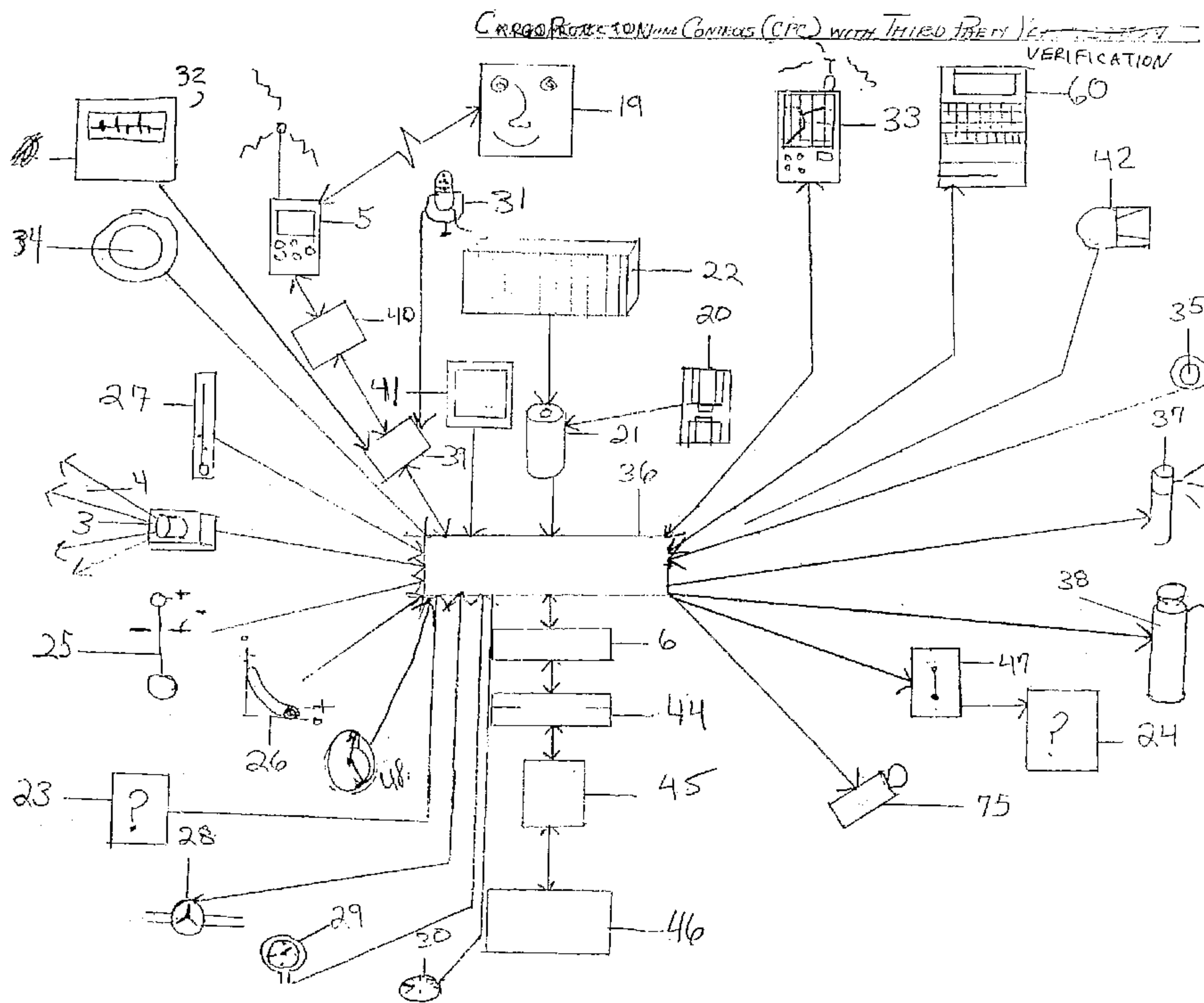




(86) Date de dépôt PCT/PCT Filing Date: 2005/06/16
 (87) Date publication PCT/PCT Publication Date: 2006/01/19
 (85) Entrée phase nationale/National Entry: 2006/12/15
 (86) N° demande PCT/PCT Application No.: US 2005/021331
 (87) N° publication PCT/PCT Publication No.: 2006/007405
 (30) Priorité/Priority: 2004/06/16 (US60/580,211)

(51) Cl.Int./Int.Cl. *H04L 9/00* (2006.01)
 (71) Demandeur/Applicant:
 BROWNEWELL, MICHAEL L., US
 (72) Inventeur/Inventor:
 BROWNEWELL, MICHAEL L., US
 (74) Agent: SIM & MCBURNEY

(54) Titre : DOCUMENTAIRE VIDEO DESTINE A EVITER DES PERTES DE DONNEES
 (54) Title: VIDEO DOCUMENTATION FOR LOSS CONTROL



(57) Abrégé/Abstract:

Systems and methods of documenting an event are disclosed. Events may include, but are not limited to, an accident, a crime, transportation of cargo, a medical procedure, a legal proceeding, an economic transaction, and/or a construction project. An event may be documented by data including, but not limited to, optical and/or audio records of the event. The event documentary may be accessible only via a database storage service bureau which has been certified to maintain accurate and authentic data by a party acceptable to a judicial system. The documentary may be admissible in a court of law. The documentary may be useful for determining the cause of an event and/or preventing a future event.

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

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
19 January 2006 (19.01.2006)

PCT

(10) International Publication Number
WO 2006/007405 A2

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:

PCT/US2005/021331

(22) International Filing Date: 16 June 2005 (16.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/580,211 16 June 2004 (16.06.2004) US

(71) Applicants and

(72) Inventors: **BROWNEWELL, Michael, L.** [US/US]; 354 Apple Valley Road, Lyons, CO 80540 (US). **BONHAM, Richard, H.** [US/US]; 1534 Mt Evans Drive, Longmont, CO 80501 (US). **MITCHELL, Ann, J.** [US/US]; 815-C Meeker Street, Longmont, CO 80501 (US). **BROWNEWELL, Linda, K.** [US/US]; 354 Apple Valley Road, Lyons, CO 80540 (US).

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

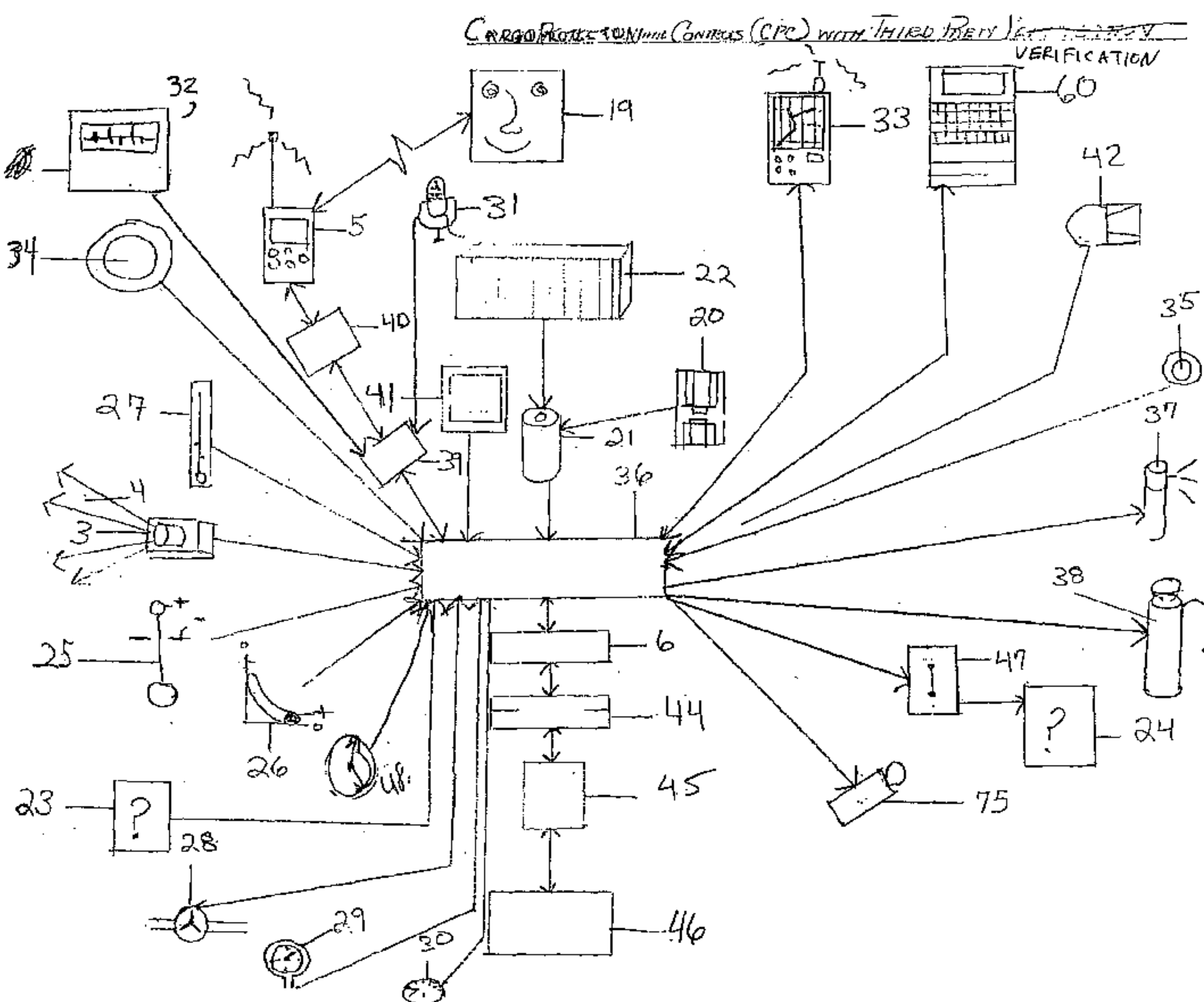
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, 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

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: VIDEO DOCUMENTATION FOR LOSS CONTROL



(57) Abstract: Systems and methods of documenting an event are disclosed. Events may include, but are not limited to, an accident, a crime, transportation of cargo, a medical procedure, a legal proceeding, an economic transaction, and/or a construction project. An event may be documented by data including, but not limited to, optical and/or audio records of the event. The event documentary may be accessible only via a database storage service bureau which has been certified to maintain accurate and authentic data by a party acceptable to a judicial system. The documentary may be admissible in a court of law. The documentary may be useful for determining the cause of an event and/or preventing a future event.

WO 2006/007405 A2

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34

TITLE

Video Documentation for Loss Control

CROSS REFERENCE APPLICATIONS

This application is a non-provisional application claiming the benefits of provisional application no. 60/580,211 filed on June 16, 2004.

BACKGROUND

The foregoing examples of the related art and limitations related therewith are intended to be illustrative and not exclusive. Other limitations of the related art will become apparent to those of skill in the art upon a reading of the specification and a study of the drawings.

Loss control has historically consisted of a series of checks and balances to guarantee the transfer and/or delivery of cargo. This was achieved by having both the delivering party and receiving party sign paper documents, each confirming the amounts and specific locations of the delivered cargo. Electronic signatures have since replaced paper documents. On June 30, 2000, the Electronic Signatures in Global and National Commerce Act (E-SIGN Act) was signed to establish the validity of electronic signatures for interstate as well as international commerce.

The ability to prove actual occurrences while cargo is in the care, custody, or control of those with legal responsibility for delivering cargo often relies on witness or third-party testimony. An example is the transportation industry in the United States. In the transportation industry in the United States, typically only the operator of a vehicle provides a point-of-view statement. Following an accident, all witnesses are questioned in an attempt to determine where fault lies. Such statements are often all a court has with which to validate a participant's claim of fault or negligence of a second party. Actual event recording, based on a third party recording and storage of the event, would greatly enhance the validity of legal claims related to the event.

What is needed is a 3rd party, un-biased video real-action documentation of an event. Such video documentation may present an unquestionable recount of events during court proceedings and may accurately challenge witness testimony as related to 'cause-of-events'. What is also needed is the ability to verify pickup and delivery of any product to the intended party.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33

SUMMARY

The following embodiments and aspects thereof are described and illustrated in conjunction with systems, tools, and methods which are meant to exemplify and illustrate, and not be limiting in scope. In various embodiments, one or more of the above described problems have been reduced or eliminated, while other embodiments are directed to other improvements.

Systems and methods of documenting an event or occurrence are disclosed. The documentary of the occurrence may be developed such that it is accessible only by a third party database storage service bureau which has been certified to maintain accurate and authentic data. Thus, the documentary may be admissible in a court of law. The documentary may be useful for determining the cause of an occurrence and/or preventing future occurrences.

An event trigger subsystem may be used to activate a system documenting an occurrence. The event trigger subsystem may comprise devices which automatically detect an occurrence. An example is an accelerometer which may detect a vehicular accident due to a sudden change in speed. Additionally, an event trigger subsystem may comprise manually or remotely activated devices.

In the event of an occurrence, encrypted data comprising the documentary of the occurrence may be saved on a local data storage subsystem. Additionally, such encrypted data may be transferred to a remote location. Other actions, such as securing cargo, may be taken in the event of an occurrence.

A smart-card system may be used to control and track cargo. By way of example and not of limitation, the smart-card system may track cargo consisting of fuel to insure it was shipped along a specific route, unloaded successfully at one or more locations, and accepted by each customer along a route.

Other features and embodiments will appear from the following description and appended claims and by referring to the accompanying drawings which form a part of this specification, wherein like reference characters designate corresponding parts in the several views.

GLOSSARY

The following terms are defined herein and will be used consistently throughout this document to mean:

1 1)'point A': the location and/or time that any cargo becomes a user's responsibility
2 through written contract, by implication through customary business practice, and/or by the
3 designation of any court of law in the territory wherein an occurrence damages the cargo.

4 2)'point B': the location and/or time that the user relinquishes the cargo and/or the
5 responsibilities assumed at Point A.

6 3)'cargo': any tangible or intangible property or data, that is in user care, custody
7 and/or control, or any tangible or intangible property or data, including money in electronic
8 transit, that is under user direction by written contract, by implication through customary
9 business practice, or by the designation of any court of law recognized by the government in
10 the territory wherein an occurrence takes place. For example, cargo includes but is not
11 limited to, funds being transferred by bank wire, credit card, or check, as well as real
12 property, product serial numbers, batch numbers, and percentage of completion of a project.

13 4)'occurrence': an event that results in bodily injury, property damage, property loss,
14 loss of income due to delay in transit, damage to the cargo, or any activity interpreted as a
15 user's responsibility by a court of law recognized by the government in the territory wherein
16 an occurrence takes place.

17 5)'event trigger': any action that precipitates and/or causes an occurrence.

18 6)'field of view': the area encompassing the image recorded by a camera.

19 7)'cause of loss': the description of an event that results in an occurrence.

20 8)'loss control': any action that would reduce the risk and/or frequency of a loss or
21 any action that would identify a cause of a loss.

22 9)'third party compliant': state where a disinterested, independent party (such as a
23 third party database storage service bureau) has certified the accuracy and/or authenticity of a
24 process, method, good, and/or tangible or intangible property or data.

25 10)'impact sensor': multiple "stop" mechanisms for activation of "loop start"
26 recording, including but not limited to, an accelerometer (or alternate method of determining
27 acceleration), deceleration or directional change outside a vehicle's normal operating
28 characteristics, etc.

29 11)'angle sensor': a device that determines the angle cargo is positioned at.

30 12)'temperature sensor': a device that determines the temperature of an area of
31 interest.

32 13)'pressure sensor': a device that detects a change of pressure in an area of interest.

33 14)'contamination sensor': a device that detects a change in the composition of cargo
34 and/or an area of interest.

1 15) 'panic switch': a manual "emergency stop" switch which may be activated by a
2 driver, machine operator, a remote party, a satellite communication protocol, etc.

3 16) 'any unit': any device that detects a change in conditions that have one or more
4 effects on cargo and/or an area of interest, and is fully integrated into a monitoring system.

5 17) 'construction related sensor': any device that monitors and/or records changes in
6 one or more of the following characteristics as they relate to building or construction site:
7 temperature, pressure, moisture, noise, atmospheric contamination, motion, vibration, soil
8 conditions, or other characteristics.

9 18) 'flow sensor': a device that determines a quantity of cargo loaded to a transport
10 apparatus or unloaded from a transport apparatus.

11 19) 'disabling substance': any form of substance released into a contained or
12 designated area intended to make the area hazardous, uninhabitable, or intended to disable
13 any human in the area.

14 20) 'fire extinguisher': any device designed to contain, eradicate, or extinguish a fire.

15 21) 'audio signal device': a device that makes noise (e.g. a horn) or that can be used to
16 transmit a voice or an audio signal.

17 22) 'any device': any device that is connected to a system and is an input device that
18 is activated or turned on either directly or indirectly by the system, any device that adds a
19 data field to the system, and/or any device that adds an output device. Examples include, but
20 are not limited to, an audio recording device and an offsite audio reproduction device.

21 23) 'interface switch': any device that completes a circuit from an information
22 processor to any device that it is connected to.

23 24) 'GPS': global positioning system which is a device designed to recognize the
24 global position of a person or property via a system of satellites.

25 25) 'transceiver': device that communicates with an outside source; relays instructions
26 for the protection of a person or property.

27 26) 'encoder': subsystem that encrypts data and/or allows access to stored data by a
28 disinterested, independent third party in the event of an incident.

29 27) 'decoder': device that processes signals received from an outside source and
30 initiates a go sequence from the instructions.

31 28) 'unit 60': Delivery, Control, and Acknowledgement (DCA) device.

32 29) 'authenticate': to verify the identity of a person, an association, an entity, an
33 apparatus, a transaction, data, tangible property, intangible property, and/or a process.

34

1 BRIEF DESCRIPTION OF THE DRAWINGS

2 Exemplifying embodiments are illustrated in referenced figures of the drawings. It is
3 intended that the embodiments and figures disclosed herein are to be considered illustrative
4 rather than limiting. Also, the terminology used herein is for the purpose of description and
5 not of limitation.

6 Fig. 1 is a top view of a trucking application embodiment.

7 Fig. 2 is a side view of a crane and rigging application embodiment.

8 Fig. 3 is a side view of an intermodal/ocean cargo application embodiment.

9 Figs. 4a and 4b are exterior and interior perspectives respectively of a
10 commercial/industrial/residential real estate application embodiment.

11 Fig. 5 is a system representation of embodiments of cargo protection and controls
12 (CPC), third party verification, and data information flow.

13 Fig. 6 is a system representation of sensor data and other device input as well as other
14 device input to CPU 6.

15 Fig. 7 is a system representation of data flow with 3rd party verification.

16 Fig. 8 is schematic representation of potential actions that may be taken as the result
17 of an occurrence.

18 Fig. 9 is a schematic description of DCA 60.

19 Fig. 10 is a flow chart of the CPC systems checks.

20 Fig. 11 is a flow diagram showing the overall interactions for the cause of loss versus
21 loss control procedures.

22 Fig. 12 is an example of an embodiment applying 3rd party compliant data and
23 storage to a medical application.

24 Fig. 13 is an example of an embodiment applying 3rd party compliant data and
25 storage to a legal application.

26 Fig. 14 is an example of an embodiment applying 3rd party compliant data and
27 storage to document a construction project.

28 Fig. 15a is an example of an embodiment of third party compliant data system
29 integrated into a trucking industry application.

30 Fig. 15b illustrates the data flow of the system of Fig. 15a

31 Before explaining the disclosed embodiment of the present invention in detail, it is to
32 be understood that the invention is not limited in its application to the details of the particular
33 arrangement shown, since the invention is capable of other embodiments. Also, the
34 terminology used herein is for the purpose of description and not of limitation.

1

2

3

4

DETAILED DESCRIPTION OF THE PRESENT INVENTION

5

6

7

8

9

Figures 1-4 are schematic diagrams of possible embodiments of documentation systems and means taught herein. Fig. 1 is a top view of trucking application embodiment 180. The top view of power unit (semi-tractor) 1 and trailer 2 shows possible locations for camera(s) 3 and respective fields of view 4 of camera(s) 3. Camera(s) 3 may be capable of fields of view 4 of up to 360° depending on the application desired.

10

11

12

13

14

Signal transceiver 5 may be located on top of the truck cab of power unit 1. Signal transceiver 5 is a device capable of transmitting and receiving data to/from a remote location and may be connected to a CPU 6 (Central Processing Unit/Data Recorder). CPU 6 may be located in the cab of the power unit 1 (and/or at a remote location). On-board controls 7 may also be located in the cab of power unit 1.

15

16

17

18

19

20

21

22

23

Fig. 2 is a side view of crane and rigging application embodiment 200. The side view of a crane unit 8 with outrigger supports 9 shows cargo 10 being maneuvered. Possible locations for camera(s) 3 and respective field(s) of view 4 of camera(s) 3 are illustrated. One possible location for a camera 3 is just above crane hook assembly 11 for possible view of cargo 10 and rigging 13. Camera(s) 3 may be capable of fields of view 4 of up to 360° depending on the application desired. On top of the cab of crane control center 12 may be signal transceiver 5, which may be connected to the CPU located in the cab (and/or a remote location) of crane control center 12. The on-board controls may also located in the cab of the crane control center 12.

24

25

26

27

28

29

30

31

Fig. 3 is a side view of intermodal/ocean cargo application embodiment 300. The side view of flatbed truck 14 shows cargo container 15 secure on the bed of the truck. Possible locations for camera(s) 3 and the respective field(s) of view 4 of cameras 3 are illustrated. Camera(s) 3 may be capable of fields of view 4 of up to 360° depending on the application desired. Signal transceiver 5 may be located on top of the cab of flatbed truck 14 and/or on top of cargo container 15. Signal transceiver 5 may be connected to CPU 6 which may be located in the cab of flatbed truck 14. On-board controls 7 may be located in the cab of the flatbed truck 14

32

33

34

Figs. 4a and 4b are exterior and interior perspectives respectively of commercial/industrial/residential real estate application embodiment 400. Fig. 4b is a side view of a structure 16b showing the location of security alarm panel 17. By way of example

1 and not limitation, safe 72 may be secured. Possible locations for camera(s) 3 and respective
2 field(s) of view 4 of camera(s) 3 are also illustrated. Camera(s) 3 may be capable of fields of
3 view 4 of up to 360° depending on the application desired.

4 Fig. 4a shows an exterior perspective view of structure 16a. Signal transceiver 5,
5 which may be in communication with a security monitoring firm, may be located on top or in
6 the attic of structure 16a. Signal transceiver 5 may be connected to CPU 18. CPU 18 may
7 be incorporated into the security alarm panel 17 or may be a stand alone device.

8 Fig. 5 is a system representation of embodiments of cargo protection and controls
9 (CPC), third party verification, and data information flow. It should be understood that a
10 plurality of embodiments are possible which may comprise some, all, or none of the
11 elements of Fig. 5. Additionally, an embodiment may comprise a single or multiple
12 occurrence of a given element.

13 Fig. 5 illustrates various types of hardware units and processes. Some may have one
14 way flow while others may have two way flow as will be noted. Data from units may
15 initially flow into interface 36.

16 The units may have three potential sources of power. External power 20 may come
17 from a vehicle or other mobile source or a fixed power distribution or generation system.
18 Solar panel 22 may be used as a primary or secondary source of power. Also, battery 21 may
19 be used as a primary or redundant backup source of power and may be recharged via external
20 power source 20 or solar panel 22.

21 The following units may have a one way data/energy flow into interface 36: battery
22 21, camera 3, on-site panic button 34, any additional input unit 23, impact sensor 25, angle
23 sensor 26, temperature sensor 27, flow sensor 28, pressure sensor 29, atmospheric sensor 30,
24 audio input recorder 31, date and time stamp 48, and/or input from medical devices 32. The
25 following units may have a one way data flow received from interface 36: any additional
26 output unit 24 (which may be controlled by switch 47), mace or disabling substance
27 dispenser 37, fire extinguishing device 38, camera monitoring device 41, and/or audio device
28 42. The following may have 2-way data flow with interface 36: transceiver 5, on-site CPU 6,
29 GPS unit 33, external command panic button 35, encoding device 39, decoding device 40,
30 and/or delivery, control and acknowledgement device 60.

31 Video images may travel from respective camera 3, to interface 36 and onto on-site
32 CPU 6. When appropriate, the images may be encrypted 44 as either stills or as full motion
33 images and saved to recording device 45. Stills or full motion images may be selected based
34 on the occurrence type and user specifications. Also, if programmed, the data will be

1 forwarded 46 on to an external source (e.g. a security monitoring station) for immediate
2 action. Data inputs may flow through interface 36 and into CPU 6 for programmed
3 instructions and/or responses.

4 Certain commands and/or responses can be issued from external source 19 through
5 transceiver 5, into interface 36 and onto on-site CPU 6. At CPU 6, instructions can be given
6 back through interface 36 to execute various procedures. For example, instructions can be
7 given to utilize audio device 42, introduce a disabling substance into a specified environment
8 37, and/or kill the ignition 75 in the cases of robbery or hijacking. For security reasons,
9 instructions can be encoded 39 at the on site location prior to transmission to off site location
10 19, and decoded 40 once they arrive back on site.

11 Should a triggered incident occur, the encrypted data stored in recording device 45.
12 may only be accessible to 'independent' 3rd parties. An independent third party may be a
13 database storage service bureau which has been certified to maintain accurate and authentic
14 data by parties such as law enforcement, the judicial system, and other interested parties. By
15 way of example and not of limitation, a party which certifies that a database storage service
16 bureau maintains accurate and authentic data may comprise individuals acceptable to a
17 government law enforcement agency, and/or a judicial agency, and/or an insurance industry
18 trade group.

19 Fig. 6 is a system representation of sensor data and other device input as well as other
20 device input to CPU 6. Flow data from flow sensor 28, or data from another sensor, may go
21 into interface 36 when activated 52. At all other times, sensors may be in sleep mode to save
22 energy. Data may flow from interface 36 to on-site CPU 6 and if programmed, onto
23 recording device 45. Data may further flow onto external control center 19 via transceiver 5.

24 In the event Delivery/Control/Acknowledgement DCA unit 60 is activated 55 and/or
25 GPS 33 is activated 57, the same procedure discussed above with respect to flow sensor 28
26 may be followed. For the purpose of this illustration, clock 48 is shown to represent the
27 time/date stamp that may be attached to some or all data when activated 56. However, the
28 time/date stamp function may be provided by hardware and/or software in CPU 6 at the time
29 of data transfer from interface 36 to CPU 6.

30 Fig. 7 is a system representation of data flow with 3rd party verification. At activation,
31 camera 3 images, if not digital may be converted to digital format. If the images are not
32 corrupt, they may be sent to CPU 6. The images may be encrypted 44 and then sent onto
33 recording device 45. The images may further be sent to external control center 19 via
34 transceiver 5 after optional encryption by encoder 39. External control center 19 may further

1 review the images, analyze the images, and/or respond to the images in the form of command
2 requests. If the images are corrupt, a malfunction notice may be sent to the appropriate party.

3 At activation (e.g. 3, 25, 26, 28, 29, or 30) of any sensor or any additional device 23
4 that requires an action be taken, recorded, or transmitted, the camera image 120 or data
5 information 121 may be converted to appropriate signal quality. If the data is not corrupt, it
6 may be sent to CPU 6. The data may be encrypted 44 and then sent onto recording device
7 45. The data may further be sent to external control center 19 via transceiver 5 after optional
8 encryption by encoder 39. External control center 19 may further review the data, analyze
9 the data, and/or respond to the data in the form of command requests. If the data is corrupt, a
10 malfunction notice may be sent to the appropriate party. Individuals at external control
11 center 19 may send commands via transceiver 5 within their directives and authority if in
12 their discretion they believe action is required based on information received from the site
13 via transceiver 5. The commands may then be decoded 40 and sent on to CPU 6. The
14 instructions may then be given to the various output devices via interface 36 and appropriate
15 action may be taken (e.g. horn 42 sounds, a fire extinguishing device 38 is activated).

16 The following is an example of a possible embodiment of a system for documenting a
17 loss in a vehicle or involving a vehicle. Such embodiment is referred to as a TR-ED in the
18 following example. It is to be understood that the following embodiment is offered solely by
19 way of example and not of limitation. Various other embodiments of a system for
20 documenting a loss in a vehicle or involving a vehicle are possible.

21 A small, easily installed video capture device may be installed inside the cab of a
22 vehicle or other equipment. It thus provides a real time recording and encoding system.
23 The device is referred to as "TR-ED" (Time Recording and Encoding Device) throughout
24 this example. The fixed, forward facing camera will provide a view of the road consistent
25 with that of the operator's field of view which is the vehicle's trajectory. An on-board digital
26 video recorder will continually "loop" the live video shot to its hard drive, only maintaining
27 that video signal upon activation of a "go" sequence. The "go" sequence may be any one of
28 multiple events, which take place within the vehicle or an incoming signal to the vehicle via
29 satellite communication (sat-com). This process will secure a desired real-time video of an
30 incident in the present invention's on board memory for future analysis by an Authorized
31 Third Party (ATP). The keys to this embodiment's performance are that the device must be
32 small enough not to impede the driver's or operator's field-of-view when installed inside the
33 vehicle or other equipment (glass, visor, dash, etc.). Specific considerations will be given to
34 its current consumption, operating voltage (e.g. 6V – 30VDC), and ease of installation. It is

1 understood that there may be a wide range of operating protocol for the device including:
2 continuous operation, vehicle-on operation, remote-on operation, etc. Consideration will be
3 provided during design for various “on/off” scenarios. The physical characteristics of the
4 device must be rugged enough to provide protection from: vehicle accident, shock, extreme
5 heat and cold (-60°F to +200°F), water, and fire. An internal battery backup must be
6 provided with duration sufficient to continue the post-alarm in the event of battery
7 termination resulting from impact, fire or other.

8 The system must run a “go” sequence consisting of pre and post alarm duration. The
9 system will continuously record activity in loop increments (duration to be discussed later).
10 Following the activation of the “loop start” function, the unit will continue to record for a
11 50% interval, then archive the incident file in its entirety.
12 Versions of the device can include: a fixed interval – single event system (FISE); a variable
13 interval – single event system (VISE); and a variable interval – multiple event system
14 (VIMS).

15 A. FISE – documents a single event upon activation of the “go” sequence. The
16 continual twenty- (20) minute loop will save ten- (10) minutes from the pre-alarm and
17 continue to run for ten- (10) minutes from the post-alarm. If the video monitoring subsystem
18 is disabled by the occurrence, then all of the storage subsystem memory (nominally 20
19 minutes) is used to store pre-event data.

20 B. VISE – documents a single event upon activation of the “go” sequence. The user
21 selectable duration of ten- (10) minutes to sixty- (60) minutes can be programmed into the
22 non-volatile memory prior to deployment of the device, and will perform similar to the FISE
23 after activation.

24 C. VIMS – documents multiple events upon activation of the “go” sequence. The
25 system will program and perform similar to VISE, with the added benefit of logging multiple
26 events as files on the hard-drive (the actual number of events and duration will depend on
27 duration of each respective “go” sequence). While running a documentation sequence, the
28 VIMS will ignore additional commands to activate the “go” sequence. Only at the
29 conclusion of a respective sequence will the device accept an additional “go” command.

30 Multiple “stop” mechanisms for activation of “loop start” recording may include the
31 following: an accelerometer (or alternate method of determining acceleration, deceleration or
32 directional change outside a vehicle’s or equipment’s normal operating characteristics), a
33 manual “Emergency Stop” pushbutton for operation by a driver or an operator, a satellite
34 communication protocol, etc.

1 A variable-frame-rate (VFR) compensation system can be integrated to the device by
2 its internal software system in an effort to conserve storage space and provide optimum
3 image quality at the time of incident. Using a software enabled pre-event alarm sequence,
4 the system will automatically recall and save images, for example, five seconds prior to a
5 stop sequence at a rate of up to about 30 frames-per-second (fps). The system will continue
6 to conserve five seconds following the stop event at this high-resolution, then return to a rate
7 of five frames per second. The ramp-up frame rate during an incident will dramatically
8 improve the possibility for positive vehicle or equipment identifying information (license
9 plate) gathering during the critical prior and post incident seconds. Changes in timing can
10 easily be programmed.

11 Fig. 8 is schematic representation of potential actions that may be taken as the result
12 of an occurrence. Fig. 8 expands on the description of Fig. 7. Once a command arrives back
13 on site and is in CPU 6, the go order may arrive at interface 36 and the appropriate action
14 sequence may be initiated. By way of example and not of limitation, an appropriate action
15 sequence may comprise one or more of the following: vehicle ignition termination 80
16 through off/on switch 84 disabling ignition 75 via remote panic button protocol 35, fire
17 extinguishing commences 81 using associated device 38, release of disabling substance 82
18 begins per use of device 37, noise 83 is used through horn or siren 42, or
19 activation/deactivation 59 or other action is commenced 85 using any other output unit 24.

20 Fig. 9 is a schematic description of DCA 60, which is a remote data entry system for
21 cargo identification, acceptance/rejection verification, payment input, and various smart card
22 functionalities. DCA 60 is a hand held device that verifies the delivery, control, and
23 acknowledgement of the receipt of cargo. DCA 60 may also accept credit card 71 payment
24 65 and any data input from a smart card 70. Data from smart card 70 may be used to
25 complete the delivery, identify the sending and/or receiving party or transfer the cargo to
26 another shipper for final delivery. DCA 60 may also be connected to Interface 36 directly
27 through the interface connection plug 67 with CPU 6 or an external CPU 19. DCA 60 may
28 incorporate a date input from an alpha key board 62, a numeric keyboard 63, an electronic
29 signature and order spot 64 for acceptance or rejection of the order 64, and/or a credit card
30 payment swipe 65. DCA 60 may transfer the information recorded in a smart card 70 into a
31 data base through the smart card insert 66. This input information, along with any other
32 information regarding the cargo from the internal CPU 6 and/or an external CPU 19, may be
33 displayed for customer verification in LCD display 61. The displayed information may then
34 be acknowledged by the recipient and the transaction may be verified and tracked for 3rd

1 party verification by activation of the final verification acknowledgement indicator 68. DCA
2 60 may be powered by internal battery 21 via switch 69.

3 Fig. 10 is a flow chart of the CPC systems checks. Fig. 10 describes the flow of
4 system checks internal to the system that may be performed on site or remotely. These
5 checks are designed to verify functionality of individual units on a regular basis so as to
6 correct problems prior to any possible incident/occurrence or allow the replacement of the
7 units as necessary. Additionally, the CPC systems checks may notify an administrator at
8 once in the event of any malfunction. Timer 95 can optionally enable periodic system check
9 90 to run, or system check 90 can have programmable activation. Periodic system check 90
10 may run periodic diagnostics. If activated, the system monitors sensor interface 92. A
11 complete system check 93 may then performed. If the result of the check is 'ok' (yes), a
12 return may be done into sleep mode 91. In not, a cause failure notification 94 may be sent to
13 the system monitor.

14 Fig. 11 is a flow diagram showing the overall interactions of the cause of loss versus
15 loss control procedures. An end user 102 places an order 103 into a main control system 101.
16 The order is verified 113 by a third party. Main control system 101 then generates invoice
17 104, which is verified 114 by a third party, and sent to distributor 105. Distributor 105 ships
18 inventory, which is verified 116 by a third party, along with an invoice for billing 107, to end
19 user 102. End user 102 then sends payment 110, which is verified 111 by a third party, to
20 distributor 105. Once payment 110 is received by distributor 105 and verified 115 by a third
21 party, bank wire 106 is verified 112 and sent to main control system 101 which routes
22 payment 109 to central bank 108. End user 102 receives product 118, which is verified 117
23 by a third party.

24 Fig. 11 thus illustrates a basic distribution/tracking model or system of secure
25 components that form an integrated solution to the problem of 3rd party compliance for
26 tracking. The system may track goods and data such as manufactured goods, percentage of
27 completion of construction projects, completed construction projects, purchase
28 agreements/contracts, services and/or associated products. For example, a 3rd party (e.g. a
29 specified agent not associated with any manufacturer, distributor, or contractor) will provide
30 hosting and maintenance of a server facilitating tracking. A security certification agency not
31 associated with the hosting agent, manufacturers, distributors, and/or contractors may ensure
32 transaction security between manufacturers, distributors, and/or contractors through the
33 issuance of a security certificate reviewed and renewed annually. In the case of manufactured
34 products, an E-commerce infrastructure may have a custom database design and

1 implementation for the storage of information relating to the tracking of manufacturer's
2 products, shipping tracking information, and distributor's receipt of goods. A database may
3 also track purchase orders and receipt of payments for exportation to other software products
4 (e.g. spread sheets). A client software application may facilitate the entry of manufacturing
5 and shipping information for products of manufacturers' clients. The software application
6 also may facilitate the entry of shipping receipts for manufactured goods and the generation
7 of purchase order requests. Software may also be available for a custom design and
8 implementation of infrastructure required for ordering and purchasing a manufacturer's
9 products online via a website.

10 A Distributor's Web-interface to E-commerce infrastructure may exist as a custom
11 design with a minimum of templates for interfacing with the E-commerce infrastructure.
12 Services for integrating distributor web-interfaces into the E-commerce infrastructure may
13 also exist for support and maintenance of distributor web-interfaces.

14 Fig 12 is an example of an embodiment applying 3rd party compliant data and storage
15 to a medical application. This embodiment integrates fields of view 4 images from camera
16 or optical device 3 and audio 31 to a medical profession application. The process may start
17 with the video and audio recording of the pre-surgery interview between a patient and a
18 doctor. The doctor may outline the treatment, operation, expected result(s), and recovery. In
19 the process, the doctor may address all concerns of the patient and releases may be executed.
20 This information may be encoded 39 and stored 45 in a manner referencing the patient's file
21 number or other identification number. During the operation, all video camera and optical
22 device 3 signals, their field of view 4, monitoring equipment 32 signals, and audio 31 signals
23 may be recorded. The data may be encoded 39, transmitted to interface 36, transmitted to
24 central processing unit 6, and then stored 45 in a manner such that it is referenced to the
25 patient's identification number. In the event that the operation is to be viewed live by a group
26 of off-site medical students or consulting physicians, the data can be decoded 40 and
27 transmitted 5 to an off-site CPU 19 for viewing. If the operation requires the assistance or
28 supervision of an off-site doctor who is participating or instructing and/or in the event of an
29 emergency, the encoded data can be sent directly by the transceiver 5, decoded 40, and
30 viewed 19. In the event that patient information needs to be reviewed prior to the operation
31 or included in the 3rd party verified data, the information can be down loaded by involved
32 off-site parties who have permission and are connected through an additional input unit 23.
33 During the patient's recovery or rehabilitation, some or all of the information that may be
34 relevant to that patient's condition such as test results, prescription relief and so forth, may

1 be electronically recorded, encoded, stored, and referenced to the patient's identification
2 number. In the event of complications, the entire file can be accessed to evaluate the
3 treatment and to review the operation and the patient's rehabilitation. In the event of
4 litigation by the patient, the entire file may be admissible as evidence. The encoded copy of
5 the file may be decoded, certified, and forwarded to both sides of the litigation and the court.
6 The fact that the patient's data file is encoded may help insure that the patient's medical
7 history privacy will be maintained. Additionally, the patient's encoded data file may allow a
8 second opinion to be offered from a remote location, may be used as a source of emergency
9 medical data (even if the patient is at a remote location), and may be used to assist the patient
10 with their own records and questions regarding their health.

11 Fig 13 is an example of an embodiment applying 3rd party compliant data and storage
12 to a legal application. This embodiment integrates fields of view 4 images from camera or
13 optical device 3 and audio 31 to a legal profession application. The current standard for
14 depositions is for legal proceeding data to be transcribed by a court recorder. With the
15 introduction of encoded 3rd party compliant data, the entire deposition can be viewed in real
16 time and/or at a later time. The video image of the deposition, through camera 3, records
17 non-verbal communication in its field of view 4. Audio 31 records all of the off-the-record
18 motions and discussions as well as the on-the-record record motions and discussions. Any
19 pertinent computer generated or scanned documents can be connected through additional unit
20 input 23. The data may be encoded 39, stored 45, and made available to review. Data may
21 be transmitted in real time or a later time to a remote location via transceiver 5. When data
22 is transmitted to a remote location via transceiver 5, it may be decoded 40 and viewed
23 through CPU 19, or the data may be decoded 40 and transmitted via transceiver 5 to CPU 19
24 for storage and retrieval at a later date. The set up and compliance to evidentiary standards
25 can be performed by any certified court reporter.

26 The end result may be one edited copy with the off-the-record motions deleted from both the
27 audio 31 and video field of view 4 signals for court and evidence use. Additionally, a non-
28 edited copy may be provided which includes all video and audio recordings. The non-edited
29 copy may be available to both plaintiff and defense attorneys. In summary, the video and the
30 audio data may be combined in a format that follows federal rules of evidence. It may be
31 encoded to guarantee validity and originality. It may be decoded and certified by an
32 independent, third party prior to review by any governmental entity, court system, arbitrator,
33 or other party that requires 3rd party verification of the validity and authenticity of data.

1 Fig. 14 is an example of an embodiment applying 3rd party compliant data and
2 storage to document a construction project. It is to be understood that the following
3 embodiment is offered as an example and should not be construed as a limitation. An owner
4 awards a contract to a construction company for construction of a project. The contract is the
5 legal framework that sets terms, which may include, but are not limited to, payment
6 requirements, documentation required to substantiate work performed, compliance to codes
7 and regulations, and methods for dispute resolution.

8 Supervision of the project and contract management is turned over to the project manager of
9 the construction company. The project manager may execute one or more separate
10 contract(s) with subcontractor(s) for work that they will perform. The management of the
11 prime contract and all subcontracts is the responsibility of the project manager, who shares
12 relevant data with parties who have a vested interest in the project. By way of example and
13 not of limitation, such parties may include:

- 14 1) Owner(s),
- 15 2) Subcontractors,
- 16 3) Banks and/or trust departments, and/or
- 17 4) Independent Third Parties.

18 The information to be shared by the project manager may be encoded. It may be
19 shared utilizing proprietary access codes functioning to give particular parties log-on ability
20 to their respective relevant data, which may be updated in real time via the project manager
21 and/or the accounting department. All access may be granted on a permission basis
22 dependent on a party's responsibility to the project. Access may be limited to selected data.
23 Additionally, permission to edit or add to existing data may be given.

24 Project data may begin to accumulate when the project commences and may continue
25 to amass until project completion. Every transaction involving the project data may be
26 recorded and encoded to provide a virtual paper trail. The project data may be subject to
27 review by various parties based upon their level of permission. By way of example and not
28 of limitation, the data reviewed may be any or all of the following:

- 29 1) Pay Request
- 30 2) Payment(s)
- 31 3) Lien Releases
- 32 4) Change Orders
- 33 5) Audits and Analysis and Final Adjustments
- 34 6) Final approvals(s) and sign-off

1 In some instances, independent 3rd party 100 sends request for payment 167 to owner
2 of the project 153, who then sends lien releases 168 to project manager 155 for signature.
3 When received, a copy is sent to the independent 3rd party and owner of the project 153 who
4 authorizes bank 165 to release payments 164. A copy of payments 164 is sent to accounting
5 department 157 and independent 3rd party 100. In no case will payments 164 be made
6 without signed lien releases 168.

7 As the project progresses, independent 3rd party 100 begins to integrate project
8 information data 158, tracking, contract compliance documents, and any other documents
9 169 relevant to completion. Independent 3rd Party 100 will maintain insurance
10 compliance(s), monitor certificates of insurance, and administer insurance compliance audit
11 programs.

12 In the case of construction projects, by utilizing the project manager as the hub for all
13 information flow and all job related activity, projects will be capable of virtual seamless
14 integration between contract compliance, estimating, accounting and all related 3rd party
15 contributors. This 3rd party integration will enable and enhance independent and verifiable
16 tracking, compliance and audit tasks.

17 Fig. 15a is an example of an embodiment of a third party compliant data system
18 integrated into a trucking industry application and follows the diagram of Fig. 1. The system
19 in this example is referred to a V-RAD unit, and comprises interface 36, camera 3, field of
20 view 4, GPS locator 33, date and time 48, and the impact sensor 25. CPU 6 encodes 39 the
21 data and stores the data in the hard drive 45. The hard drive continuously records the data in
22 a loop until such time as the impact sensor 25 is activated. At that point, data recording
23 device 45 records the encoded data until the data loop has record the specified time in the
24 software program or recording time setting. At any point in time, the encoded data in the
25 hard drive can be downloaded and directed 46 into the encryption transmission signal coding
26 44, and transmitted through the signal transceiver 5 for storage in the offsite CPU 19 or
27 decoding in the event of an occurrence to start the 3rd party verified data analysis and
28 introduction as evidence.

29 Fig. 15b illustrates the data flow of the system of Fig. 15a. Data from camera image
30 120 and data from information sensors 121 is routed through the signal transceiver 5, CPU 6,
31 and encryption/signal coding 44. In the event of live transmission to off site CPU 6, the data
32 is routed for direct transmission through signal transceiver 5 to off site CPU 19, or is,
33 encoded 39 and routed to hard drive 45 for storage. The data in the hard drive is continually

1 being rewritten until the data is directed to be preserved. The data can be encoded for secure
 2 transmission 39, or routed from hard drive 45 to signal transmitter 5 to the off site CPU 19.

3 A detail of the image resolution is to follow.

4 An example of a possible image resolution can be seen in Table 1 below.

5

VERTICAL RESOLUTION	1,200
HORIZONTAL RESOLUTION	1,600
	1,920,000
FPS (FRAMES-PER-SECOND)	5
	9,600,000
CAMERA/LENS CONFIGURATION	Pinhole
VIDEO SEQUENCE	Stop Action
SPEED = 60MPH	88
FT VEHICLE TRAVELS / SECOND	18
TOTAL MINUTES	15
FLASH PROCESSOR CAPACITY	8,640,000,000

6

TABLE 1

7 Video sequence(s) access is restricted for review only by an authorized third-party
 8 (ATP). A detailed and proprietary encryption sequence may be developed for ATP analysts
 9 exclusively. The ability to guarantee authenticity is critical for the submission of the video
 10 evidence into court proceedings. The V-RAD hardware system will encrypt the video "loop"
 11 after activation, following its termination of the respective loop, the file will be archived in
 12 the on-board hard-drive. The device must then be either directly connected or remotely
 13 connected (via secure internet connection or for fixed applications inside a cab by short-
 14 range carrier – 802.11b, low-power data transceiver system, etc.) to an ATP for download,
 15 decryption, review and analysis. During the decryption process, the ATP's registration
 16 number will be encoded with a "virtual water-mark" on the file for chain-of-custody
 17 purposes (including time and date of access). Only following the authorization of the ATP's
 18 registration number can the file be downloaded to CD, DVD, or analog medium as a MPEG-
 19 2 digital file. When downloading from the VIMS version of the system, the ATP will have
 20 time/date prompts from which to select scenes. Once a scene is opened, it is permanently

1 marked with the ATP's registration number. Multiple ATP's can access the same file; each
2 will be logged in the respective file's "virtual water-mark."

3 A single software system will accompany the VISE and VIMS versions of the V-
4 RAD, each containing a single-user license. The software will enable the customer to
5 program the VISE and VIMS version of the system prior to installation into a vehicle.
6 Software is projected to be a DOS base system with serial port program capability.
7 The Analysis software will be available only to authorized ATP's who have completed the
8 registration process. Each is a single user license and will require on-line, live activation
9 prior to issuance of an authorization code. The ATP software will contain the decryption
10 algorithms for video, audio, and project or product tracking retrieval and analysis, as well as
11 standardized methods of storage and download.

12 A key component of the V-RAD is the development of an "Authorized Third Party"
13 evidentiary verification system. The ATP would act as an intermediary between the
14 owner/operator of the vehicle and the insured, providing an unbiased report pertaining to:

- 15 1. The incident, relating to causes that were either in or out of the control of the
16 operator.
- 17 2. The pre-alarm findings, what lead-up to the circumstance and again was the operator
18 in or out of control of the events.
- 19 3. The post-alarm findings, what events took place following the event and what were
20 the specific actions of the operator.

21 The development of the ATP verification system must be a collaborative effort
22 between the insured, law enforcement, judiciary council and various representatives from the
23 transportation 1, crane and rigging 2, and other equipment 3 industries.

24 While a number of features and embodiments have been discussed above, those of
25 skill in the art will recognize certain modifications, permutations, additions and sub-
26 combinations therefore. It is therefore intended that the following appended claims
27 hereinafter introduced are interpreted to include all such modifications, permutations,
28 additions and sub-combinations are within their true spirit and scope. Each apparatus
29 embodiment described herein has numerous equivalents.

30

1

2

I CLAIM:

3

4

1. An event documenting system (EDS) functioning to document an event in a monitored area, the EDS comprising:

5

6

a video monitoring subsystem having an output signal representing an image of the monitored area;

7

8

an event trigger subsystem capable of detecting the event;

9

10

an encoding subsystem capable of encrypting the video monitoring subsystem output signal;

11

12

a storage subsystem capable of storing the video monitoring subsystem output signal;

13

a control subsystem capable of controlling the EDS;

14

wherein the video monitoring subsystem is continuously operating while the EDS is operating;

15

16

wherein the encoding subsystem encrypts the video monitoring subsystem output signal;

17

18

wherein the storage subsystem stores the encrypted video monitoring subsystem output signal;

19

20

wherein when the event trigger subsystem detects the event, the control subsystem instructs the storage subsystem to preserve a pre-event data segment and a post-event data segment;

21

22

23

wherein if the event renders the video monitoring subsystem inoperable, then storage subsystem's complete storage capacity is used to store the pre-event data segment; and

24

25

26

wherein the encrypted video monitoring subsystem output signal can be decrypted only by a database storage service bureau which has been certified to maintain accurate and authentic data.

27

28

29

2. The EDS of claim 1, wherein the event trigger subsystem further comprises an environmental change detection subsystem.

30

31

3. The EDS of claim 2, wherein the event trigger subsystem further comprises a mechanical force detection subsystem.

32

33

4. The EDS of claim 2, wherein the event trigger subsystem further comprises a flow change detection subsystem.

34

1 5. The EDS of claim 2, wherein the event trigger subsystem further comprises a
2 pressure change detection subsystem.

3 6. The EDS of claim 1, wherein the monitored area further comprises a vehicle's
4 trajectory.

5 7. The EDS of claim 6 further comprising a vehicle monitoring subsystem
6 having an output signal representing one or more of the vehicle's operating characteristics.

7 8. The EDS of claim 1 further comprising a transmitter capable of transmitting
8 the encrypted video monitoring subsystem output signal to the database storage service
9 bureau.

10 9. The EDS of claim 1, wherein the event trigger subsystem further comprises a
11 panic switch for manual triggering.

12 10. The EDS of claim 1, wherein the video monitoring subsystem further
13 comprises a camera installed on a vehicle's exterior.

14 11. The EDS of claim 1, wherein the monitored area further comprises real
15 property.

16 12. The EDS of claim 1, wherein the monitored area further comprises a
17 construction apparatus.

18 13. The EDS of claim 1, wherein the monitored area further comprises a cargo
19 container.

20 14. The EDS of claim 1 further comprising a receiver capable of receiving a
21 command from a remote party instructing the EDS to take one or more actions.

22 15. The EDS of claim 14, wherein the one or more actions further comprises
23 disabling a subsystem.

24 16. The EDS of claim 14, wherein the one or more actions further comprises
25 activating a subsystem.

26 17. A method of documenting an event in a monitored area, the method
27 comprising:

28 operating a video monitoring subsystem having an output signal representing an
29 image of the monitored area continuously;

30 encrypting the video monitoring subsystem output signal via an encoding
31 subsystem;

32 storing the encrypted video monitoring subsystem output signal in a storage
33 subsystem;

1 instructing the storage subsystem to preserve a pre-event data segment and a post-
2 event data segment when an event trigger subsystem detects the event;
3 preserving in the storage subsystem's entire storage capacity a pre-event data
4 segment if the event renders the video monitoring subsystem inoperable;
5 and
6 permitting the encrypted video monitoring subsystem output signal to be
7 decrypted only by a database storage service bureau which has been
8 certified to maintain accurate and authentic data.

9 18. An event documenting system (EDS) functioning to document an event in a
10 monitored area, the EDS comprising:
11 a video monitoring subsystem having an output signal representing an image of
12 the monitored area;
13 an event trigger subsystem capable of detecting the event;
14 an encoding subsystem capable of encrypting the video monitoring subsystem
15 output signal;
16 a transmission subsystem capable of transmitting the video monitoring subsystem
17 output signal to a remote site;
18 a control subsystem capable of controlling the EDS;
19 wherein the video monitoring subsystem is continuously operating while the EDS
20 is operating;
21 wherein the encoding subsystem encrypts the video monitoring subsystem output
22 signal;
23 wherein the transmission subsystem transmits the encrypted video monitoring
24 subsystem output signal to the remote site at a predetermined time
25 interval; and
26 wherein the encrypted video monitoring subsystem output signal can be decrypted
27 only by a database storage service bureau which has been certified to
28 maintain accurate and authentic data.

29 19. A method of documenting a medical or dental conference and a medical or
30 dental procedure, the method comprising:
31 operating a video monitoring subsystem covering a pre-procedure medical or
32 dental conference;
33 operating the video monitoring subsystem during the medical or dental procedure;

1 encrypting the video monitoring subsystem output signal via an encoding
2 subsystem;
3 storing the encrypted video monitoring subsystem output signal in a storage
4 subsystem capable of storing the video monitoring subsystem output
5 signal; and
6 permitting the encrypted video monitoring subsystem output signal to be
7 decrypted only by a database storage service bureau which has been
8 certified to maintain accurate and authentic data.

9 20. The method of documenting a medical or dental conference and a medical or
10 dental procedure of claim 19 further comprising operating the video monitoring subsystem
11 during a post-procedure data collection session.

12 21. A method of documenting a legal proceeding, the method comprising:
13 operating a video monitoring subsystem having an output signal representing an
14 image of the legal proceeding during the legal proceeding;
15 encrypting the video monitoring subsystem output signal via an encoding
16 subsystem;
17 storing the encrypted video monitoring subsystem output signal in a storage
18 subsystem capable of storing the video monitoring subsystem output
19 signal; and
20 permitting the encrypted video monitoring subsystem output signal to be
21 decrypted only by a database storage service bureau which has been
22 certified to maintain accurate and authentic data.

23 22. A method of documenting an economic transaction, the method comprising:
24 providing a database storage service bureau which has been certified to maintain
25 accurate and authentic data;
26 authenticating and recording an end user's order via the database storage service
27 bureau;
28 authenticating and recording an invoice corresponding to the end user's order via
29 the database storage service bureau;
30 authenticating and recording shipment of property corresponding to the invoice
31 via the database storage service bureau;
32 authenticating and recording the end user's payment of a bill via the database
33 storage service bureau; and

- 1 permitting stored records of the economic transaction to be accessed only by the
2 database storage service bureau.
- 3 23. A method of documenting a construction project, the method comprising:
4 providing a database storage service bureau which has been certified to maintain
5 accurate and authentic data;
6 verifying data related to the construction project via the database storage service
7 bureau;
8 encrypting the data related to the construction project;
9 creating a documentary of the construction project by storing the encrypted data
10 related to the construction project in a database associated with the
11 construction project maintained by the database storage service bureau;
12 providing read only access to the database for the construction project maintained
13 by the database storage service bureau to a first group of parties; and
14 providing read and write access to the database for the construction project
15 maintained by the database storage service bureau to a second group of
16 parties.
- 17 24. A portable apparatus functioning to document and facilitate the delivery of
18 cargo, the portable apparatus comprising:
19 a keyboard to capture character data;
20 a bank card interface to capture bank card data;
21 an identification card interface to capture identification card data;
22 a communication interface to connect to an external communication network;
23 a user interface for a user to acknowledge acceptance or rejection of the cargo;
24 an optical screen for displaying data;
25 wherein an operator may document transfer of the cargo via the keyboard;
26 wherein the user may be identified via the identification card interface;
27 wherein the operator may be identified via the identification card interface;
28 wherein the user may purchase cargo via the bank card interface;
29 wherein the user may acknowledge receipt of the cargo via the user interface; and
30 wherein the operator may transfer data comprised by the portable apparatus to the
31 external communication network via the communication interface.
32

Fig. 1

TRUCKING APPLICATION
TOP VIEW

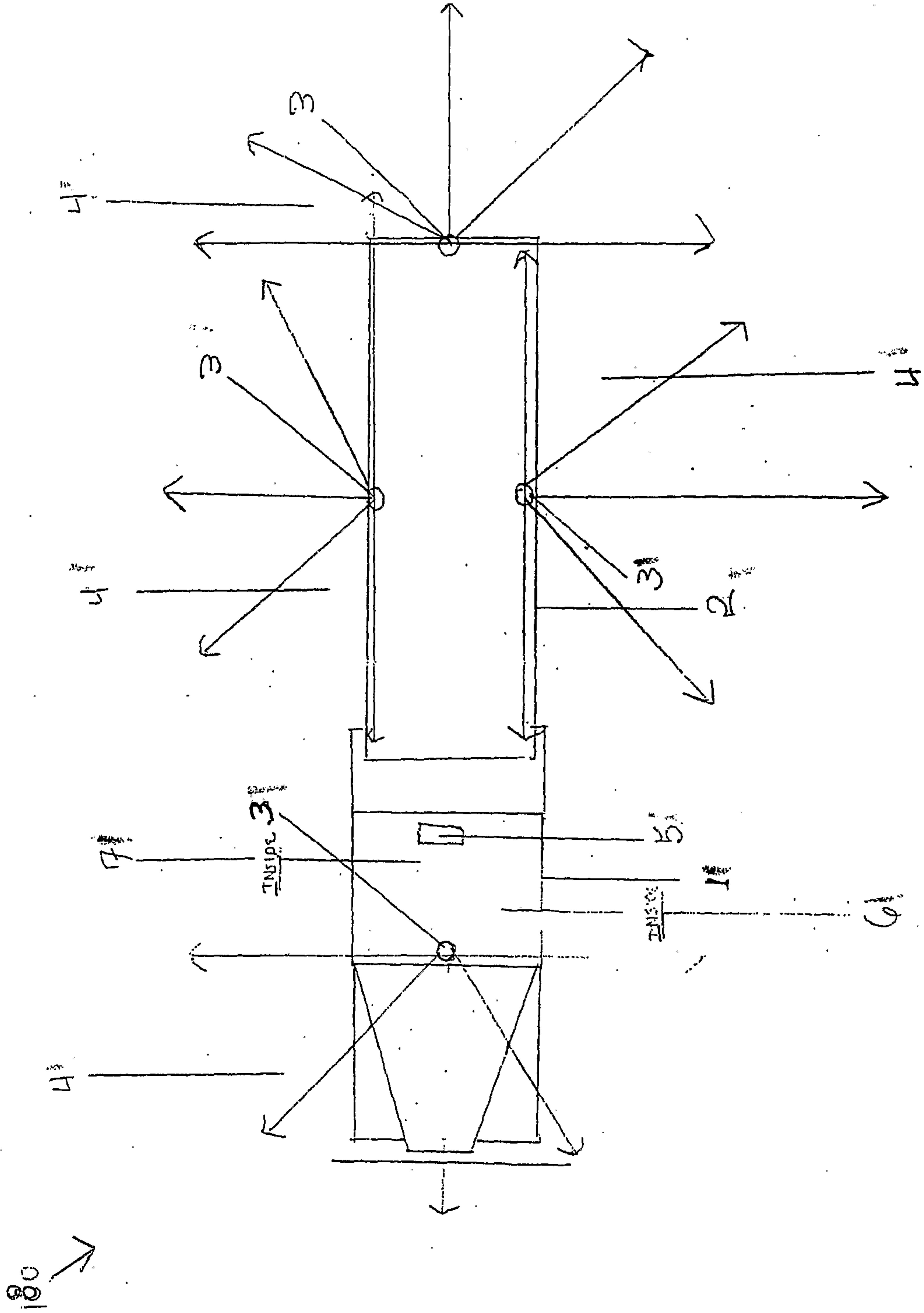
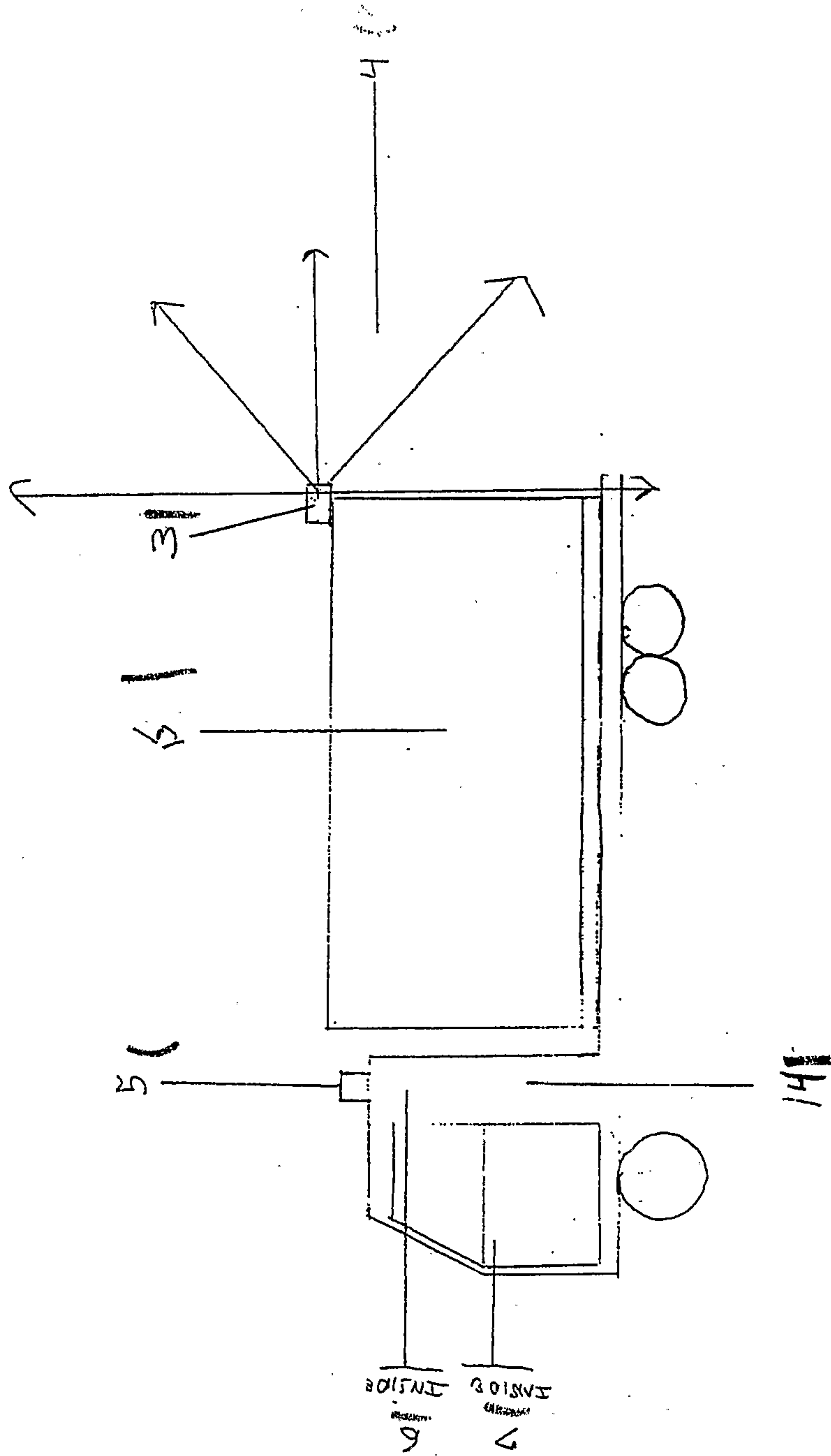


Fig 3

INTERMODAL / OCEAN CARGO APPLICATION
SIDE VIEW

300
↓

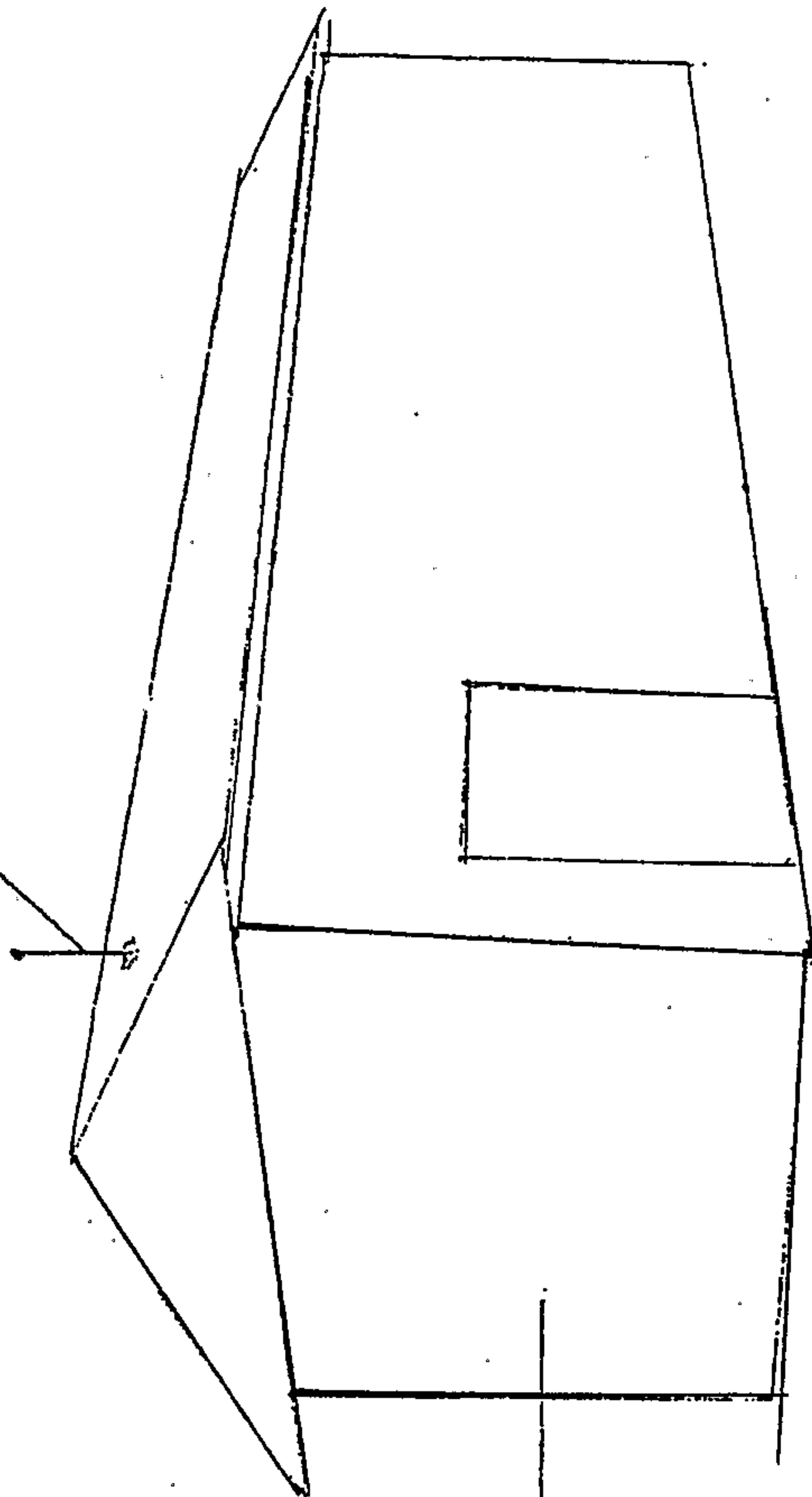


COMMERCIAL/INDUSTRIAL/RESIDENTIAL REAL ESTATE APPLICATION
EXTERIOR VIEW

Fig 4a

400 ↓

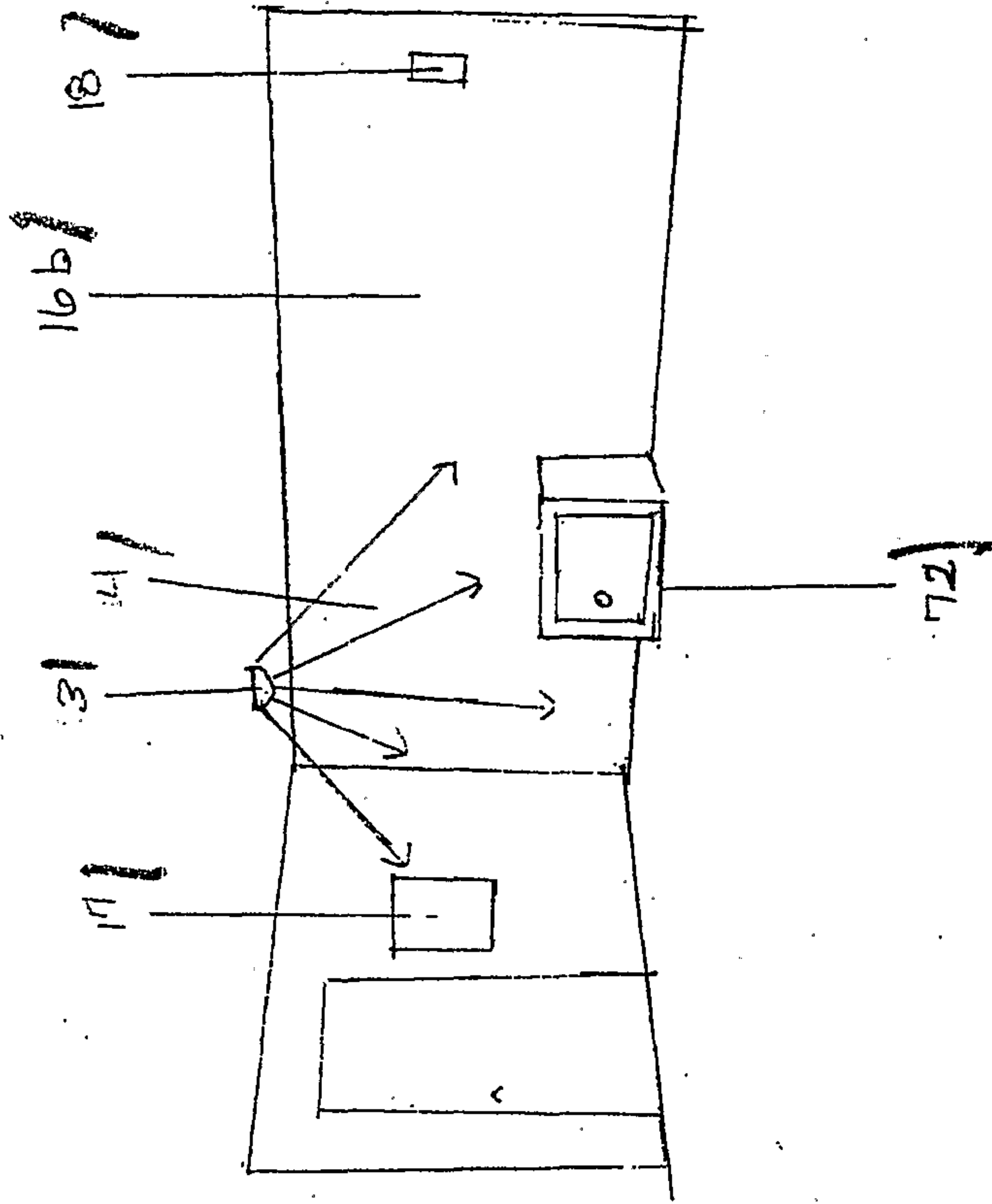
51



16A

Fig 4b
COMMERCIAL/INDUSTRIAL/RESIDENTIAL REAL ESTATE APPLICATION
INTERIOR VIEW

400
↓



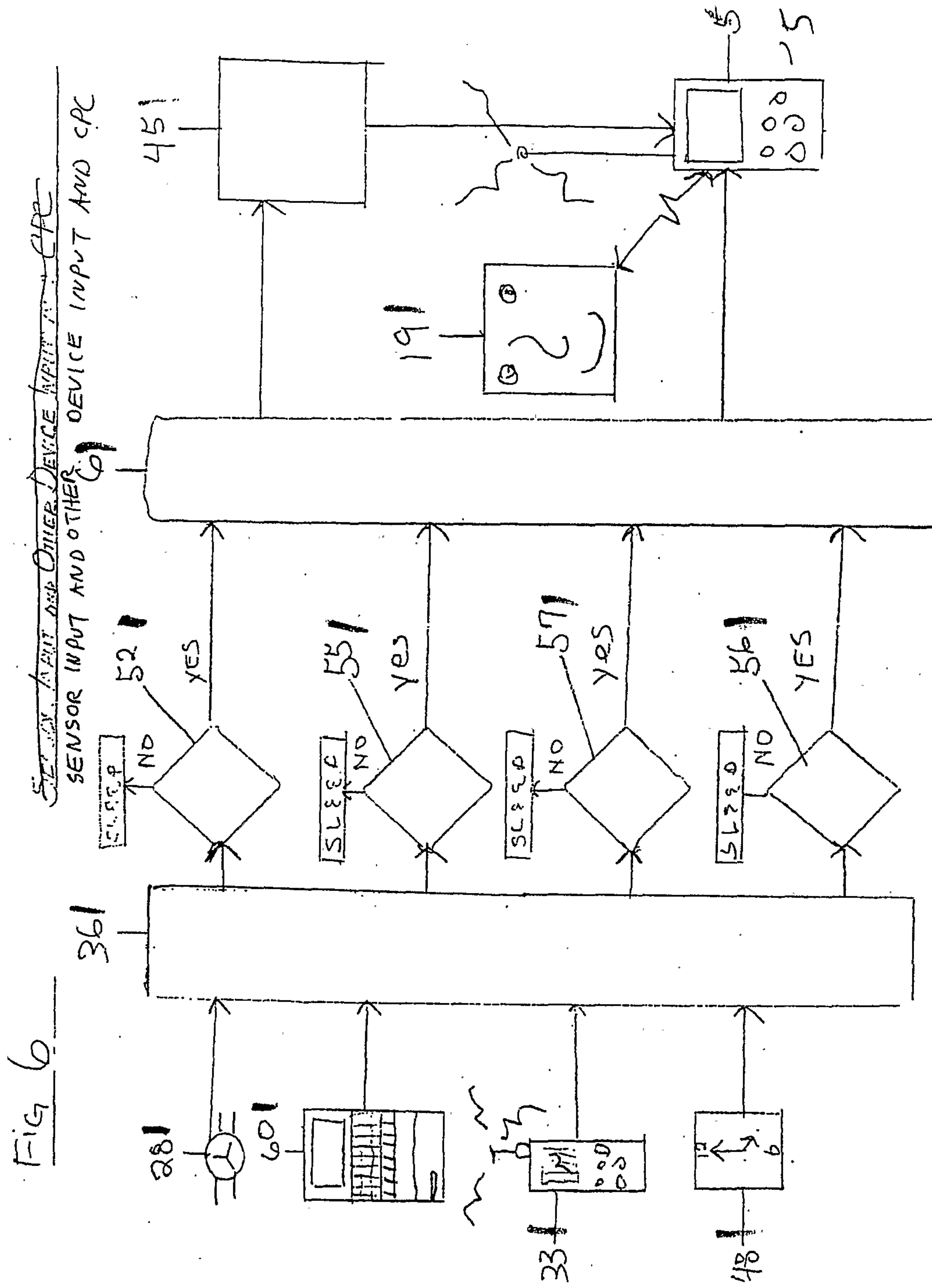
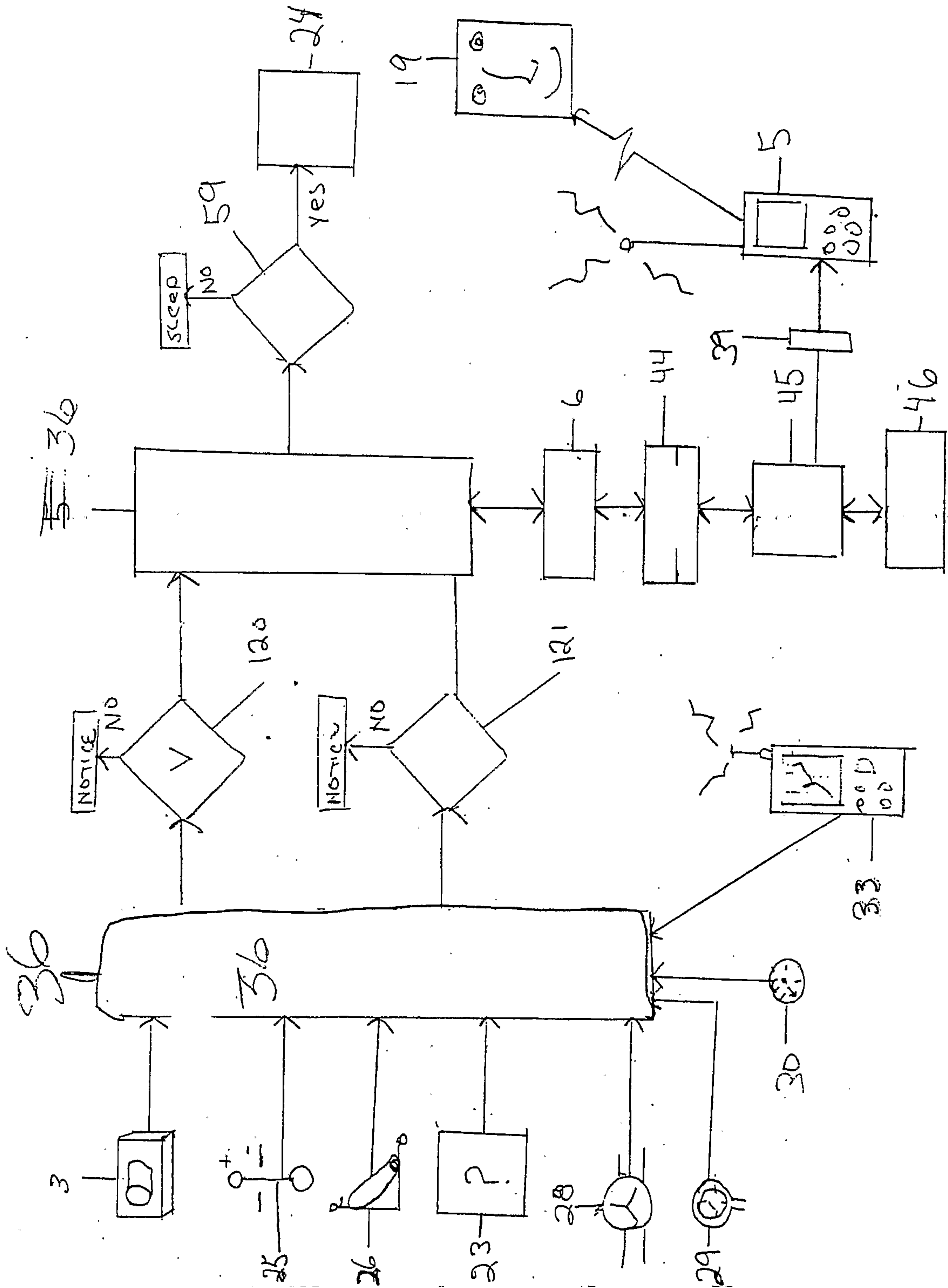
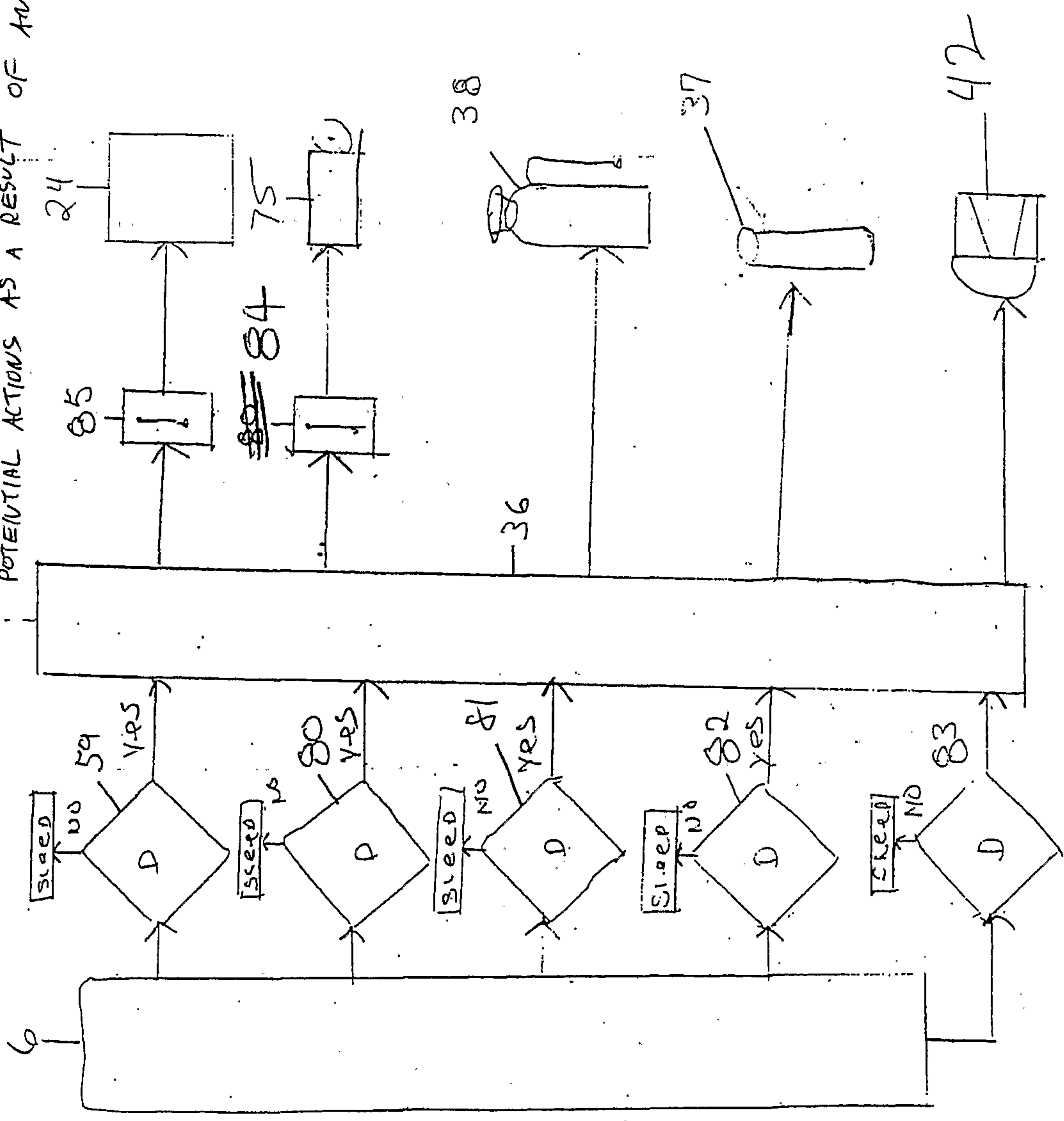


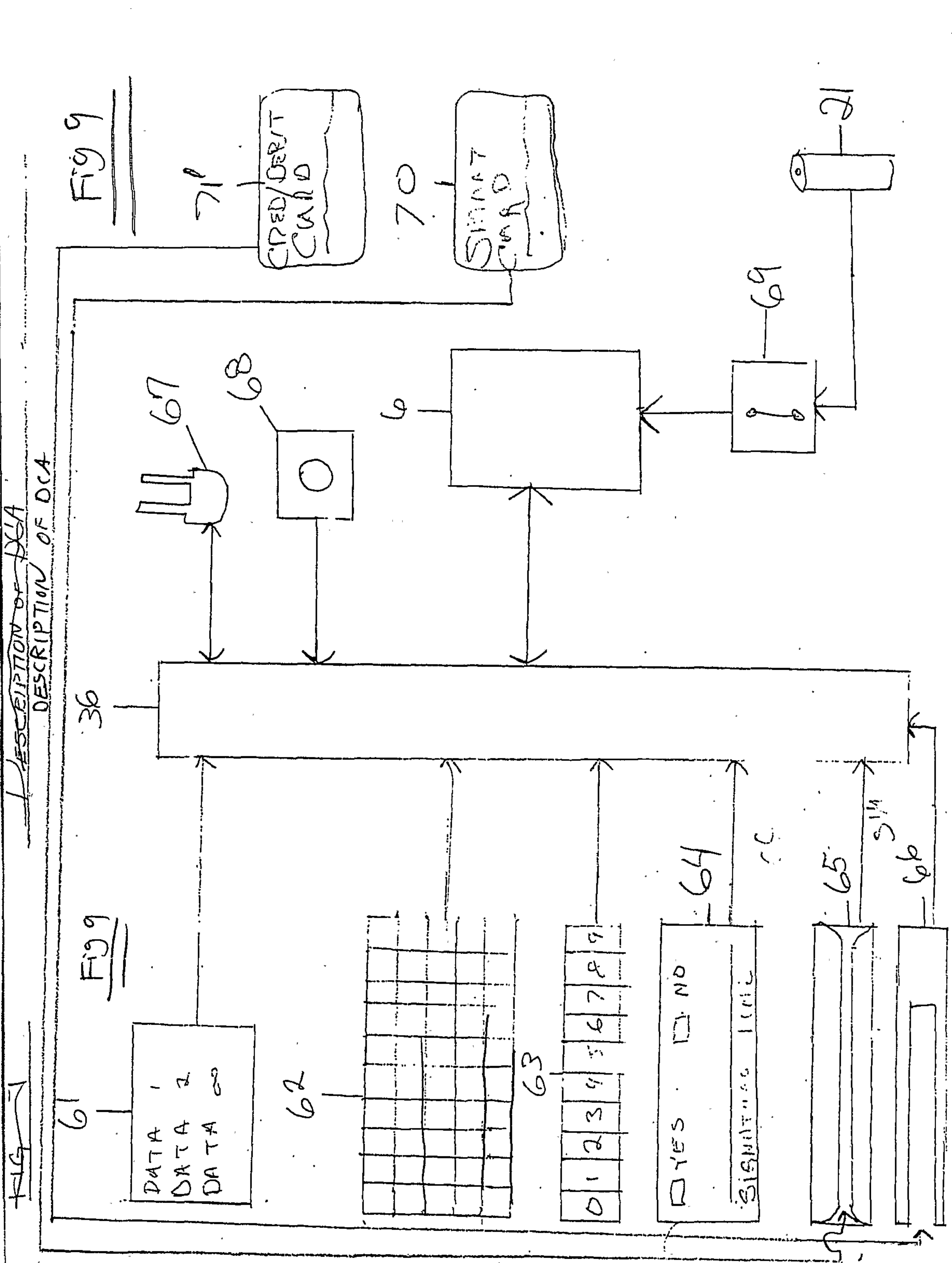
FIG 7 SYSTEM REPRESENTATION DATA FLOW WITH 3RD PARTY VERIFICATION



POTENTIAL ACTIONS AS A RESULT OF AN OCCURRENCE

Fig 8 POTENTIAL ACTIONS AS A RESULT OF AN OCCURRENCE





SYSTEMS CHECK

Fig 10

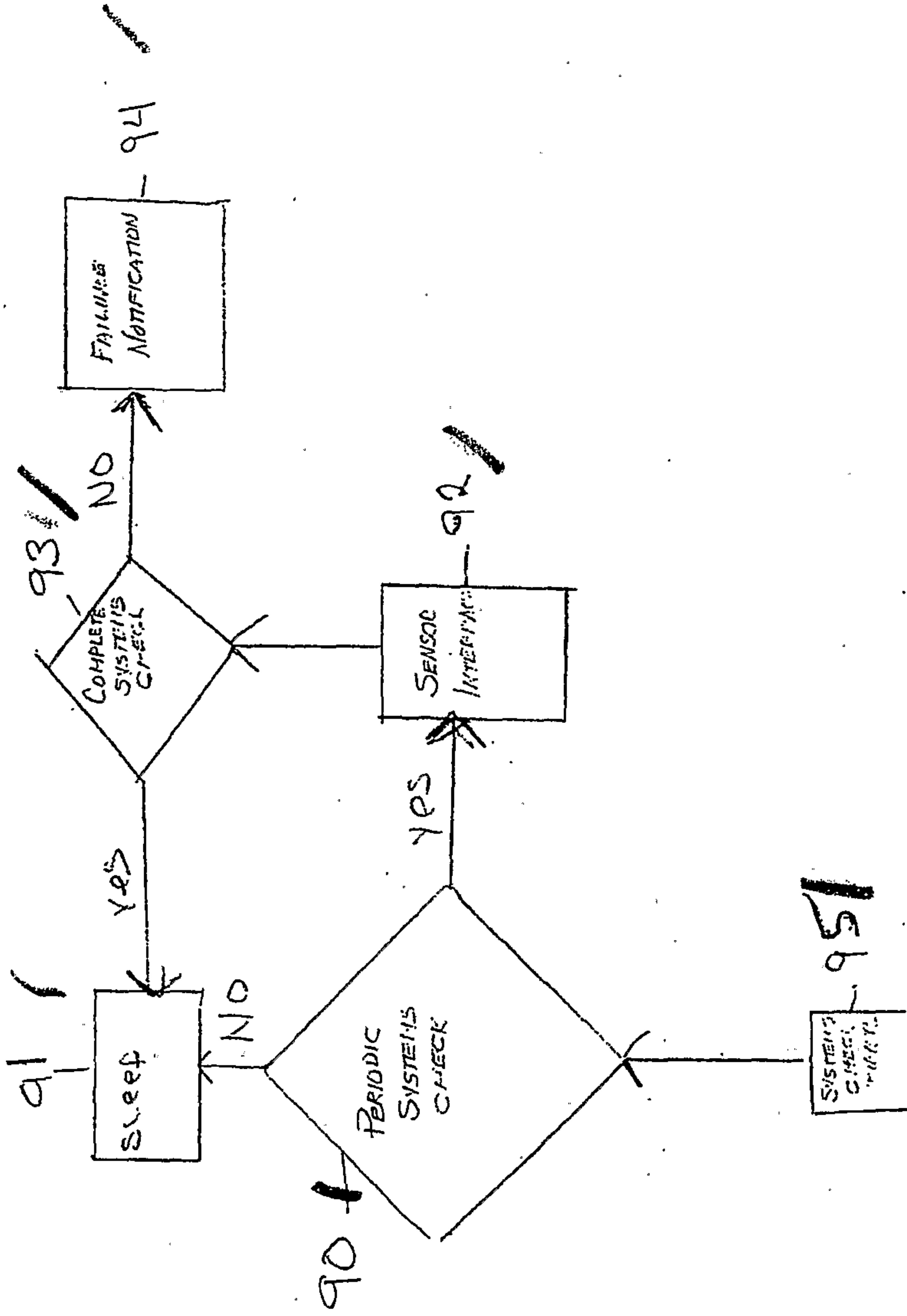


FIG 11 TRANSACTION AND VERIFICATION FLOW

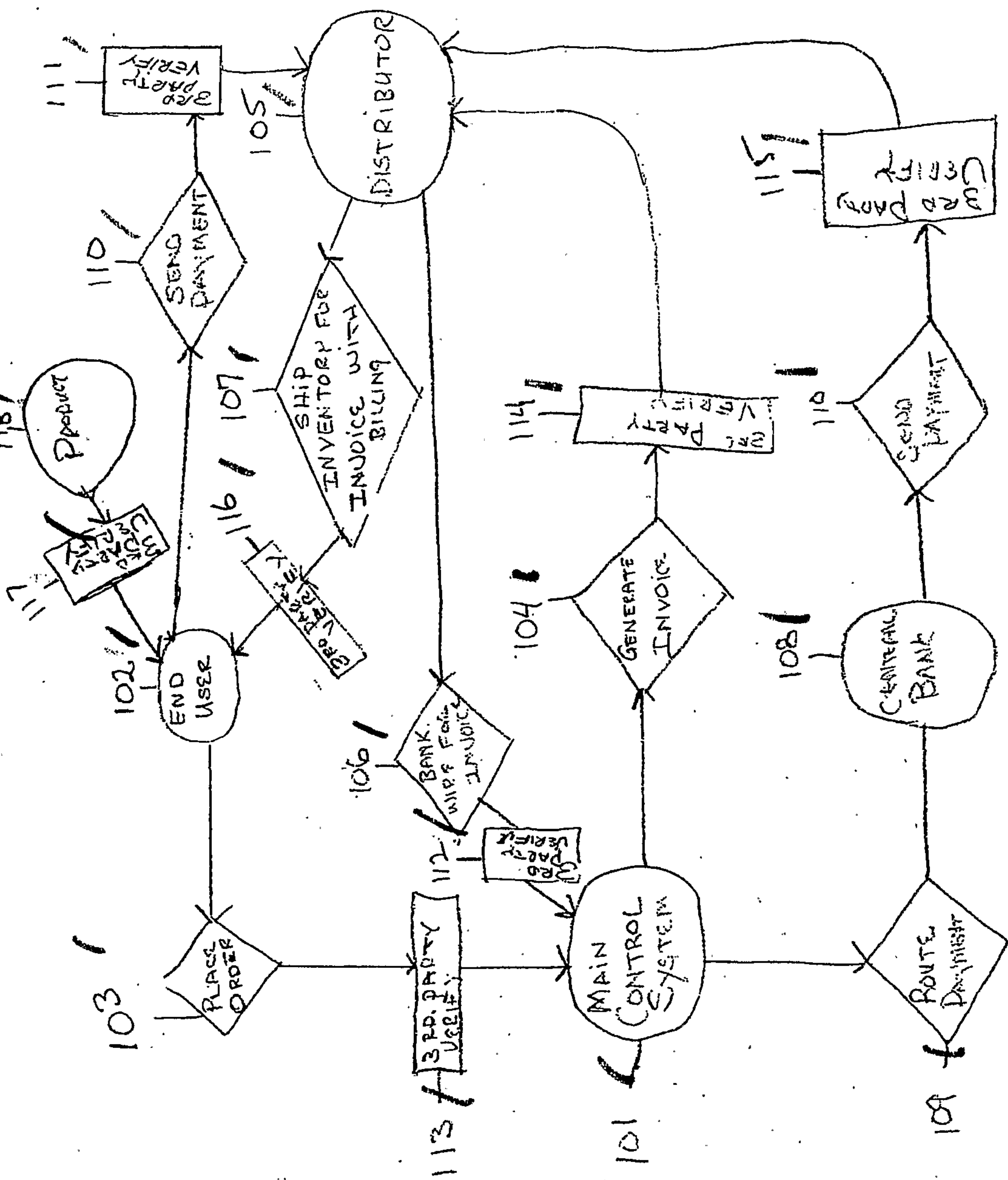


FIG 12
MEDICAL TREATMENT AND CONTROL (CPU)
WITH 3RD PARTY VERIFICATION

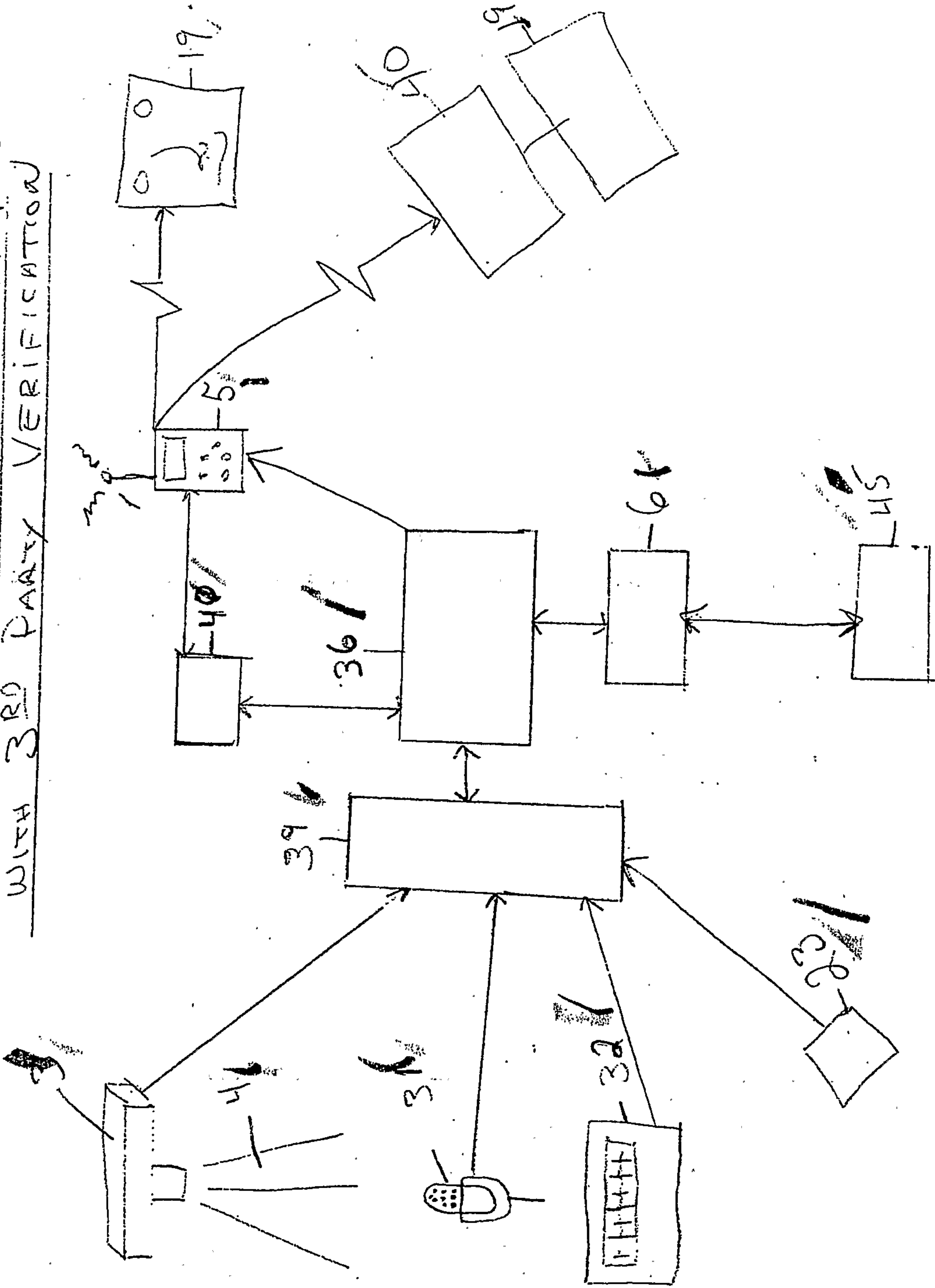
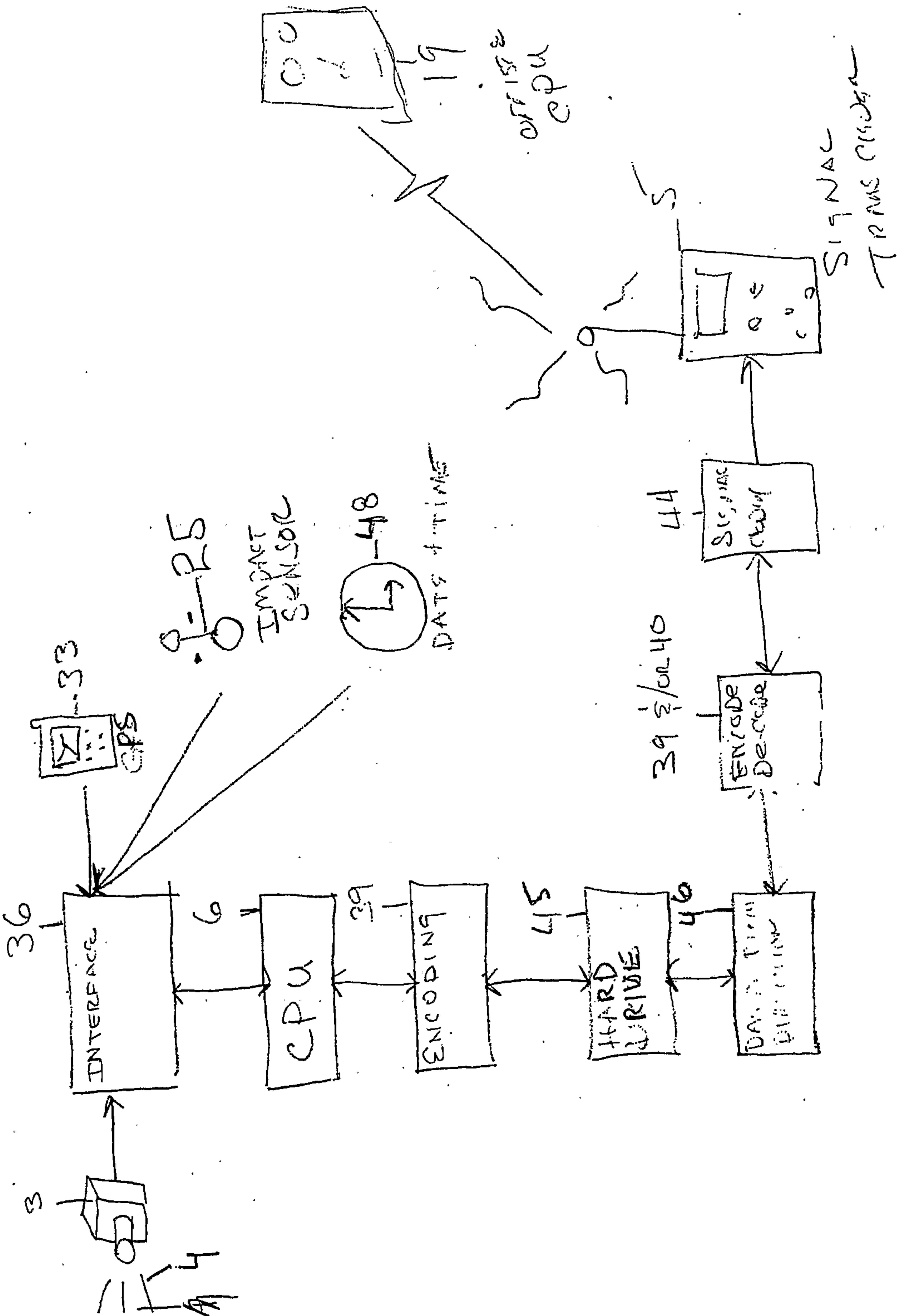


FIG. 15.A

V-RAD



CARGO PROTECTION ONLINE CONTROLS (CPC) WITH THIRD PARTY VERIFICATION

