits provides a rather limited count range of only 0 to 3, as well understood by those of ordinary skill in the art.

[0037] With present reference to subject Figure 2, there is illustrated an exemplary format generally 200 of an enhanced standard consumption message herein after noted as an "SCM+" message provided in accordance with present disclosure. By expanding the length of the tamper fields presently illustrated as field #7 and field #8 of exemplary representative format 200, to 2 bytes instead of 4 bits, several improvements can be made over the prior art. For example, in order to better support event logging, metrology and non-metrology tamper counters may be added to the expanded tamper fields in the SCM+ message to track each metrology-related and non-metrology-related reprogramming of the endpoint.

[0038] Such tamper counters become part of the message that is transmitted by the endpoint and received by a reading system. Head-end systems may be configured to compare the reported tamper counters with previous values to identify, for example, programming changes. Any identified changes can be compared with known work orders to audit or verify the validity of the reprogramming.

[0039] By using tamper counters as opposed to a simple flag, the number of changes can be tracked even using Handheld or Mobile collection without having to rely exclusively on the network to constantly monitor for such tampers.

[0040] Applications that may take advantage of tamper monitoring methodologies in accordance with present disclosure include, but are not limited to, counting reprogramming events between an endpoint and a programming device that can be used with auditing software on head-end systems to determine if unauthorized reprogramming has occurred, separately counting metrology-related programming from non-metrology related programming, and adding previously unflagged events such as, but not limited to, low battery indication.

[0041] In addition to the flexibility accorded with expanded tampers and endpoint type fields, those of ordinary skill in the art will appreciate that contemporary endpoints often may be generally configured to include two-way communications capability, unlike the majority of legacy endpoints employing prior SCM communications protocols, which were more often one-way devices. Coupling such two-way capability to the expanded tampers enables an endpoint to set one of the additionally available flags in the present exemplary SCM+ message to indicate to a collection device that it has additional information to report. Such associated collection device can then request from the endpoint the additional tamper/status information. Such presently disclosed subject matter greatly expands, beyond the newly expanded 2 byte fields, the number of possible conditions the endpoint can report to a collection system, such that rarely expected events or conditions can still be reported without disadvantageously having to dedicate capacity for reports in a bubble-up SCM+ message. Such ability to keep expanded tamper information outside of the base SCM+ message also keeps on-the-air packet length as short as possible to increase aggregate channel capacity and reduce susceptibility to interference.

[0042] With present reference to Figure 3, there is illustrated an exemplary tamper field mapping generally 300 of bytes within the presently disclosed SCM+ message format generally 200 as illustrated in present Figure 2 as may be used for communications exchanges from, for example, a gas endpoint. It is to be understood by those of ordinary skill in the art that the present technology is equally applicable to metering of various, different utilities. As may be observed, several types of tamper signals may be provided including those generated resulting from magnetic tampering as well as tilt tampering. In accordance with the present disclosure, other exemplary types of tampering including variations in

metrology and non-metrology program count may also be detected as previously noted. In addition, a spare flag F, that generally will have a value of zero, may also be included for future use (such as future added or future developed types of indications).

[0043] With present reference to Figure 4, there is illustrated a diagram generally 400 showing an exemplary architecture of a system constructed in accordance with present technology. As illustrated in present Figure 4, requests for work orders flow from the utilities CIS 402 and work orders systems 404 down to crews with programming devices, such as handheld computer 406 or laptop computer (not separately illustrated) with attached radio or other interfaces to the meter endpoints (not separately illustrated) to facilitate a connection to the meter 408 for programming.

[0044] A file logging the results of the programming is saved within the programming device after completion of the programming and is either transmitted back to the utility at that time or later when the worker returns to a utility facility and can connect to the IT network and download the logs.

[0045] During endpoint programming, the reprogramming tampers in the endpoint are appropriately incremented based on the number and type of parameters that are changed. The tampers transmitted in the SCM+ message are set to match these changes and are reflected in all subsequent SCM+ transmissions, until another programming occurs in the future.

[0046] The collectors, for example handheld collector 410, that read the meter 408 record the SCM+ message and include the tamper fields in the files that report to their corresponding head-end systems. Those head-end systems may look for a change in reprogramming tampers and create an event to send to the event logging system 412 or they may export all tampers to the Event Log Monitoring system(s) at the utility where the event logs from various systems are compare and correlated to identify unmatched or otherwise exceptional events that might indicate some form of security breach. Such potential breaches are reported so the appropriate IT security personnel can be notified and any appropriate investigations can be performed.

[0047] While many possible methods of assembling, correlating, and identifying anomalous events would occur to those of ordinary skill in view of the present

disclosure, an exemplary such methodology is illustrated in flow chart generally 500 as illustrated in Figure 5. With reference to present Figure 5, is will be noticed that a determination of an alarm condition signifying, for example, an unauthorized programming event, may be made by first receiving at step 502 tamper reprogramming event counts from the data collection system. A determination is made at step 504 as to whether a tamper has been detected.

[0048] If no tamper has been detected, the decision flow returns to step 502. If, on the other hand, a tamper has been detected, instructions are given to compare the tamper to previous work orders at step 506. If, when compared in step 508, the work orders and tampers match thereby signifying occurrence of authorized programming, the decision flow again returns to step 502. If, however, the work order and tampers do not match, an alarm may be generated at step 510 and passed from, for example, event log monitor 412 (Fig. 4) to appropriate personnel for action.

[0049] As should be appreciated from discussion herein above, tampering detected in accordance with present technology may be indicative of a large variety of events including, without limitation, metrology as well as non-metrology events. Thus, the present technology may be used to detect unauthorized programming of a meter via attempts to alter both metering and non-metering functions related to, for example, meter 408 as well as more common forms of tampering including use of magnetic fields and attempted movement of the meter.

[0050] While the present subject matter has been described in detail with respect to specific embodiments thereof, it will be appreciated that those skilled in the art, upon attaining an understanding of the foregoing may readily produce alterations to, variations of, and equivalents to such embodiments. Accordingly, the scope of the present disclosure is by way of example rather than by way of limitation, and the subject disclosure is not intended to preclude inclusion of such modifications, variations, and/or additions to the present subject matter as would be readily apparent to one of ordinary skill in the art.

WHAT IS CLAIMED IS:

1. A method for providing enhanced tamper detection functionalities in an advanced metering infrastructure, comprising:

configuring a data structure to include at least one field configured to convey a tamper count;

comparing the tamper count to a known count; and

issuing an alarm when the tamper count fails to match the known count.

2. A method as in claim 1, wherein the known count corresponds to a count of authorized programming events.

3. A method as in claim 1, wherein the known count corresponds to a count of authorized metrology programming events.

4. A method as in claim 1, wherein the at least one field corresponds to at least one byte.

5. A method as in claim 1, further comprising at least one second field configured to convey a second tamper count.

6. A method as in claim 1, wherein the tamper count is incremented in response to programming events for an associated endpoint.

7. A method as in claim 6, wherein the programming events comprise metrology programming events.

8. A method as in claim 1, wherein the data structure includes separate counts for metrology-related and non-metrology related programming.

9. A method as in claim 1, wherein the comparing includes comparing the tamper count with a record of associated work orders.

10. An automatic meter reading (AMR) system, comprising:

a consumption sensing meter;

an endpoint device associated with said meter, said endpoint device configured to transmit signals using a data structure including at least one field configured to convey a tamper count; and

a head end device configured to receive said signals and to compare the tamper count to a known count,

wherein said head end device is further configured to issue an alarm when the tamper count fails to match the known count.

11. A system as in claim 10, further comprising a portable programming device configured to receive said signals and to transmit said tamper count to said head end device.

12. A system as in claim 11, wherein said portable device is a handheld device.

13. A system as in claim 10, wherein the known count corresponds to a count of authorized programming events.

14. A system as in claim 10, wherein the known count corresponds to a count of authorized metrology programming events.

15. A system as in claim 10, wherein the at least one field corresponds to at least one byte.

16. A system as in claim 10, wherein said tamper count is incremented in response to programming events for said endpoint device.

17. A system as in claim 16, wherein said programming events comprise metrology programming events.

18. A system as in claim 10, wherein the endpoint device is further configured to transmit signals using a data structure including at least one second field configured to convey a second tamper count.

19. A system as in claim 10, wherein said data structure includes separate counts for metrology-related and non-metrology related programming.

20. A system as in claim 10, wherein said head end device is configured to compare said tamper count with a record of associated work orders.

21. A metrology device, comprising:

a consumption sensing meter; and

an endpoint device associated with said meter, said endpoint device configured to transmit signals using a data structure including at least one field configured to convey a tamper count;

wherein said endpoint end device is configured to respond to programming events by incrementing said tamper count.

22. A metrology device as in claim 21, wherein said endpoint device is configured to respond to metrology programming events.

23. A metrology device as in claim 21, wherein said endpoint device is configured to transmit signals using a data structure including at least one second field configured to convey a second tamper count.

24. A metrology device as in claim 23, wherein said data structure includes separate counts for metrology-related and non-metrology related programming.

25. A metrology device as in claim 21, further including an associated head end device configured to receive said tamper count, to compare said tamper count with associated work order data, and to issue an alarm for further investigation if such comparison does not match.

100

FIELD #	BITS	VALUE(HEX)	DESCRIPTION
1	20	F9530	Preamble
2	1	0	Preamble (extension)
3	2	x	ERT ID (Upper 2 Bits)
4	1	x	Spare Bit (Repeater)
5	2	x	Tamper 1 Count
6	4	x	Endpoint Type
7	2	x	Tamper 2 Count
8	24	xxxxxx	Consumption (Adjusted)
9	24	xxxxxx	ERT ID (Lower 24 Bits)
10	16	xxxx	CRC Checksum

FIG. 1

200

FIELD #	BYTES	VALUE(HEX)	DESCRIPTION
1	1	55	Preamble
2	2	16A3	Frame Sync
3	1	1E	Protocol ID
4	1	xx	Endpoint Type
5	4	xxxxxxxx	Endpoint Serial Number
6	4	xxxxxxx	Current Consumption
7	1	xx	Tamper Count 1
8	1	xx	Tamper Count 2
9	2	xxxx	Packet CRC

FIG. 2

300

MSB LSB

B	F	Q2	Q1	Q0	M2	M1	M0

Tamper (LS Byte)
Q[2:0] = Metrology Program Count
M[2:0] = Magnetic Tamper
F = Future Spare Flag
B = Low Battery Flag

MSB LSB

B	F	Q2	Q1	Q0	M2	M1	M0

Tamper (MS Byte)
T[2:0] = Tilt Tamper Count
N[2:0] = Non-Metrology Program Count
F = Future Spare Flag

FIG. 3

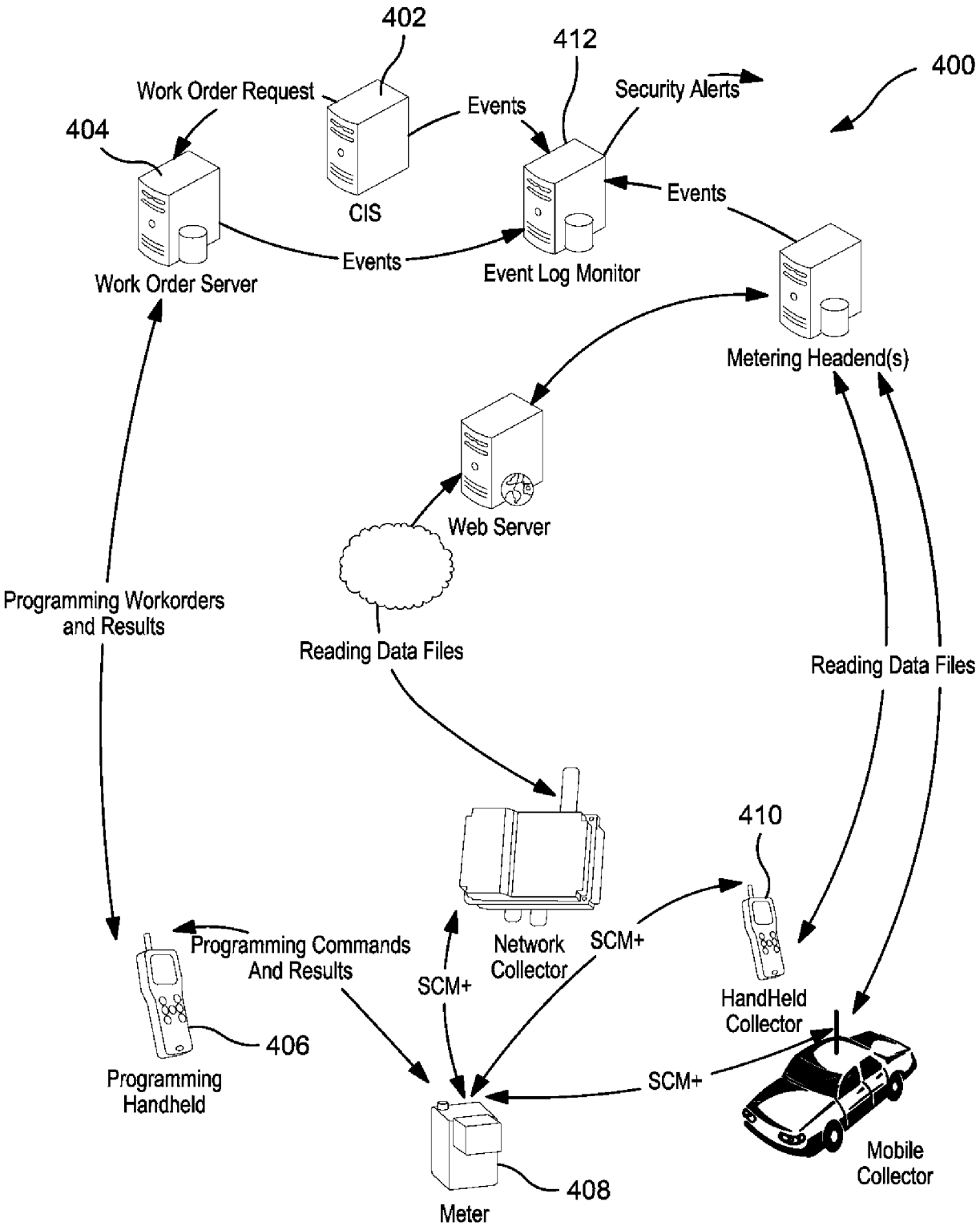
402
412
400
Work Order Request
Events
Security Alerts
404
CIS
Events
Work Order Server
Events
Event Log Monitor
Metering Headend(s)
Web Server
Programming Workorders
and Results
Reading Data Files
Reading Data Files
410
Programming Commands
And Results
Network
Collector
SCM+
SCM+
HandHeld
Collector
406
Programming
Handheld
SCM+
Mobile
Collector
408
Meter

FIG. 4

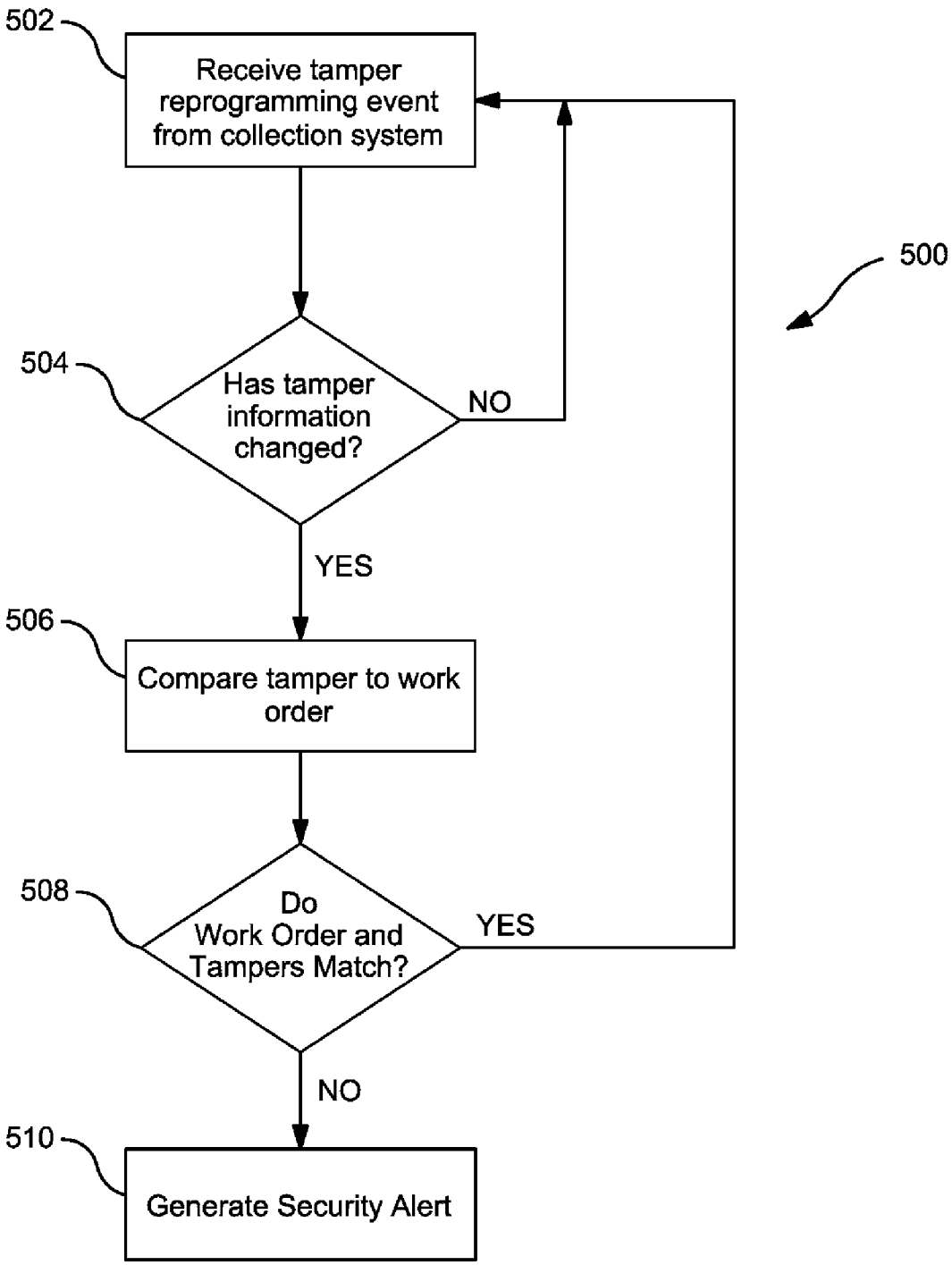
502
Receive tamper reprogramming event from collection system
500
504
Has tamper information changed?
NO
YES
506
Compare tamper to work order
508
Do Work Order and Tampers Match?
YES
NO
510
Generate Security Alert

FIG. 5