

REC'D 03 AUG 2000

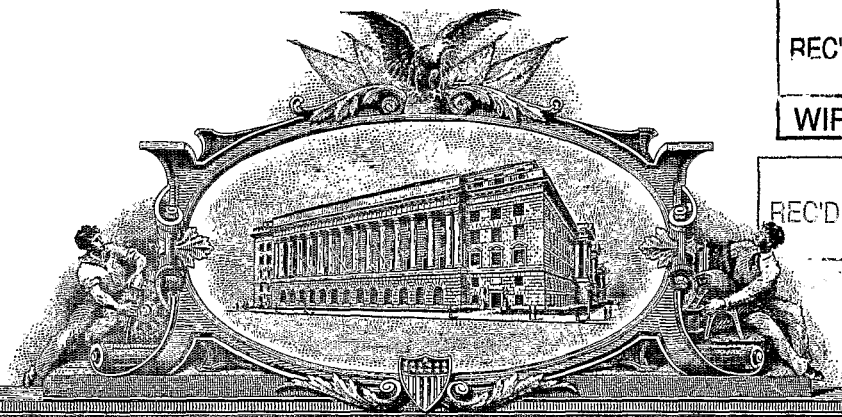
WIPO

PCT

REC'D 03 AUG 2000

3

PI 279113



THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

**UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office**

July 28, 2000

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

**APPLICATION NUMBER: 60/176,818
FILING DATE: *January 19, 2000*
PCT APPLICATION NUMBER: *PCT/US00/16381***

**By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS**



L. Edelen

**L. EDELEN
Certifying Officer**

**PRIORITY
DOCUMENT**

**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)**

01/19/00
1c713 U.S. PTO

PROVISIONAL APPLICATION COVER SHEET

A/P/PCU
U.S. PTO
60/176810
01/19/00

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR 1.53(c).

Docket Number		112756.401	Type a plus sign (+) inside this box →		
INVENTOR(s)/APPLICANT(s)					
LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OF FOREIGN COUNTRY)		
WALKER	Richard	C.	Waldorf, Maryland		
TITLE OF THE INVENTION (280 characters max)					
PROTECTED ACCOUNTABLE INTERFACES TERMED PFNs WITH SECURE MODULAR AND PROGRAMMABLE SOFTWARE TERMED TRAC TO MONITOR, MANAGE STORE AND REMOTELY CONTROL ANY DATA AND EQUIPMENT FOR EVERYDAY USE TO EXTREMELY AGGRESSIVE HIGH SECURITY APPLICATIONS					
CORRESPONDENCE ADDRESS					
PEPPER HAMILTON LLP 600 Fourteenth Street, N.W. Washington, DC 20005-2004 (202) 220-1200					
STATE	DC	ZIP CODE	20005-2004	COUNTRY	USA
ENCLOSED APPLICATION PARTS (check all that apply)					
<input checked="" type="checkbox"/>	Specification (including cover sheet)	Number of pages [177]	<input type="checkbox"/> Small Entity Statement		
<input checked="" type="checkbox"/>	Drawings	Number of sheets [60]	<input type="checkbox"/> Other (specify): _____		
METHOD OF PAYMENT (check one)					
<input type="checkbox"/>	A check or money order is enclosed to cover the Provisional filing fees		PROVISIONAL FILING FEE AMOUNT (\$)	\$150.00	
<input checked="" type="checkbox"/>	The Commissioner is hereby authorized to charge filing fee and credit Deposit Account Number: 50-0436				

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

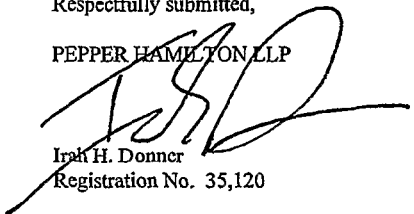
No.

Yes, the name of the U.S. Government agency and the Government contract number are: _____

Additional inventors are being named on separately numbered sheets attached hereto.

Respectfully submitted,

PEPPER HAMILTON LLP



Irsh H. Donner
Registration No. 35,120

600 Fourteenth Street, N.W.
Washington, DC 20005-2004
(202) 220-1200
January 19, 2000
Facsimile: (202) 220-1665
DC: #138720 v1 (2Z1C01! WPD)

PROVISIONAL APPLICATION
FOR
UNITED STATES PATENT

To all whom it may concern:

**Be it known that I Richard Clark Walker, have intended certain new
and useful improvements in:**

**PROTECTED ACCOUNTABLE INTERFACES TERMED
PFNs WITH SECURE MODULAR AND PROGRAMABLE
SOFTWARE TERMED TRAC TO MONITOR, MANAGE
STORE AND REMOTELY CONTROL ANY DATA AND
EQUIPMENT FOR EVERYDAY USE TO EXTREMELY
AGGRESSIVE HIGH SECURITY APPLICATIONS**

Of which the following is a full, clear and exact description:

005710" BFBKFB

RELATED APPLICATIONS

This formal application 112756-401 claims priority from 112756-500 filed June 15, 1999 which claims priority from U.S. Provisional Patent Application docket number 112756-400 filed February 26, 1999 and U.S. and PCT International Application filed January 15, 1999 docket number (112756.202) incorporated herein by reference. This application is related to U.S. Provisional Patent Applications Nos. 60/071,392, filed January 15, 1998 (112756-201), 60/089,783, filed June 18, 1998 (112756-300), incorporated herein by reference. This application is related to U.S. Patent Application No. 08/975,140, filed November 20, 1997, and PCT Application No. PCT/US 97/21516, filed on November 24, 1997, which claim priority to U.S. Provisional Patent Application No. 60/032,217 filed on December 2, 1996, all of which are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

Due to the basic need for an inexpensive protected electrical interface control and management system this inventions PFN and connectables has been configured to allow for the rapid conversions of Commercial Off the Shelf Equipment COTS products to handle hostile environments e.g. harsh chemicals, rough service, tampering, life-threatening substances, e.g., radiation, medical, industrial wastes and toxins and the many needed national defense applications for a more extreme protected electrical environmental package against, e.g., Microwaves, or any Electromagnetic Fields (EMFs) generated from conventional blasts and or nuclear weapons and or weapon grade magnetrons designed to disrupt solid state circuitry, etc.

So this application has been developed to continue the normal commercial and governmental uses of the protected accountable remote and automated control system

006110.03894.F09

on all equipment known as the Primary Focal Node or PFN. The standard PFN always provided a monitoring system and/or network to record and report on aggressive remote and automated control as well as provide more accountability and versatility to any security system with more control options. RPV and many automated and remote control military systems eg automated weapons exist today and this was not the major focus or thrust of this application. The major purpose of this application was to create a universal standard protected interface platform that will benefit the present developing remote control and robotics in every day life and also provide for the quick accountable conversions for national emergencies, military operations and extremely aggressive security options. To allow for the control and management of these devices and systems by the proper authorized government agencies charged with Public Safety and National Security in a cost effective manner.

The Primary Focal Node PFN is a Protected electrical interface system of all electrical components on a host piece of equipment, but it specifically provides communication and computer controllers with two local levels of memory storage in a physically protected encasement to provide accountable remote and automated control and data management.

This standard PFN\TRAC\FACT\DES\CEW management system has been enhanced in this application for higher security functions and has a plurality of responsibilities including surveillance, remote control in hazardous environments, and a remote monitoring system to include, a network of on, in, out, and off board devices working together with people through software and hardware interfaced components to provide security services and make machines and their actions accountable, through safe, secure communication and control devices in real and/or very near real time. This is accomplished through modular and programmable software termed TRAC which stands for Trusted Remote Activity Controller.

The invention as always is designed to account and provide for various levels of remote control for all machines, vehicles and equipment functions, as well as alter them, to be suitable for certain environmental conditions. Specifically, in this application the invention or device employs the Protected Primary Focal Node (PFN) on every piece of equipment, mobile and or stationary and out fits the PFN with any and all sensors A/V equipment to report on the physical state of any designated secure area and its equipment

components as well as remotely control the same equipment either locally or at any progressive level of monitoring and remote control network to extend to and or include a worldwide capability, with any number of security terminals if so desired.

Along with this completely described system is additional security devices networked together as various hardware, hardware embedded firmware and software TRAC and FACT Federal Access Control Technology that protect and condition any signals through encryption technology e.g. DES or PGP as might be required to complete these accountable operations locally, regionally and around the globe in as secure a manner as warranted both governmentally and or commercially.

So for these security concerns this application will deal with three additional properties. First, the PFNs must be able to specifically provide reliable remote control function in these high security and destructive environments. For this to be possible the PFNs will be physically constructed to handle highly specialized environments, for unusual rough service applications and even be armored for ordinance protection, as well as shielded from radioactive environments, electromagnetic fields, bio and medical waste and \ or harsh chemical environments, extreme temperatures, ect. then the PFNs must also be able to transmit and/or store their data in secured communication protocols like the Data Encrypted Standard (DES) for government purposes involving high security. And in Pretty Good Privacy (PGP) like Netscape, etc. for commercial high security or the encrypted codes some of the monetary institutions use. These DES functions are performed by specialized chip sets that have physical separation within the chip to process the sensitive data and are in place on both ends of any transmission/reception process at any level if need be, e.g., on the host equipment and local, regional and/or worldwide monitoring and remote control terminals. The physically modular and programmable PFNs on all normally manufactured equipment will be designed to accept government DES chip sets for easy government conversion of universal products Commercial Off The Shelf Products COTS to be used in high security control tasks.(PGP) with special FACT access.

In this second section of software development the Federal Access Control Technology FACT will be developed with a National registry and how the program will be run in the varied PFN/TRAC systems. A description of possible Internet Protocols (IP) access to maintain high security for normal accountable aggressive remote and automated control as well as an automated policing of machine activation and activity will also be

C O T S . P F N . T R A C . F A C T . D E S . P G P .

completed by the National FACT Registry in sound constitutional ways and respecting the rights of privacy for the individual.

Finally this high security application requires specific sensory and control peripherals, e.g., radiation detection equipment or any transducers to produce physical data into an electrical signal, hydraulic weight transducers, etc., that will be discussed in this application and the formal on equipment electrical control devices application from the provisional application numbered 112756-300. All these devices and systems are completely described within this application, and the other the related applications incorporated herein by reference.

However, the reason this application is being filed separately and specifically is that it defines the specific commercialization of the high security uses of the invention for large commercial and governmental use. Hopefully world stability and organization can be improved through the invention . And a continual socio-economic technical development can be maintained and harmonized to best preserve the optimum physical environmental state for human existence and an improved quality of life for all.

In the related patent applications, the PFN is described as a hardware device that is called a protected primary focal node that ultimately can be placed almost everywhere for remote monitoring, management and control including any vehicle, machine or piece of equipment . Basically, it has been designed to monitor accountably from a secure local environment, and provide aggressive remote control capability to equipment in any physical environment. This will include any and all actions of machines and or man for the purpose to acquire specific data on conditions actions and or functions; and to record this data on location, as well as, report back this same data redundantly to any appropriate concerned individuals, and or the public in general through wireless and wired communications to computer networks and data storage systems. This can be a closed circuit monitoring and remote control system e.g. physically isolated or transparent on the (IP) with encrypted level seven application layers combined with random timed entries as firewall protection) , and networked either publicly and or privately on a larger scale. It may utilize and or include in many cases the World Wide Web for inexpensive mass access to handle data, which will be provided medium to relatively

SECRET

high commercial security protocols through these software innovations of PGP and other Commercial Off The Shelf C.O.T.S. products. Many such companies today have web sites and security firewalls to keep out unwanted hackers..

This patent will have some focus and utilize existing C.O.T.S software products that are available today and are easily configured for the purposes, stated throughout all the related patent applications. It will also, however, offer proprietary configurations for new uses of any utilized C.O.T.S. software products as well as, provide a unique modality to handle data in an accountable manner in the PFN\TRAC and or FACT system. Or for the use of TRAC\ and or FACT with any other processor that require accountability for activity controls and or sensor inputs. The reason for such a high concentration on COTS products in this technology that provides a protected universal interface is because the communication industry, computer industry and inexpensive memory storage are all moving so fast in offering cross over products one of the main purposes of this invention is to provide a secure environment of plug and play interfaces for these developments to give inexpensive versatility and to make them all accountable In the data they handle and host controls they effect, while still maintaining free development and enterprise.

Once again TRAC stands for Trusted Remote Activity Controller and it is for the most part the programmable and modular software necessary to provide accountability to aggressive remote control for society. Fact is The Federal Access and Control Technology that provides authorized government local , national, and globally the real-time powers to control vehicles and equipment use in the safest manner to preserve human life, tranquillity, the environment and social stability,

The objective of this technology is to provide a secure communication and data management system initially in the PFN (the protected primary focal node) with TRAC / FACT system a most unique and ideal software modality, that can be used as a universal program and or a standard, to format accountability for aggressive remote control. The technology will seek endorsement by the insurance industry to provide trusted

SOFTWARE COLLECTION

accountability in the liability assessments and rate assignments for aggressive automated and remote control in any and all such man and machine shared control scenarios.

Automobiles and highway travel and it's safety will be a major focus of course, but this technology is planned to provide this secured trusted analytical data tool for every mechanized ,automated and or remote controlled insurable action and or function . The total goal of this application is to also receive approval and certification for the payment industry and their software products, processes, and protocols . Nationally, governmentally, commercially, socially, ect) for the Banking Industry, payment industry and credit or debit card systems and or for any financial transaction approval. Also and equally the technology will seek approval from the Government agencies and or institutions, and or any Security organizations (, the Automobile Industry, the International Electrical Engineers Association (IEEA), e.g. Consumers Electronics manufacturers Association CEMA, computer engineers and or programmers associations, and or any other Science , Technology and Society concerned citizen groups, organization, and or commercial interests as well as all government agencies. This technology seeks to help create a set of standards for accountable automated and remote control and will work in this direction through any commercialization of this invention.

The TRAC/FACT system and software will be programmable and modular and be deployed as software and firmware in all types of hardware. It will also employ and be capable of processing analog and digital signals and or any and all data streams, encoded and or encrypted signals including; all data, audio and video signals as well as telemetry for man and machine operation and environmental monitoring, along with any other application specific data streams determined as necessary.

This application is providing this proprietary firmware and or software system so that it can track any electrical signal received and or processed by this Protected PFN technology and or any of it's devices as well as, track and record any application specific reactions to the signals by any host equipment, personnel, environmental condition change ; and also, continue the accountability functions for off board tracking , through

CONFIDENTIAL

the management and storage of data handled through the PFN \ TRAC monitoring and or remote control system and or Network.

The remote control accountable software for tracking will require personnel Identification (PINS and or fingerprint or pupil ID), Electronic Serial Numbers (ESN), from the transmission equipment used, GPS, land line numbers , ect., and or any other locating system coordinates. There will be time and date data as well for every appropriate command that results in any application specific reaction performed by the host machine via a PFN, and or due to any remote control command. This will always be standard operational data acquisition necessary to perform any credible remote and or automated function completed with a PFN. Basically the TRAC system in the PFN is a modular system that will authorize and authenticate commands and activities for aggressive automated and remote control with local and remote redundant memory systems. This is how this technology plans to provide trusted accountability for insurance and governmental backing. The manufactured commercial products employing this technology's PFN and or TRAC system's innovation will be responsible for obtaining certification in their design, construction and use by the governing bodies as well as provide FACT access and control protocols for public safety and national security reasons. The FACT system is still completely accountable for any and all that are using it whether they are ,civil servants, high government officials or regular citizens..

The mass of all data collected in real time for a temporary memory shall be controlled by being erased in this re-writable memory and not stored in the permanent memories (local) if deemed unessential by application specific onboard firmware and or software criterion. and not reported redundantly to any remote location unless countermanded by the off board monitoring and control systems that authenticate as valid for this activity.

This technology has provided for it's PFNs and or any other technology's processors or programmable controllers a set of secure accountable software comprised of programs and designed to be modular. The base and or operational system once again is termed and referred too hence forth as TRAC, which stands for Trusted Remote

REF ID: A64500

Activity Controller. This is a programmable and modular system in the PFN that authorizes automated and remote activities and then authenticates the response and stores the data in a plurality of memories. The specific protocols ideally to be determined by standards committees, which will be structured to the application specific guidelines for this technology's deployment with the governing principle to safely and to appropriately full fill society's needs and requirements for accountable aggressive and or passive remote control and robotics.

Brief Description of drawings

Figure 1

Is an illustration showing the monitoring and control system and a PFN enclosure with it's characteristic communication options, processor and computer capability and it's accountable data storage systems, as well as, it's electrical interface connector to connect with a host machine. This is in keeping with the same technology from the first application and the remainder of the drawings will display and describe more varied levels of capabilities and sophistication to meet the present high security requirements needed in special government and

Figure 1a

This figure is the software that provides a Trusted Activity Controller the TRAC system of software and software embedded hard ware or firmware and or microprocessors FACT chips individually assigned and incorporated as identifying circuits and mini processing centers to insure accountable remote control tracking integrity as a system and for any and all individually directed activities no matter the origin of order and or purpose.

TRAC a Trusted Remote Activity Controller has easy technical capability for any and all of humanity. However, all forms of human governance will have to be responsible in determining how to best use this accountable technology.

Figure 2 (commercial high level security protocols).

The protected containment has many various different applications so specific configurations have been deliberately avoided . Therefore, this number two drawing of the high security PFN'S wall is shown ,as well as, how they will be altered to complete their specific tasks for every application and will be ultimately determined by a standards.

Figure 2A

This figure first appeared in earlier related patent applications for the use of pagers the primary communication technology and will be used in one and two way transmission application for the least expensive communication means in PFN's in normal applications and altered in wall structure for higher security applications.

Figure 2B

This is an add on system also appearing in an earlier related patent application and it's wall structure will also vary as per application as detailed in figure 2. This system utilizes wireless or cellular phone service for it's two way communication medium

Figure 2C

This is another built in PFN system with it's two way and locking system detailed in another earlier application for the automotive industry to organize all electrical devices in a plug and play system of drawers and compartments and displays numerous components and devices. This system can also have it's physical wall structure customized for specific high security applications

Figure 2D

This drawing continues on to develop 2 C on the interior of the dash PFN in a mobile piece of equipment. showing in greater detail some possible movement component and device and this drawing as well appeared in an earlier patent application

Figure 2E

This figure shows three drawers which are a continuation of 2D as a possible arrangement of components for this multi interface system for electrical components.

Figure 2F

CONFIDENTIAL INFORMATION

Two F is the first of two figures showing a proprietary electronic heat seal system to insure there has been no tampering with the protected PFN are for legal evidence.

Figure 2G

This is the second drawing of the security seal and it describes how the seal functions

Figure 3

Shows the two basic PFN communication categories which are being developed . There will be one way transmission devices and there will be two way transmission devices. The drawing also illustrates the monitoring and remote control system from the local level to the global level. The figure also shows all the qualities and peripherals as well as the security systems for conditioning any two way signal transmissions.

Figure 3A

This is a self explanatory chart to show the accountable data storage for on board in the PFN and off board within the monitoring and remote control system. This chart can be referred to when reading and viewing figures 3-4-5 & 6 with all the different types of communications detailed. The chart will quickly provide the basic report back properties and data storage systems to expect from an individual PFN by the communication service it is employing. However in many cases a PFN might interface a plurality of communication systems.

Figure 4

This drawing is of the simplest one way communication PFN and these basic electronics have already been prototyped used and proven from and for the other related applications. Basically with the one way communications systems data storage is on board the host in the PFN at two separate locations and require physical retrieval of the data. This device in it's most basic form will not report back to any remote control and monitoring system, but can be sent messages, which will activate preprogrammed responses.

Figure 5

This an illustration of the simplest two way communication systems and the necessary security devices to condition the signal with encryption for high security

SECRET 014900

protocols. It is basically another flow chart showing the data from the remote control and monitoring network as well as all the data and control signals to the data storage and the peripherals through the many possible processor options. This is the same as figure 4 , however it is in two directions with the remote control and monitoring system and there by creates three accountable levels of data storage on and off the host piece of equipment. Two levels on the equipment and at least one remotely stored copy of any pertinent data.

Figure 6


Employs the most sophisticated high security two way communication capable of full real time video with either cellular or digital phone or any radio frequency specially delegated for these purposes. These types of devices will carry all types of report data signals and cost will be proportionate to the level of sophistication and the hardware and software required to support the services desired by all accompanying peripheral devices.

Figure 6A

This drawing details how drawings 3, 4, 5, and 6 are merging the communication technologies with computers and memory as well as automated control systems and data management and sensory systems. And more specifically it details the growth and development of the components and separate devices into one set of secured accountable PFN circuits and provides for all the future commercial Off The Shelf Products to be used in the PFN. With plug and play universality but achieving the same stated purpose as has been proposed for the invention all the time. Which is to provide a secure protected accountable electrical interface.

Figure 7

Depicts a security enclosure and in this case it illustrates a nuclear scenario requiring unique types of monitoring and remote control. This could be any security scenario with different requirements and specific peripherals with varied protected circuits, but with the same need. To monitor and control a restricted secure area with accountable remote control or robotics from local, regional, and global monitoring networked together and also in a secure manner.


Figure 8

Illustrates the many varied high security purposes of the installation secure area system depicted in figure 7. It shows some of the governmental uses, and commercial applications for a secure installation , that are hazardous and can be enhanced by unmanned operational functions. eg oil , gas and chemical plants, medical waste and sewage facilities, nuclear substance use, and nuclear waste storage and a multitude of other science , energy technologies as well as monetary processing either in hard currency or credit - debit data

Figure 9

Is a list of the allocated frequencies and their use and the agencies that use them

Figure 10

Is a continuation of the list of allocated frequencies from figure 9

Figure 11

Is a more extensive detail of the TRAC software flow and the all the application specific programs running in the Trusted Remote Activity Controller

Figure 12

Shows a world view of all the communication linked PFNs and their application specific uses in normal everyday life.

Figure 13

This ia a 26 page listing of all the national government agencies that are supporting web pages and this invention details how to hyperlink them into four public web account pages utilizing the data recovered from the PFN/TRAC system and processed for or by these agencies as part of public accountability and interaction with government and commercial interests.

Figure14

This drawing further details the PFN applications and shows there uses in every day management applications

SECRET 011900

Figure 14 A and B

Is two pages of charts and descriptions that were taken off the Internet detailing The International Standards Organization or (ISO) Reference Model. And with a basic discussion in reference to the Open System Interconnection or the (OSI) of networking including the seven levels to creating net work communications between computers and how FACT and the Registry can operate.

Figure 15

This drawing introduces FACT as individual chips that will be manufactured into all electrical components to track and control their authorized use and value that use.

Figure 16

This illustration details how the FACT chips work inside the PFN/TRAC system to be an accountable and well organized use of electrical devices on each and every piece of equipment. The individual chips in each component or device identifies the component to be recognized by the National registry after the initial data is processed by the PFN\TRAC\FACT computer programming when it is connected to the uni-buss either in the protected containment of a PFN or some input output port

Figure 17

Is a further description of the FACT TRAC system that originates in the PFN device and pinpoints; interaction in any platform of communication to be identified as legitimate electrical technology that is made accountable in it's manufacture or creation and legitimate and accountable for it's use civilly.

Fig 17 details National Regional and Local Governmental control and management and the employment of the FACT system secondary failsafe check to insure accountability of legitimate product use.

CONFIDENTIAL

Figure 18

Is a more detailed view of the devices interfaced to perform the Federal Access Control technology FACT. And Commercial Encrypted Web CEW technology to perform secure and accountable tasks through the three main communication mediums , of one and two way Paging, wired and wireless telephone technology and all forms and frequencies of radio communication. This drawing shows the Data Base Connection and the Internet use.

Figure 19

Shows the lines of interactive communications from the PFN all it's sensory inputs the commercial servers and public provided nodes linked to local government state and national government and screened interfacing with world organizations and the uses of all types of communication links to provide a secure accountable network.

Figure 20

Shows a base application of the software flow activities both at the PFN level and in the main registry and a typical interchange concerning the main purpose of a such an accountable network .e.g. To reduce the crime of component, device and or equipment theft, provide greater National Security through properly identified and qualified components being made accountable for performing automated and remote control activities for society's and their institutions. And finally to provide greater accountable public safety e.g. a fail safe capability by being able to individually address numerous similar functioned electrically inventoried devices as operational through PFN management devices to perform a task . e.g. Cell phone failure and a pager is interfaced switch communication use to the pager system to receive signal for an authorized remote command. Even a standard car radio or audio system interfaced through the PFN will be able to receive one way

E017E31B-01100

communications to perform PASSS The proprietary Aggressive Slow Stop, and Securing of a piece of equipment.

Figure 21

This diagram is more descriptive of the software functions of management and control commands. It shows basic driver and or owner notification functions and those that could be completed with out notification as per constitutional law to be written and legislated extending court order wire tap and phone taps being extended to use of this security function in the PFN/TRAC system and incorporated into FACT software protocols.

SUMMARY OF THE INVENTION

These innovations have been predicted and partially described in the earlier applications. They are the security protocols and are intended for the High security development mentioned in the "Stop and Control Box", Black Box, and Billing Boxes and their combined functions that were described in all the related patents but most especially detailed in the formal patent # 112756-202 as the secure and protected PRIMARY FOCAL NODE or (PFN) also with all the possible computer networking including the Internet..

Along with the varied PFN devices that will be attached to all equipment ,machines vehicles and environmental sensors and devices is the evolved third embodiment of the first application . A flexible in size and capable monitoring and remote control system that can be singular and local or networked to any extent with all the variations of PFNs and other systems if so desired through FACT software and national and local connectable FACT registry . From the first application of this invention has prescribed a secure accountable remote control electronics package as it's a major objective for this technology . So it is only fitting that even the first commercialization of the invention increase security for

life, society, government, business and industry ; because of all the basic accountable features the invention can provide to any present security management and or control system. Some of the enhancements are obvious in the areas of impregnable electronics, and also the versatility in providing levels of inexpensive remote-control for secure areas requiring automation to replace and or reduce personnel at risk.

The invention provides for at least three levels of accountability in it's most sophisticated functions . Two on board and at least one in a remote location. The invention has always claimed to provide a secure physical environment for the electronic components and devices, but in this application the PFN's are specifically designed to protect any of their transmitted signals by first conditioning them by encryption, so only the authorized personnel and terminals can decipher their encryption's and gain access to the data. This security protocol is also carried all the way though the system and will therefore easily marry into any existing system, which requires these same Protocols DES and PGP. Which stand for the government Data Encrypted Standard and the commercial versions Pretty Good Protection, However, PGP suppliers will be required to coordinate and incorporate their encryption with FACT software algorithms To provide for the Federal Access and Control FACT registry of component, devices and equipment, ultimate interdiction and control when they are going to perform aggressive remote and automated control activities in a host machine. (This is legal for the automated equipment to be policed by societies automated policing systems)

The monitoring and control systems for high security application will most probably be closed circuit with an individual set of government allocated frequencies, and specialized hardware firmware and software (Government \DES systems). However, with the software, and or commercial firewall protection known as pretty good protection (PGP) inexpensive monitoring can be provided in near real time with only marginally diminished security in any direct PFN

CONFIDENTIAL - 019900

transmissions to the world wide web WWW phone node servers and their inexpensive gateways and or any networking from the local computer terminal to a WWW server phone node. This option for many small and medium commercial operations will be provided more economical possibilities for their semi sensitive or less secure needs to monitor current events at isolated installations globally in any specific installation . If through this casual monitoring it was necessary to give a remote command to a PFN controlled piece of equipment based on the web image The remote control commands can be given through regular phone services and or any other privately owned and operated communication system, that the PFN has as a communication device on board for. This would allow for limited use of expensive phone services or commercial satellite communications for the long process of monitoring a remote secure area and only require the expensive communication technology to send short commands. These monitoring functions were described in the second patent for a community web page monitoring of unrestricted governmentally prepared PFN generated public information data streams. The difference here is the use of PGP and or DES or any encryption to conditional a signal limiting access to these types of data streams whether they be commercially generated and altered or governmentally controlled . The other security measures are limited access to a web site or controlling access by special identification measures e.g. pin numbers and synchronized timed personal access number cards. Otherwise the automated dial ups to the server phone nodes or web gateways could operate the same as the second formal application 112756-202 . Or the use of the local control computer 300L to do the dial up and or act as a RF repeater station for a local page network of PFNs which would make the phone node connection to the web (optionally automated) . This could be utilized in much the same manner as has been described in the second patent 112756-202 for the separate government agencies that provide direct phone node equipment to their agency network as well.

SECRET 011990

However, this describes how the PFN can be first sold as a commercial product , but to coordinate and use this technology on a massive bases the most important development in this application is to use the PFN/TRAC/FACT Registry system in harmony with all the PFNs and an entire web that provides for individual PFN direct access to the registry and or though any and all isolated systems that have their own gateway to function (but FACT licensed) through the PFN\TRAC \FACT system . (this development will be governed by legislated law ,codes, regulations and standards in the future but for all intensive purposes will be detailed here and now so that anyone can understand this accountable management system and so those skilled in the arts could easily construct it)

As described in the second application 112756 202 and 112756 300 for the spider eyes systems all the PFN activation's require all the electronic serial numbers , land line numbers and or RF ESNs from all communication links as well as personal ID verification e.g. finger print, card swipe and or Pin numbers, or any synchronized personal ID time changing pin code verification devices or systems, ect. And along with this data is always the date and time for any remote control command, which is always accountably recorded with all the electronic serial and ID numbers ect as the command string in the PFN any remote control contact. Also , any response telemetry data generated from the action to a remote command is recorded and stored for an application specific time period and then either entered into the permanent PFN record storage or delete for space. And any and all installation PFNs that are working in concert (net worked together) to achieve a remote control action will also establish their telemetry records in the same manner providing a multitude in many layers of accountability header provided with the appropriate FACT ESN , MIN, VIN or necessary FACT manufacture data and nay activity application data that is programmed into the firmware or software.

This application details the quality and properties of the accountable modular and programmable software termed TRAC that authorizes and

SECRET 011900

authenticates commands from wireless and land line telephone and or RF equipment and or light transmission technologies to remotely activate and confirm automated controls and functions through it's PFN processors controllers and or computers. As TRAC processes this data in a secure manner it stores it in a protected storage on board a piece of equipment in this technology's PFN on location and in the two way transmission PFNs it reports back to at least one remote location to achieve at least a third redundant memory storage. The reality of the invention is proven in the feasibility prototypes of the earlier related patent products. However, the need for governmental and commercial collaboration is essential to the entire FACT system 's Reality

This TRAC system was designed to distribute communicated commands to their appropriate application specific preprogrammed protocols, while authenticating the authorizations and preserving and accountable record on both sides of the remote control communication scenario and through out any redundant transmissions or data storage. The TRAC system of software has been designed to develop a Trusted Remote Activity Controller for all of societies needs regarding accountability and liability as well as to preserve and organize secure modalities to manage and control automated equipment, and financial legal transactions.

With the advance in electronics, communications and computer processors the automation of equipment is rapidly approaching aggressive remote control and robotics and needs to be made as accountable as the owners and operators who have been solely responsible for machine control in the past. Because, control responsibility will be shared at first between man and machine and might very well always be this way; accurate telemetry of both will be essential to provide organization and proper management and legal control in this scenario. This technology's PFN protected primary focal node and The TRAC software system has been constructed to provide the means to accomplish these control and

CONFIDENTIAL

accountability tasks and to serve as an electrical interface, physical platform, and software control center to write standards too.

These are just some of the increased synergistic benefits added by the invention's secure and accountable remote control when made part of any existing security system. The invention's security uses are endless, because of the great inventory of possible C.O.T.S. components, and devices that can be integrated and interfaced. The designed universal plug and play versatility has been deliberately developed to combine and work with all other pieces of equipment and systems where ever possible. This has always been another goal of the invention from it's inception. To provide a practical focal point that is a universal physical platform to support a versatile electrical interface for responsible remote control for every piece of equipment, machine , vehicle and environmental need to increase public safety ,national security, to provide just and fair monetary exchange and respect for each individual in a society. Accountability for the use of equipment and Data acquisition is the best way to achieve and assure these things and it must be built right into the interface and protected as well by backed up remote traceable memories.

All the patent applications first combine all these present separate parts, products and systems as interfaced separate entities and in this application they are progressively consolidated and standardize the electrical interface and circuits of this protected physical structure to the most concise set of universal application specific controls in appropriately sized physically protected containment. (known as a PFN)

Through out this application all the security ramifications and uses will be described in detail . And with the related applications incorporated herein by reference the list of possibilities is not only endless and feasible, but also practical and a necessary direction for future security scenarios for all aggressive remote control . This application combines security technology with machine communication to create commercial automated and remote control with an ideal

FOR RELEASE UNDER E.O. 13526

organizational platform to set standards for society in general and all the regulating government bodies ,FCC, FAA, DOD, DOT, FBI, CIA, NSC, and various professional organizations IEEE , Fire and Alarm industry, insurance industry and on and on .

At no time does the invention in any particular field attempt to set standards or criterion for any specific technological applications or use. But the invention address almost all responsible modalities and or issues in a clear and evident manner to practically achieve all the claims of this invention. The invention only seeks to provide the present world's technologies a set of more universal secure accountable electrical interfaces of physical platforms for remote control and robotics, which are designed to provide accurate information and control options reflective of human needs with present and future machine interaction . With this accomplished hopefully this will improve the likelihood and chance that logical common sense and scientific decisions by societies, their commercial interests, and their authorities can be aided in making the best choices for the world's populous to secure peace, tranquillity, as well as, develop a healthy respect for one another, and maintain a safe environment in a timely manner with as little unnecessary disrespect, disruption , depravations, destruction and death. Ideally individual freedom will be guaranteed by a developed social respect for the individual secured by accountability, because most certainly personal privacy is going to continue to be reduced by all of these developing data acquisition technologies, which also have the potential to provide a better quality of life in general for the whole of humanity. This is an important issue and always will be.

The invention has been designed to provide humanity with the tools and capability to provide secure organization and informational data for this most natural and appropriate human knowledge quest and assist in obtaining an optimal growth in these directions for humanity's development , while maintaining fairness and order for all individuals to develop in their individual existence in

0057080409

using these extended freedoms and tools responsibly and respectfully and pain of the law for any miss conduct.. But this invention's implementation and any societies use of the invention is and always will be in their hands and have to be responsibly shouldered by all of the individuals of any society that uses it.

Detailed description of drawings

FIGURE 1

Is an illustration showing the monitoring and control system and a PFN enclosure with it's characteristic communication options, processor and computer capability and it's accountable data storage systems ,as well as, it's electrical interface connector to connect with a host machine. This is in keeping with the same technology from the first patent application and the remainder of the drawings will display and describe more varied levels of capabilities and sophistication to meet the present high security requirements needed in special government and commercial applications. FACT is introduced as the Federal Access and Control Technology that will be running in all remote control capable systems governmental and civilian. It is an encrypted operational data system software that will allow for accountable access to all such systems and under proper court authorization allow for undetectable monitoring and control of any and all equipment. Fact processor chips will be in all responsive connectable components for remote control as well as in expensive electronics to keep track of their legal and illegal use through and by any PFN system running TRAC/FACT software. TRAC stands for Trusted Remote Activity Controller and is the base operating software system operating in all PFNs

First however, is the base hardware components and systems running these programs of which TRAC & FACT are only two of them. The components in figure one as numbered are as follows. Number 300 shows all three levels of a possible network of off board computers in which the local computer is the standard gate way, but not the only control terminal and it is not a necessity that

CONFIDENTIAL

the control communications even go through the local terminal. With the use of cellular phone technology, RF signals, and paging devices as the receivers and transmitters, signals can be sent from any terminal if so desired. (e.g. emergency situations). And also by employing the equipment identification system (ESNVIN) and or (ESN SN) or MIN protocols and personal ID devices properties and qualities detailed in all the earlier related patents for the (spider eyes program 112756-202 and 112756-300) coupled with the on board data storage devices numbered 105-106-107 in this drawing . And the off board report back data storage; provide total accountability for remote control activity which can be established through the entire system from all of the off board monitoring and control systems to each individual peripheral system attached to a PFN numbered 200-204 in this number one drawing and most especially with the incorporation of TRAC and FACT soft ware programs. The multi numbering is for the different styles of security and protective packaging of PFNs and data storage devices and systems, which are all detailed in great length in the earlier related filings.

100 is a wireless phone, either cellular, digital ,satellite or even cordless either as represented as a hand held C.O.T.S. device that has an interface modem and or cable to connect it up with one of the five computers detailed in the preceding related application 112756-202. or as an IC chip set integrated circuit and or interfaced with any of the onboard processors, programmable controllers or computer boards either by edge connectors or direct hard wiring or IEEE couplers. And 100 can also be PCMCIA card or "Complete Card" TM Cell phone card with antenna. (This system will be first utilized in all prototypes including high security.

101 is the standard time honored pager in this drawing showing only the reception capability of the standard C.O.T.S. pager. This is done to accent that there is a real cost effective use for one way paging in high security applications as will be completely described within this application. However, also in this

001756-01900

document it will be equally illustrated that the new reflex paging protocols of Motorola can also serve inexpensively and offer limited two way communication capabilities. The first related application totally details many different modalities to utilize the standard paging devices and is incorporated herein by reference. However, also through out all the related applications the incorporation of C.O.T.S. paging IC. chip sets accompanying circuits and software protocols have been incorporated into PFN consolidation of circuitry and size, as referenced by the design use of Motorola's Create-a Link TM combining communication and processing, in some limited switching functions in the protected accountable PFN system.

102 is any other RF frequency that can be used to send and or receive either a guarded or unguarded signal. to a PFN device. And the following frequencies are listed in an Allocation table as figures 9 and 10 of this application as they are known today. The list is in no way to be considered the only frequencies that this invention claims and in fact any and all wireless communications and hard wired communications are claimed to fall within the nature and scope of the invention when they are used in an accountable and or protected interface for remote control.

103 refers to the proprietary Parallax computers stamp I and stamp II and 104 refers to all five of the 100 Euro-board mini computers named in the preceding application 112756 202 with their varying degrees of capabilities. And also in this formal application there will be a complete set of drawings detailing the prototypes to make them more resistant to EMFs and other damage from radiation for the high security and hazardous or hostile environments.

105 -106-107 is the on board data storage components of the PFN. However, there is only 2 levels of memory or data storage generally planned for in the PFN. One is a re-writable memory recording predefined data unique to equipment and or personnel. The second is priority data which is stored in a non-volatile and protected memory (determined by application specific protocols). And

CONFIDENTIAL

number 108 up in the 300 block of computers networked together illustrates at least one remote storage out of the PFN. And this will be a redundant storage of the same application specific protocol data stored permanently on board. This provides three last minute comparable records which are all timed and dated for analysis and accountability. The number 105 generally refers to embedded hardware, firmware , EEPROM, and or flash memories and 106 refers to hard drives and 107 to writable CD and MO disks as detailed in the earlier applications . These can be part of a integrated or interfaced circuit with any of the processors and or mini computers and or stand as separate components interfaced through hard wires and or physical connectors, which also has been thoroughly detailed in the earlier applications. Anyone of these data storage components can function as re-writable data storage or as permanent storage.

108 is the off board storage and it is also detailed in earlier applications but it is safe to say that all data stored for these high security applications will have specific systems and protocols to manage any stored data. TRACS and FACT will be detailed through out this patent application as an exemplary software protocol for handling this data on and off the board.

FIGURE 1A

This figure describes the Trusted Remote Activity Controller TRAC, which is the basic operating system to provide accountability . It also calls for two standardization efforts for internal communication and external communication, for universal connectability which will be elaborated in much more detail in figures 6A ,17 and 19 Trusted Remote Activity Controller (TRAC)

OPERATION

The Trusted Remote Activity Controller provides all local vehicle or device control and event storage relative to PFN (Primary Focal Node) operation. It

2025 RELEASE UNDER E.O. 14176

interfaces to any RF telemetry link, which may consist of a one or two way paging system. More sophisticated links could be used such as digital cellular or PCS (Personal Communication System). Typically, a Remote Management System (which may be as simple as a single page, or as complex as a controlling PC or Server) initiates a TRAC function, such as an automated slow, stop and secure sequence or involves robotics including guidance systems more and varied speed control and or any accountable aggressive remote and automated function. The signal or paging command is received securely via encryption) and decoded by the TRAC. Optionally, a local display or audio speaker may provide local status of the TRAC function being executed, with appropriate progress tones, voice queues or displays to provide a local operator feedback relative to the progress of the function.

In performing the function, all Activity controls are initiated by the TRAC and monitored by the TRAC from start to finish. This is accomplished through feedback sensors. Feedback Sensors may be electrical, mechanical, fiber optic, infra red or other technologies. Since the function being performed requires a high level of accountability and trust that the sequence was in fact executed properly, every step of the process is monitored through appropriate feedback sensors to attain the reliability and trust required. This positive feedback in the TRAC is the key feature which distinguishes the TRAC from other electronic or software controllers; making it a fully "trusted" system for the task being accomplished. Additionally, all events and status relative to the function are recorded locally in the Local Event Storage Memory. This is termed the System Function Data. The level of redundancy in storage of System Function Data and the level of

COPYRIGHT © 1999

additional feedback and checking required in order to verify the Activity or function was accomplished properly, is directly related to verification requirements. These requirements may be regulated and approved by local or federal law, law enforcement or insurance agencies, World Bank, EPA, ICC, SEC or other regulatory agencies.

Interim progress of the sequence, activity or function may be optionally transmitted back to the remote management system through a 2-way phone or paging link. This may occur as the function is executing or may be programmed to occur after completion of the sequence. In any event, local, redundant storage of the event is always contained within the PFN for subsequent or simultaneous retrieval of event information and proof for accountability purposes. The PFN enclosure and TRAC monitoring of tamper sensors guarantee the information has not been compromised.. Also unique sealing systems further provide tamper detection Other types of information along with the System Function Data may be stored in the TRAC Local Event Storage Memory. This auxiliary information may include digital or analog data not directly related to the function being monitored and executed, but important for evaluation and determination of liability, collection of evidence or environmental data. Examples of these include road condition information or surveillance audio and/or video.

IMPLEMENTATION

TRAC implementation may be accomplished in many ways, depending on space or funding constraints and level of integration required for the system. A PCbased system may be in the form of a desktop system, laptop or embedded system (PC 104) with a dedicated DOS or Windows based TRAC program, consisting of machine language, Basic, C, C++, Visual Basic, Visual C or C++, or other high

SECRET

level language which accomplishes the TRAC function through software control. Interfaces to the System Under Control (SUC) may be accomplished through appropriate I/O cards, either analog or digital. PC compatible Modems or Cell phone interfaces provide the interface to the Remote Management System (RMS). SUC and RMS interfaces may be in the form of ISA, PCI, PCMCIA, VME, Compact PCI, Future Buss, or other commercial interfaces compatible with the PC-based system used by present technology. More compact and custom implementations of the TRAC may consist of dedicated state machine controller implementations in which TRAC functions are executed through embedded firmware. These implementations may incorporate multi-chip solutions using EPROM or EEPROM interfaced to Arithmetic Logic Units (ALU), I/O ports and discrete memory elements a basis for FACT Federal Access and Control Technology where microprocessor and ever expanding memory circuits and devices are emerging. They may also be microprocessor or microcomputer based. A large variety of board level products are commercially available for such an implementation. Single chip or high density implementations might consist of Field Programmable Gate Array (FPGA) or Application Specific Integrated Circuit (ASIC) based devices. These implementations may incorporate all sequencer, firmware, I/O and storage functions on a single device and would provide the highest level of integration and smallest size. Display, Video and Audio (Auxiliary Data) for the TRAC can be in many forms and types. These may range from analog systems, in which tape or other magnetic media store the analog signal, to digital systems in which data is stored on hard disks, EEPROM or RAM. Data format may be modulated through FM or AM, compressed, packetized or otherwise encoded for reduced

CONFIDENTIAL

bandwidth or for transmission over the Internet (packet audio and video). And even modulated over power connectors to save space and individual material component use. Figure 1A is to show a software diagram that can perform remote and automated controlled functions and also authenticate their performance. It is also a precursor or base operational system to operate more controlling management system in a socially responsible and accountable manner. In this patent application the major issues of freedom and privacy will be legally addressed with humanity's need for civil control and all will be held accountable.

FIGURE 2

It is important to remember that any structure designed to protect the electronic integrity of any interface and performs the described functions of a PFN as well as, provides protection for any of it's essential peripherals to increase performance, longevity, durability or to increase reliable service, and or to better perform accountable remote control like protecting a system like the PFN/TRAC system in any environment or from tampering fall within the nature and scope of this invention and all of the above related filings. This is and always has been a major attribute of this technology. To be either universally, and or generally and or specifically construct for the purpose of protection against any rough service environments and or vandalism or tampering. (The demonstrator prototypes for high security will also have detailed drawings in this formal filing that will basically divide this technology into two product lines of capabilities determined by the type of communication technologies employed. They will be either one or two way transmission capable. However, they may or may not both use the same containment structures or provide both forms of communication if so desired. They will once again utilize pager technologies, cellular phone technologies, and or any other RF systems, as well as, light communications either independently or in combination, as has always been maintained throughout all of the related filings.) The only other governing

SOFTWARE OF THE FUTURE

factors will be the requirements of the host equipment, the desired functions or capabilities, and it's operational environment. It is these considerations that will determine the physical protective characteristics and configuration of any specific PFN.

The other related patents incorporated herein by reference already detail pager and a cell phone PFN s for other commercial industries with less secure requirements. So many of the same innovations and devices will be employed in these high security protocols. Another exception is the detailed described development of greater signal security_not just through physical protection of the PFN and peripherals , but also, accompanied by special electrical hardware, firmware and or software TRAC\FACT that will handle encrypted conditioned signals generated from a PFN or to a PFN if need be. Also, in this formal application certain other circuits and or electrical components will be specifically designed and or chosen, because they operate well in high electro-magnetic fields (EMF s) and or ectro-magnetic waves EMW environments and or radioactive environments . This will also be the case for many other hazardous or hostile environments (Application specific physical and electrical structuring of the PFN)

In figure two only the wall structure is discussed at this time as it will be constructed for specific applications. Ideally the wall will be constructed as a laminated or composite structure for the most cost effective manufacturing, however, in the very specific security applications these wall components might well require specific customization and because of their limited markets increase the cost of a PFN. Ideally universal structures will be standardized in application specific areas to keep cost at a minimum.

200 is the thermal insulating center lamination between two walls, the outer 201 and the inner 202. This center as already detailed in earlier filings and can or will be composed of either fiber glass products, gypsum, fire gels (from diapers), solid smoke silica, mica, asbestos, or asbestos replacement products , Teflon and or high temperature plastics e.g. polysulphone. all of which would either be adhered to 201 and 202 or merely sandwiched between the two walls. However , one product has been chosen for the experimental prototypes, and it is called "solid smoke" and is a product developed by

COPYRIGHT © 1998

N.A.S.A. for the space tile replacement and is completely detailed in earlier application 112756-202.

Due to this center area 200 being a somewhat flexible fill insulation area between generally two solid structures a wire screen mesh, net, grid, or grill of metal properly spaced and constructed from metal products possibly copper, lead, ect. will be placed to block even more EMF \ EMW and or various forms of radiation in special nuclear applications ect. To achieve an additional radiation screen. The mesh can be pressed or impregnated into this insulating composite section in the center of these two walls to add greater protection for the electronic products housed inside the PFN. This center can and will be designed to provide a soft seal when mated with another section of a PFN wall that will be resistant to the normal elements and harsh chemicals when end sections of 201s are butted up to other 201s end edge sections e.g. corners (the same for 202s) to provide another surface to seal upon e.g welding, resins, glues.

Manufacturing can also reduce cost by making three concentric boxes or containers of any application specific PFN shape. One the largest out of 201s outer wall, 200s the second insulating section and the third and final inner wall box out of two sides front and back of 202s. A non flammable glue adhesive or solvent for the insulation section would be applied to the center section and the larger 201 box would have it's inner surface chemically etched or conditioned to receive the pliable adhesive. And the outer surface of box 202 on the smallest box would have its surface prepared in the same way to receive the adhesive (if the surfaces are metal products). The protected cable access hole will be positioned to allow the trapped air to escape upon assembly of all three box sections. This leaves only one side to be installed with mating beveled edges which are both glued and sealed e.g. welded. This last side or plate will contain the access panel with locking mechanism and hardware (physically and or electrically controlled in most cases with special seals). And special consideration is given to any antenna and locking mechanism that is part of this protected containment with hard wiring routed with in the structure (these considerations are application specific with a lot of details in earlier filings) Three such earlier drawings with scaled back walls sre

CONFIDENTIAL

detailed in figures 2A, 2b, 2c,2d, and 2e. Figures 2 f and 2 g detail a special security seal around an access door.

201 points directly to the outer wall and this wall will be made of hardened metal products (described within) that resists physical penetration as a primary consideration. It also could be coated and or covered on either side, and or even be replaced by a penetration resistant plastic like Kevlar or other projectile and sharps resistant plastics Teflon, nylon ,and, vinyl ect (especially when the PFN is employed in exposed electrical service application with high current. This evolution of the outer wall is in keeping with all the earlier designs and claims to provide PFNs to all equipment and environments as continually claimed in all the related patents. However, this exterior wall in some applications will be constructed out of stainless steel and or coated with corrosion resistant coatings or made out of plastic and given special textures or wire webs, grids or grills. that can also help trap EMF\EMW waves and or radiation so as to block their penetration into the electronics housed within the PFN and or any peripherals, if so determined by an application to require this type of protection. Once again any and all of these technical variations can be employed, with the consideration of the tradeoffs . Which are almost certainly to be cost vs. desired and or necessary practical protection .

Through this entire description it is important to remember that any and all of these protective innovations may be employed, but final products will be constructed application specific and in the most cost effective manner for obvious commercial uses and reasons. An effort will always be made to create the greatest security for the lowest cost, however, the more secure, diverse and specifically sophisticated the unit and system is the greater the cost will be for any single PFN and or the peripheral system.

202 is the inner wall which can and will be constructed of various different materials as already named in the last outer wall description_ if so determined necessary by application specific criterion_for any specific PFN application. It may as well be constructed of hardened steel thermally tempered to increase carbon content in the molecular bonds or a metal alloy composite product may be utilized with , titanium, tungsten depleted uranium ect.(this is the same for all hardened metal applications for

CONFIDENTIAL

the outer wall as well). The inner wall could also be completely constructed of solid lead to create a final protective inner seal against radiation . Or a composite plastic already listed for the 200 and 201 parts with a EMF\EMW wave and radiation screen as already described for 200 and or 201 parts. Once again these could all be used in a laminate of layers or any one could be singled out for application specific priority to control cost. There are also recommended protective handling specifications put out by the federal government and industry for the best modalities to deal with and handle hazardous materials e.g radioactive, chemical, bio and medical waste, EMFs ,high electrical currents ,ect. All the materials used and the manner in which they are used will be developed for the PFN prototype construction with full consideration and compliance with these recommendations and regulations to insure that this technology will be inline with any standard set for any application.

203 shows the thickness of the entire wall, which is once again application specific and will vary as a general rule , but also as a general rule the different PFNS will be designed to be as universal as possible in shape, size and structural composition. The individual walls 201 and 202 may vary in thickness as well as the necessary thickness of insulation . All of these considerations will be application specific. For example in the automobile industry and normal civilian use the protective structuring can be scaled back to a standard that does not require the kind of protections detailed for high security to meet an acceptable standard. This will be true for all applications. They will individually have to be structured to meet the requirements of the application.

204 points out that the PFN will also be structured to be actually part of the host equipment physical structure in some security scenarios and in this case the system would have to be secluded and require limited and or controlled access if it were to have the appropriate military value. It would be structured to assert final control over a piece of equipment but it's influence would be undetectable and or camouflaged to a large extent and above all extremely difficult to access or terminate. (these systems are reserved for special disclosure and development)

CONFIDENTIAL

However, in many cases the PFN will be used to house and protect the host programmable controller (HPC) in the drawings 4-5-6 next to the mini computer contained in the PFN . These functions will ultimately in many cases be integrated with the obvious advantage being consolidation of the vital functional controls of the equipment integrated with partial or the whole data storage, remote control technology with the necessary security components all in one secure spot in a plug and play modular or card form and operated by TRAC software. Which can be physically displaced for an immediate disablement and total secured piece of equipment if so desired. But only by authorized and authenticated entry if this is a feature or capability so desired .And Of course any portion of these electrical components can be given this same plug and play capability if so desired. Because this Protected PFN\TRAC system & structure which is a protected physical electrical interface center of such wide base use and application ranging from high security, hazardous environments and military applications to standard civilian use a third standards effort will also be necessary involving agencies like NEMA, DOT, DOD, Highway Safety, and professional organizations like CEMA, ITS, and manufactures to decide on the application specific PFN containment wall structures that will be manufactured and or added to any and all equipment to provide legal physically protected areas to monitor, authenticate, record and perform remote control for each of the varied applications. All the base components ,elements and their properties and qualities are addressed in this application and the related applications. And as is true with all the components in the PFNs the PFNs them selves can be also exchanged to meet either more or less demanding environmental and application demands; e.g., The government purchases a standard automobile that is going to be used in a high security installation or hostile environment like an Embassy. In this case the PFN structure will be explosion proof containment and un-penetrable by projectiles and EMFs ect.

FIGURE 2A

(This is FIGURE 9 FROM PROVISIONAL 5)

00670784700

It is a figure from the original patent and it illustrates a one way pager PFNTRAC containment with it's protective encasement. Because there is a need for many cost effective receiving devices for the MMN. This one way pager system was created to perform the proprietary vehicle shutdown PASS as a cost effective modality to be added on to cars to aid law enforcement end high speed chases. However this system can be used to remotely control in an accountable manner a piece of equipment when connected up to the appropriate activity controls that either interface electrically or perform push \ pull and or rotational operations to control virtually every piece of equipment through automated and remote control.

2A01 is a manual lock for the PFN and these can be at any quality desired. It also has an electrical connection to be use in arming the device. 2A02 is the memory storage in this case audio recordings and a flash memory of operational data (Sony's memory stick 8meg a bites a piece). 2A03 is using a stamp processor as the controller . 2A05 is employing OCR systems however Motorola has many COTS products that can hook up with direct connections and all are covered in the related patents. In fact this entire system has been well detailed in all the related patents. Originally this drawing appeared in the PCTUS97121516, and in that PCT application the wall structure was described as one solid plate of Abrasion Resistant steel. This was being used only for the purpose of restricting unauthorized access to the protective interface compartment for the unique purpose to slow stop and secure a vehicle in real time. However in this application the space between the lines of the wall structure I am redefining to represent any necessary variation of the double wall structure as detailed in figure 2. Also the manual locking system could have the special thermal plastic seal in applications requiring this type of security measure for societies institutions to authenticate it's functions and records. And finally this PFN containment for the COTS Pager could be constructed for any COTS RF

CONFIDENTIAL

equipment receiver and or transceiver and or wireless phones e.g. cellular, analog, digital, cordless ect and or constructed to protect any interfaced integrated system that comprises communications/modems/ locating equipment/processors/memory/critical connections/emergency or supplemental power source.

Figure 2b

Displays two variations on the billing box accrediting system and the credit card devices and phone devices that have been innovated for these purposes. Primarily the billing box was designed to be an add on unit or after market device to collect a fee for use of a vehicle, e.g. rental cars, taxi cabs, buses, ect. Part 2B01 is either a standard credit card, ID card or any other information card that one wishes to use to enter information to the billing box (PFN). However with the price of the smart cards being greatly reduced; this device is not just designed for the regular magnetic strip cards as has been described earlier, but is designed to stay current with the more sophisticated cards, as well as evolve with other recognition systems e.g. finger print and voice and pupil identification systems. Of course the data retrieved from these magnetic cards can be recorded on board in the billing PFN as well as transmitted back to any network gate way computer communication terminal that can make the necessary land line connection to any credit check procedure and mass banking management storage for accounting purposes and records. And when this is done through a Billing box or PFN and TRAC system it is a commercial service product of the invention. TRAC can run the Bank card/Stock Exchange Transaction products and algorithms via the commercial 128/64 bit Encryption or web transaction products . And or utilize the COTS banking products and protocols like NCR systems for ATMs. These transactions will be provided memory storage for personal accounting and verification to the financial institutions as proof of payment. PFN's will be every where and all those with ID systems PIN number and key pads, finger prints and other forms of personal identifications will allow for any personal

CONFIDENTIAL

payment, authentication, and or verification of transaction virtually anywhere.

Part 2B02 is a cell phone handset configured with a forced card reader slot and sensing head to accept the card in the track or slot and extract the stored card data on the magnetic strip to produce an electrical signal that provides encrypted encoded data to a converter circuit that has a processor chip with a firmware algorithm that can compare and prepare the data into discernible language equivalents. Or after the card reader prepares a signal one of the PFN mini computers will process the signal and or encrypted and encoded data through software programs running in the TRAC software e.g. CEW Commercial Economic Web transaction products either proprietary , Governmental, and or Commercial Off the Shelf products either past and or present or any newly developed algorithm with higher security. With the use of the cell phone handset configured with the card reader and slot the lower bill box could be configured with out a key pad. It would be possible to use the phone hand set key pad to give pin code and or input data to the PFN box for the most rudimentary communications. Part 2B03 is a standard key pad that can be used to communicate with the bill box when connected and interfaced with any the invention's computer and supported with the proper interfaces and software and or firm ware. Part 2B04 is a multi-bus bar connector universal with 29 contacts so that it can support any system/device entered into the bill box. These were earlier designs. And this earlier design will probably not be used and will be replace by the multi bus system IEEE1394 or the universal bus and or any IrDA interface. Or completely replaced by the universal plug and play uni- bus as described with it's essential properties and qualities in this application and all earlier related patent applications no matter what transmission medium is utilized to complete the tasks. So these earlier mentioned COTS connectable systems converters and or interface circuitry will always be relevant; because the base PFN/TRAC system or the invention is designed to provide forward, backward and present engineering to be a complete universal plug and play physically protected accountable interface that provides accountability to real time remote and automated control and management functions, for all vehicles, equipment and machinery.

In the past and present Part 2B05 represents a quick connect end on one portion that will make a pigtail to connect with any combination of electrical connectors on the other end of this second portion, e.g., computers, any electronic connections, radio or automobile. But in this case it is depicted in the drawing as e.g. RS232 part number

SECRET 01900

2B06. The other short pigtail is part number 2B05, of which there may be 5 to 10 in quantity or more, that can easily slide back and forth to allow many varied positions for the different devices and the space they require.

As mentioned earlier hardwire connections could be made with Commercial Off the Shelf devices in the box or by infrared com-port connections and or a new and unique total plug and play uni-bus interface, that will be detailed in this patent application as to quality and properties and elaborated on as to the most favorable modality but will ultimately be designated and prescribed physically by a standardization effort involving government, commercial interests and public and private organizations. However this universal interface capability has always been part of this invention from the first patent application in 1996. The invention has always called for a Protected electrical interface of controls, communications, processors, with accountable records to provide an organizational platform for all electronics on a host piece of equipment . Basically, the PFN\TRAC system is this control center interface with total accountability for any and all electronics on a host piece of equipment, whether it would be a vehicle, a piece of stationary equipment or any machinery, and or an environmental sensing system, which would and or could provide the appropriate data to any and all in the appropriate manner to develop public trust, while simultaneously protecting individual anonymity and or privacy in an accountable responsible manner with and through the qualified appropriate authorities in such a manner , that the legitimate legal tort system could illustrate and use this properly gathered accountable evidence of any and all real-time activities to either properly defend or prosecute on an incident and or individual as fairly and respectfully as possible and needed.

Another uni-bus system described earlier is the segmented infrared bar that can be aligned to any device's infrared window to communicate with the invention's control circuits. Also there are varied but designated power connections to supply power to any device by priority. Once again most all devices presently will be configured to IEEE1394 USB connections and have their drivers and software supplied by the manufactures to quickly install almost any desired system as easy as buying a product peripheral for a personal computer. This is one of the main reasons for the timely presentation of the invention

After the devices are installed and connected, foam pad shims are placed between the different devices to quickly secure them in a protected stationary position. The dotted

lines show adjustable bin space for the user to plan their own devices. Part 2B07 is a mouse ball that one can use to run window type graphic programs either displayed in the unit display 2B08 and/or any larger display within the field of view for the driver, either LCD vacuum tubes e.g. VGA flat screen, or the new hologram wind screen in the newer cars (e.g., Pontiac Grand Prix). Part 2B08 is the unit display, part 2B09 is an emergency power pack, and part 2B10 is the secure bill box.

The structure of the box has been described in the best mode of carrying out the invention in 112756-202 related patent and all related patent applications. As to any specific wall structure and insulated characteristics and modalities will be modified and or configured in many different shapes and sizes as are deemed necessary and appropriate , and are already exemplified and detailed through the extreme variations in all the related patent applications. However, as stated earlier the third standardization effort called for and detailed is for the physical protected structures of these PFN/TRAC electrical connecting interface /system. Meaning all boxes, coverings, enclosures. protected couplings, specialized signal converting circuits that are clearly developments of the invention , which are all utilized in the secure PFN electrical organizational platform .

This particular device (the invention) has been designed specifically to be an accountable interface for electrical communications to perform robotics, and or aggressive remote control; and to provide accurate and responsible data both in anonymous and accountable formats for the public in real time through Internet links and web pages as part of a massive Machine Messaging Network (MMN) which through the PFN phone ,RF and paging Gateway nodes connect with the (WWW) either through private networks or commercial networks , public or private web page gateways (big or small) to web as Internet providers and commercial servers.

This figure was originally drawn for the Cab industry and is designed to be an add on device for older equipment. Any of the PFNs can be configured to handle CEW Commercial Encryption on the Web , which in many cases will be provided by the bank card companies and the payment industry as their COTS payment industry products to conduct business through the PFN\ TRAC software hardware as a CEW application.

PATENT # 6,111,900

These transactions are accomplished through the detailed com links, which are created to handle these financial high security data applications and deliberately provide the necessary protected secure accountable electrical platform that is both physically and legally protected and mandated on all pieces of equipment as part of any standard, legal statute, rule and or legislation .

TRAC is designed to handle 128 /68 bit. This is sufficient for present requirements but the invention is designed to stay current and incorporate any newer technology that can handle greater data and process it and maintain it in an accountable manner incorporating the necessary security standards and all standards as the aim and goal of the invention to maintain a secure and protected primary focal node. As part of the nature and scope of this invention, this invention will incorporate any and all such technical improvements and advancements that better provide data acquisition for man and machine as well as improve controls and management of PFN equipment and machinery, for real time control , accountability and or management, of the machinery, and environmental sensing, including effected infrastructures, the economy, normal commercial transactions of society, and maintain the best accountable protection and respect of the individual as part of PFN primary function.

FIGURE 2C

(FIGURE 10--EXAMPLE--CAR DASH SECTION FOR A NORMAL AUTO (112756-202)

Shows a picture of a dash board in a traditional sedan. Just right of the steering wheel is the PFN and it is depicted as a box with a personal computer slid all the way out of the containment with the lid or screen display opened so that the driver could use the computer screen with a GPS system like DeLorme running to receive automated directions to an address she/he was unfamiliar with. Below the computer and the secure lock up center section rests a cellular photte that has its phone modem connector coupled to the heal of the phone and directly to the right is a second communication device a pager that is also coupled to an optical scanner in this case as was described in the first

SECRET

patent. The lock up 2C004 in the center can house permanent invention computers and storage records plus GPS and any communication devices that are desired on the vehicle all the time, This lock up section is only accessible by authorized personnel in the most ideal situation and hopefully mandated by law. This section would house the PFN invention computers and in the place of an on board personal computer their would be an LCD screen that could display map graphics if need be, through the on board computer systems. This is only one basic configuration for a PFN and the system could be re arranged in any number of ways.

Now for a more specific parts description of the individual parts numbered. The square boarder with circles inside is the walls of the PFN case. 2C001 is the outer metal case plate which can be up to 3/16" thick made out of AR metal plate to resist penetration or drilling. 2C002 is the inner metal plate up to a 1/8" thick and it is made of the same AR plate. 2C003 is an insulating product and their is two that are being used to construct the prototypes. One is "solid smoke" a product developed for the space shuttle and "Geo-bond" a gypsum product. None of these products or specifications should be considered the only way to create a secure PFN containment to fulfill any part of the nature and scope of this invention. The thickness of 2C003 the insulating section would not exceed 3/8". 2C004 represents one kind of lock cylinder like those used in safety deposit boxes, however, not made of a soft metal like brass. From 2C004 can be seen two flat bars that go out past the inner plate 2C002 where they pass through a solenoid catch mechanism that when it is de-energized will not allow the bars to pass out of the front edge of the encasement. 2C004 in the center can also be opened manually with a key. once again their are many manual and or electrically automated locking devices that could be utilized for this same purpose. In fact in a later drawing in this application figures 2f and 2g depict a proprietary locking seal system that uses a thermal plastic seal and seal stamps to better assure that the protected areas of the PFN containing either vital components or sensitive data have not been tampered with.

In figure 2C, 2C004 is displaying the bottom compartments access panel swung open on a piano hinge part number 2C006. So the view is displaying the back of the panel so bars can be seen and that is why they are depicted as solid lines. Behind 2C004 lies the secured section which is represented with dotted circles because they are located in back of the bottom access panel in the open position. If the center section is the designated section to handle or store the legal storage electrical components it will not have an

CONFIDENTIAL

electric lock release or it will be disconnected to only allow for the proper authorities to remove this data or component parts. 2C005 is the bottom access door in the closed position and that is why the bars are depicted in dotted lines. Once again 2C006 is a piano hinge and is a part on each of the three sections as a point of articulation for the panel door. 2C007 is the standard glove box that can either be used or discontinued to allow for other rerouted accessories HVAC vent, ducting and plenums or blowers motors, etc. 2C008 is the SIR compartment which is the sudden impact restraint or the Air bag. With on board distance sensing for front and rear as well as even side surveillance of the environment any impending impact would be sensed and automatically withdraw any opened draws in use into the containment which would allow the aesthetic skin panel/drink holding table to spring return to a closed position. If the drinks were in the table with the table in the down position all 3 access panel doors would be closed and secured. this would be accomplished by electric servo motors or vacuum motors or cylinders or diaphragm systems for speed. Also the electric cylinders could be used, e.g., "Memory metal cylinders". At no time would the center section or a part of the center section be open to the cabin during operation as this is the protected black box storage area. Of course these configurations are flexible and the designs can vary greatly, but when a permanent area is chosen it has to remain inaccessible till the proper authorized personnel supervise any reconfiguration, e.g., certified service personnel that have to enter their service identity credentials. Otherwise a customer's insurance company must do the same or support clerical personnel for the police or department of motor vehicles.

2C010 is the pager as earlier described with an OCR scanner on the front however any interface and connector system could be employed in the PFN. Also Motorola pager processor "Create a link" could be utilized here and even as an effective processor in the center section that is closed for the ultimate secure service functions as another C.O.T.S. computer communication combination for the inventions control center. 2C011 is the standard cell phone with a connector modem, which will be wired through the trays to any of the on board computers to receive and transmit data to any system in the PFN or connected to it. 2C012 is a specialized tray connector made by or for the personal laptop computer that will provide all or any of the desired physical connections to interface the computer to the host vehicle or any other peripherals or to network it with any other

CONFIDENTIAL

primary computers. The holding and securing tray will then couple to the sliding either motorized or powered by vacuum. And so the electrical connections to be functional here it will have a controlled flex cable to 2D103 the central buss channel or channeled or race way where it will route wiring up and down inside the containment.

Once again these connectors are past and present COTS devices and in figures 6a, 17, and 19 of this application the universal plug and play buss of the future is detailed as to what necessary properties and qualities will be needed to develop a standard. Also, many functional modality options to accomplish this uni-buss standard for the automotive industry and basically for all applications are detailed in these same figures and in all the related patents to create this accountable protected and secure interface for any and all electronics on any one piece of equipment through this PFN structure physically and electronically interfaced through TRAC.

FIGURE 2D

Figure 2D shows two more structural detailed views of the secure box or PFN in the Dash. The top view is of the back of the box cut off so the components can be viewed. The top shelf is showing a laptop with all its varied connections that have a performed shelf designed to supply the necessary connections directly to the laptop connectors. There also is a tube or channel part 2D103 running from top to bottom in the back of the case in which all the shelf connecting leads are channeled together and all the appropriate connections have been secured to the devices in their shelved trays. This same tube works as an antenna galley and channel to house the control buss of wires to the out side of the secured and protected PFN . These wires are protected in a armored flex cable like the one described in the first patent for the protected beeper.

When 2D103 doubles also as a antenna galley in the back of the PFN and for the full height of the containment the outer metal plate part 401 is replaced with a strip of Amoco's poly-sulfone thermal plastic 1/2" thick 1 and 1/2" wide strip which runs the height of the box some 9 to 10 inches long. This thermal window is provided in the back of the PFN to make it very difficult for anyone to tamper with these vital circuits and to also allow for a signal to be received when the C.O.T.S. products patch antennas are not sufficient and they have provided for an external antenna hook up. And as also mentioned

SECRET 01100

earlier there is another option to provide for reception in the protected containment to receive any necessary signals through using the same poly-sulfone product and creating port holes for the necessary signals to enter into the protected containment to reach the standard C.O.T.S. antennas e.g. patch type , but also provide protection from heat and fire . And of course these port holes would be located in hard to reach areas.

The bottom box illustrated in figure 2D is showing the lock access panel doors with a piano hinge 2C06 for this sturdy structure .This 1/8" thick access door is made out of stainless steel and numbered 2D10 in figure 2D. As mentioned earlier along with adding an additional way, the access doors 2D10 can be opened in three different ways, one with a key in two places as displayed in figure 2D, another as described in figure 2C with the throw bars out to the electric solenoid catch mechanisms and there by finally opened by electric solenoid release triggered from the inside program software of the inventions on board controllers which is reliably energized by the emergency batteries inside the PFN; including the electrically controlled and activated proprietary seal detailed in figure 2F and 2 G of this patent application. The two key systems would also have the same solenoid lock release system electrically. These access doors automated locks and tamperproof seals are finally covered by an upholstered and padded dash plate / drink holding table numbered 2D07 which is illustrated in the down and open position and appears as the end view of this dash plate / drink table . The front is molded and formed to create a uniform appearance to the dash board and through a ribbon connector can provide connect-ability to any and all necessary switches for manual electronic controls as a compliment to verbal commands to control audio sound levels atmospheric temperature augmentation lighting and or driver assist systems to greater enhance safety ,luxury and security. This aesthetic dash front may be constructed by covering the compartment panels with cushioning and traditional interior upholstery coverings like foam and vinyl and not having the drink top dash panel.

However, 2D01 represents a molded rubber gasket that is grooved to accept the dash control plate(w/ ribbon connector)and or /drink table in the closed position. 2D02 is the two sided lock placement cylinders if this type of lock system is employed. And 2D11 depicts the electric latch plate and solenoid assembly that receives the lock bolts from the keyed cylinders. 2D05 is another piano swing hinge for the table / dash cover plate. 2D04 is a coiled spring that returns the dash plate when all the drawers and or trays are retracted. 2D06 is a shelf roller that can be slid into any number of slots in

many places of 2C01 the inner wall of the box . These slots will either accept a tee ended fastener that supports these shelf casters or rollers or it will allow a compartment plate or separating partition wall to be slid down the slot. These compartment shelves or rollers can be moved or exchanged to create any number of configurations, however, the trays will be standardized to certain sizes that will be customized by the manufactures to accommodate their products.

These separating plates have lock blocks that have drillings with 10/32" screws that will thread into tapped receiving holes in 2C01 the inner wall. 2D08 in one of these partitions. 2D06 the rollers have a screw that can be tightened to clamp the tee device against the inner wall skin- part 2C01. 2C12 is the personal lap top in the top shelf.. 2D09 are more trays that ride on the rollers. These trays presently are designed to either be half the size of the PFN or to go all the way across the containment. This is not the only design for the movable trays and adjustable flat compartments and should not be considered so, but this design is being proto-typed presently. Any protected containment or interface that is structured to coordinate and control remote functions on a machine all fall within the nature and scope of the invention.

FIGURE 2E

Is only one suggested example of many possible commercial tray component layouts and integration's for the PFN/TRAC/FACT/CEW /MMN/WWW and in no way should it limit the claims of this inventions PFN to any secure protected accountable electrical interface structure on vehicles machines and or equipment

Figure 2E tray modality is a plug and play component design, which claims a total physical and electrical protected interface for all electrical components as well as accountability and integrity checks to insure inventory of the systems components. This inventory integrity check is accomplished through a role call dialog with each components FACT chip and the PFN computer. The running TRAC/FACT program on start up will seek out all components at last shut down and handshake with the components FACT chip to compare ESN and other vital data with last operational record stored. Any new devices or components will have a hand shake and or identity

CONFIDENTIAL

check and the PFN computer will request the operator through any available display or audio verbal commands to install any installation software disks in the appropriate drives to create the appropriate drivers. At this same time the operator may be requested to provide registration numbers or pin numbers to activate a legitimate device. The PFN will at this time call the National Registry to check the component out. This registry will have manufacture information crime data and national security alerts and public safety warnings at the very least. This Federal Access and Control Technology FACT part of TRAC PFN software will be detail much greater in figures 16,17,18,19,20 and 21. Presently this figure is devoted to the physical lay out of components and COTS devices

This figure depicts 3 possible drawers configurations for a possible application of the secure box and or the PFN systems. The top draw houses the laptop computer 2C012, the bottom draw houses the power pack batteries 2E01 and 2E02, the transformer 2E13 and the inverter 2E03 along with power supplies that are varied power taps 2E17 for the C.O.T.S. products housed in the PFN. And the center drawer houses all the essentials to complete the necessary function for the PFN. It has a GPS 2E16, A Cell Phone 2E05 a Pager 2E09 and a small PFN computer or controller 2E11 and a data storage MO or re-writable CD's disk drive or hard drives or memory sticks 2E12. With the drawers and compartments 12.5 x 12.5 x3" all components easily fit into the three drawers.

The top drawer 2C012 is showing the multiple fittings that would be molded into the tray and not visible as a end view but instead shown here as a top view. In most cases the manufacture would not have to outfit a tray and probably would not do so for all the possible connections for the laptop. However they are shown here and mentioned as all being possible. Reading from left to right the first connection would be for 14.vdc as a power input for the computer and is supplied by the bottom shelf tray from part 2E14. On the top shelf again the next round circle to the right of the DC power connector icon the PS2 mouse or keyboard connection for an external mouse or GPS 2E16 connection in some cases. The next comport is a 9 pin serial port and the following one is a 9 hole additional monitor port. Then the little square is the infrared communication port, and the very next one is a parallel printer port 25 hole LPT1 port

SECURITY INFORMATION

and the last one on the left is the a USB communication port and most likely the one that will be used with any peripheral hook ups in the box , however any of these connections might be used for any number of interface connections and it is possible that a laptop manufacture or secondary provider for the trays may outfit any and or all the communication ports with a service connector in the tray. Ideally the placement into the tray or cartridge that is affixed to the rollers and rolls it self or is placed on a shelf and does so . In any case the tray or cartridge for any peripheral will instantly plug up to the laptop or other device when placed and secured in it. This would replace any need for thumb screws to complete any required secured connecting unions. And would accomplish a plug and play modality for rapid deployment into a PFN's electronic array of accessories as a compliment to the full complement of the inventions electronic devices and innovations housed in the PFN and supported by it's electrical interface. These have been detailed earlier and their exact configuration will depend on how much the OEM of the host machine will provide in their PCM controller options and or accessory's control options. But as was illustrated earlier the components to provide all the stated services are available through the inventions technology if need be. Of course this is going to be greatly enhanced with all three standard efforts detailed in this patent application and all the related applications since 1996 for all the automotive manufactures and other industry specific manufacturers of host equipment and all related government agencies e.g. FCC, DOT DOD & FBI and professional organizations e.g. CEMA, ITS ect. However, even with this present diverse state with all the proprietary couplings and connectors today this PFN / TRAC system has addressed most all the possibilities to create an accountable automate and remote control and management system for any host piece of equipment with present Commercial Off the Shelf Products (COTS) and to keep the PFN current with all the technologies merging to provide accountable aggressive remote and automated control and management systems.

The middle shelf or power tray as designed for this prototype will have two batteries one a 12vdc part number 2E02 and a 6vdc part no. 2E01 and these two batteries are wired in series to create 18 volts, which are wired into the primary windings of the transformer 2E13 that provides multiple current level taps or solid state regulated chip circuits to energize all the varied C.O.T.S. products in the PFN. These prototype voltages are 1.5 vdc, 3.vdc, 6 vdc, 7.5 vdc, 9vdc, 12 vdc, 14.5 vdc. 18-19.5 vdc and also

COTS INFORMATION

because in many cases people will enjoy being able to plug their computers right in 2E14 is provided as a transformer and rectifier or converter and tied directly to the primary coil of the transformer 2E13, 2E03 receives it's power from a 120 vac circuit that is created from the host vehicles 12vdc supply of 6 amps and the PFN battery pack energizing an inverter of 250 watts 2E03, which also supplies 120vac to a plug prt.#2E14 in the front stainless steel access plate for other devices that people might need 120 volts AC. e.g. small heating blanket, coffee pot and/or hair dryer

In the second draw 2E07, 2E08, 2E14 are OCR optical character recognition scanning devices and they are wired to a micro processor so that the unique digital signal from a scanned alpha-numeric image on any and all of the devices that have LCD displays, e.g., GPS, cellular phone, pager and respond to any appropriately addressed message with the proper preprogrammed response as described in the first application.

CONFIDENTIAL

This scanning interface is only one example most all the of these COTS devices have their own interfaces to allow them to communicate with any onboard computer they are connected to, e.g., serial or TTL, etc. And any of the IC components would be all part of a circuit if it was in the secure lock up as a mandated circuit function by law. 1206 is a connector for a cellular phone. and on the back of the tray are a number of different sockets for data transfer cables to the 503 wire race or cable channel that goes from top to bottom in the containment.

In the back of the middle drawer part number 2E15 indicate a lock partition wall in this prototype and behind this wall is where the PFN controller/computer 2E11 is along with its' data storage system 2E12.

Note: if it is necessary to use two drawers to provide all the elements of a Protected Primary Focal Node such as is the case in this illustration both compartments will be sealed and securely locked to prevent any tampering or damage. In this case the 3rd draw and middle power tray would be secured in this fashion.

FIGURE 2F

Along with many other secure sealing mechanisms this technology provides an additional security feature for the PFN secure on board memory as well as, any other necessary electronic parts e.g. communication equipment processors, memory locating equipment and emergency power to complete all PFN operations. This is a electronic certification seal system: Figure 2F is utilizing one thousand series numbers in all related patents because it uses the trickster circuits relay systems to activate the heater wire to release the seal to physically enter the safe box memory containment section of any PFN TRAC system certified for record keeping of any kind for accountability.

The trickster circuits are a unique proprietary micro relay signal system that generate a specific signal via a micro processor and com link to inexpensively create an artificial signal that triggers a specifically desired response from a preexisting control system and

it's standard circuitry.

2F10 25 is the security relay switch and can be a silicon relay with a gate lead 2F1033 or a standard mechanical relay where 2F1033 would be one of the leads to a primary coil the other terminal would be connected to the opposite pole in this circuit. 2F1026 is a wire or thin piece of conductible metal covered in a substance that will melt when heated to 300 degrees F or something less (application specific) the prototypes will use a product call poly-sulphone which is a heat resistant plastic. The inside of a PFN should never reach this temperature as it is insulated .2F1027 is the plastic well anchors for the seal with galleys to accept the liquid plastic during an authorized installation of clean memory and the removal of a un-tampered memory component. They are positioned structurally around the access door and are stamped with an registered ID number for legitimate access to this compartment. 2F1034 is the negative terminal and can be provided a contact terminal or wire to ground in the automotive applications. 2F1035 is the positive lead and it too can be provided a terminal or wired to a fused positive lead with the appropriate hard wiring and fuse amperage. 1030 is the negative power lead and 2F1029 is the positive power lead. 2F1031 is the processor and can send the appropriate signal to the gate circuit out fitted with a 2F1003 trickster circuit that is resisted to a set signal, or the processor can energize the other side of a mechanical relay 1025 and there by turn on the current and melt the plastic seal. Or 2F1032 can be used to send the correct electrical signal to switch the security relay 2F1025 and it's resisted trickster circuit also energizing the seal system separate of the processor in the event the processor has been compromised.

Fig. 2-G

Is a physical view of the PFN secure area for memory storage. This drawing does not depict any specific guarded area . it is used to show the physical locking of the access door and the seal going around through the anchor seal wells 2F1028 SA. 2G1036 is the

physical lock throws through the side of the PFN. These can be operated physically and or electrically if so desired. 2G1037 is the key slot cylinder and this cylinder can be constructed like the new ignition cylinders and outfitted to read a resister chip in the key to activate the SR or switch part 2G1025 in figure 2G and melt the seal the seal 2F1026 that goes around the entire access door and passes through the SA anchor seals. SG1038 is the secure box itself.

So there will not be any miss understanding the PFN box can provide interfacing protection and security to a lot of electrical components and personal property items , however the memory storage and any circuits responsible for TRAC routing or PFN/TRAC completed operations will be provided the highest level of security and protection . These components or linked devices will be electrically secured and physically secured in the certified or sanctioned area with locks and seal to protect the memory at a level that can be used as legal evidence and to insure a tamper proof environment as much as possible to maintain credibility for the data stored in memory

FIGURE 3

Shows the two basic PFN communication modalities, which are being developed as prototypes. There will be one way transmission devices (basically pagers and RF receivers, including an accessibility to any responsive broad band scan function for the standard AM and FM car radio receiver as well. With a radios standard seek and scan function initiated by the TRAC PFN software (FACT for example, through this connectable interface) allows law enforcement to give remote commands through the PFN TRAC processor to perform this technology's PASSS and PAGSSS shut downs and securing of a suspect vehicle. This can likewise be performed by the pager system or any long or short range RF receiver or transceiver on board that will be applicable to the circumstance. With all receiving equipment interfaced through the PFN and controlled by it's computers the PFN computers can query any receiving unit for specific addressed

FACT commands given to it's PFN ESN or the host equipment's ESN to all legitimate law enforcement and the proper authorities many communicative avenues for long and short range simultaneous control of a suspect car or out of control vehicle or piece of equipment

Basically however in figure three there will be two levels for the two way transceiver devices . One in the US employing the two way pager systems developed by Motorola. (the reflex products and protocols) and the other more sophisticated using wired telephony technology and or wireless RF equipment and or Cell phone technologies. The varied peripheral capabilities and containment or extended physical protections will be application specific and determined by the modalities used to interface the necessary components to provide an accountable PFN system to comply with any standards effort and current technical development.

PFN structure shape and size will be governed to some extent by the hardware employed. Some exterior containment might be the same for one and two way pagers and the same for many of the solid and or integrated circuit evolution's and combinations. The containment will house the standardized TRACFACT Software in a processor and or any and all accompanying IC chip sets for pager cellular phone, RF circuits, and GPS. And or interface any current C.O.T.S. communication products or devices through the modalities detailed throughout all this technology's related patent applications. This versatility will be replaced with universal interfaces, components and structures as a progressive accountable focal node for all automated and remote control functions as are created for these specific applications and in the areas on mobile management, home management, commercial management, and control security technology.

The drawing also illustrates monitoring, remote control and or management systems from the local level to the global level. This figure is utilized in other related applications 202 and 300. The 300 network displayed at the top of the figure three is the basis and structure for 1100 and 1200 series monitoring and control systems. This

networking can support this technology's "green eyes" and "spider eyes programs" at varying levels of public involvement and acceptance with varying levels of security, either as part of the Internet or in part as isolated networks interfaced and protected behind fire walls from general view on the Web if so desired. The data and its use will be determined by the public, it's governing bodies, processes and agencies to set the appropriate rules, regulations, laws, specifications, codes and standards, for any Internet and or world wide web engagement and the equipment use. However, this machine messaging network MMN interfaced with the web WWW and utilizing the detailed communication systems of phone nodes, modems RF equipment interfaced with gateway computers can provide all the secure connectability for servers and providers to commercially full fill all the above detailed primary and sub programs desired to be run in a PFN TRAC\FACT\CEW software programs in a module form or in any manner prescribed by any and all governing laws, rules and regulations to insure accountable remote and automated control and or management. In the top local section 108 or 1208 in the 300 patent application is one remote storage but a plurality of memory storage is possible and probable in many applications throughout any of the networking.

The figure also shows all the qualities and peripherals, as well as, the security systems for conditioning any two way transmissions. There is many encrypted C.O.T.S. products to condition a data signal, and this technology will attempt to accommodate any and all hardware embedded software, and software encryption programs as possible to provide greater commercial and security options for any signal from a PFN. The many products will be named in an appendix to this application and this technology will do everything possible to cooperatively develop joint ventures in an effort to expand this technology and others to increase world stability through good management of the socioeconomic environmental interaction between man and machine. Humanity will still be the governing control over the PFN \TRAC\FACT\CEW systems through it's evolving nation states however, it will be provided more accurate and real time data in an

organized fashion to aid in the appropriate real-time decision making process in the future development of humanity in a more harmonious mode with itself and this earth.

Directly below the monitoring and control net work are two dotted lines representing wireless transmissions. The two directional dotted line on the right represents two way transmissions and has the letters DES on the left side which is an abbreviation for Data Encryption Standard and PGP on the right which is an abbreviation for Pretty Good Protection.

DES is a protected government technology that has specific hardware, for high security data. The software or embedded firmware for the government is handled strictly and provided through the government for their high security applications. This invention would of course be capable of employing this DES security system protocol on all of it's one or two way transmissions between devices e.g. PFN's TRAC\FACT\CEW system computers terminals and or gateways, their wireless and or any land line communications to PFNs as deemed necessary or standardized. Or to other networked terminals and or any data storage systems that were approved for this type of security system by the government or it's authorized agencies, the Justice department FBI or any national security agencies the Secret Service ,CIA and DOD ect. This is being mentioned presently to make clear that the standard PFN and TRAC module will be capable of accepting any DES hardware or software as part of this technology's primary program FACT and as a plug and play but securely protected circuit. FACT is TRAC's Federal Authorized Control Technology. There are varying levels of DES security presently and FACT's capability by application and use would be determined by the United States governing bodies and agencies, as per the publics empowerment and acceptance for national security balanced with individual freedom and the respect for the individual citizen privacy in the deployment use and functions of any monitoring and or remote control of and through privately owned possessions, such as automobiles.

This technology has been designed to provide more organized control and accountability to humanities equipment, machinery and vehicles for the optimal management of the equipment to increase public safety, national security while improving the quality of life for the individual with the respect for their privacy. This requires accountability for the collection and use of PFN TRAC/FACT data and or any other parallel remote control and monitoring technologies. The use of these technologies have to have the best temper proof measures and the strictest criminal and civil penalties for any miss use or abuse of data; either when it is collected or dispersed in a reckless and or negligent manner. For these technology's to better humanities quest to better itself and it's total survival these technology's need to be structured and standardized in accordance with society's law and order and in the case of the United States tailored with respect for the individual's privacy Because the individual citizen is continually ask to compromise more personal privacy with any and all data acquisition to provide more improved and better services, which require more enhanced and freer access to personal data and knowledge. So there for the greatest controls have to be put into pace to maintain the respect for the individual citizen and their rights to privacy. All data acquisition systems most certainly be commercialized with a standard of operational practices that are clearly understood and agreed upon by all parties and that are true in practice to the United States constitutional guidelines and guarantees.

Once again this technology address these issues as it's nature and scope claim and as a necessary and correct approach in the development of standards to provide responsible and accountable aggressive remote control, monitoring and robotics. In this effort this technology seeks out all parties commercially, governmentally, socially, environmentally, and financially to address the issues and form joint ventures to achieve sound safe guidelines that marry up well with society' social-economic and environmental intrests. This should be the basis to commercially develop these technologies to evolve the economic tool to better value and reflect all aspects of

equipment use and to improve safeguards to all such transactions and impact on society in general.

As mentioned earlier there are many types of encryption protocols for security. PGP is the commercial versions of encrypted data. And as explained earlier there is a great number of such systems that can afford reasonably good protection for many security programs. Some of these are just software down loads and can be part of the software in a PFN TRAC\CEW system and capable of running an encryption program piggy backed through other servers signal conditioning software. As detailed earlier the primary programs software will delineate restricted data from unrestricted data if so desired and this capability exists for DES with hardware chip sets and embedded software or firmware, as well as, solely performed by software programs . With both DES and PGP both ends of the transmission must be equipped to electronically cipher and decipher through a encryption and de-encryption key program no mater which technology is used and in what form of hardware , hardware embedded software firmware, or solely software added to any existing hardware either in the processor or computer section of a PFN , it's modem circuitry, and or as part of any of it's communication devices circuits and or any remote monitoring control management and storage system responsive to any PFN TRAC unit.

** These security protocols for the highest security have to be maintained in every transmission including throughout the 300 network for wireless and land wired systems and this is why the phase "Same Security Protocols" (with arrows) parallels the horizontal 300 network labeled -----world ---local---and sectional. Sectional represents states, regions, or areas more geographically located or electronically designated.

The basic reason the encryption protocols are only shown on the two way transmission PFNs is, because, they could be broadcasting secure installation video and other sensitive telemetry data from a e.g. compound or installation. It may not be as necessary to protect one way directional remote control communications in all security

applications or in many of the management applications, because, there will be less of them transmitting data back and thus more difficult to figure out their purpose or instructional command codes. However, in the highest of security applications signal encryption may be required as well, for one way command level remote control , and therefore is shown as a possibility in drawing 4 number 403 .

301 is the two way communication device with the DES and the PGP systems on each side showing the options of encryption and the small arrow to the right of PGP points to the right block as a 2 stage memory on board the two way PFN, which are parts numbered 105-107 in figure one. Number 302 is a line list of possible accountable functions for full remote control and remote monitored robotics. At least one variation of this two way PFN will completely support all of these functions including any special sensors, e.g. GPS or locating equipment, identification systems environmental sensors, audio video systems, all machine controls and will monitor all machine sensors. 301 memory storage are shown here as a plurality of local memory. One a current running loop of application specific determined length and content. And the other local memory a application specific incident based or event storage. This second data storage is permanent and housed in a protected area with special authorization necessary to physically and or electronically to access the data. The proprietary design, also, provides either a redundant storage of this same incident or event data in at least one remote location or a limited message flag (for the data limited two way pager systems) to be sent to an appropriate authorized monitoring E-mail address, or computer network or RF receiving node. While these memories are detailed in a plurality for local and remote locations this is merely done to provide these options for any standards effort that can be applied to the application specific protocols and areas

303 points to the simple one way receiver PFN. The dotted line coming down from the top depicts the one way communication for one way remote control of equipment. However, 303 also can support the same two stage local memory storage.

With this one way system, there is no wireless remote storage, without the physical removal of the data or through local physical connections. There is no report back function in real time if the one way system is the only for of communication. The one way system can also support the same processor capacity to do all the same functions as the more sophisticated two way PFN, but is limited in remote control by not having a real time monitoring in a remote location to guide tasks by video. The 303 one way system must have it's data recovered physically through a secure download communication port. This interface communication port can, also, be in place on the two way PFNs if so desired. However, remote control functions can be preprogrammed and or guided and or confirmed through other two way PFNs on location that can video the one way PFN systems host and or report on other telemetry data about the one way PFN that warrants specific remote commands. So by teaming one and two way PFNs one can provide a complete remote control system for the one way PFN. Total accountability is still provided in two levels in the one way PFN (re writable and permanent) . Also an extendible and retractable connector either hydraulic, air or electrically activated and controlled can connect the one way PFN to any of the communication ports on same equipped two way PFN to report back any pertinent data that needs near real time consideration. In fact in a security setting only one two way PFN mobile device could recover data from all the inexpensive one way PFNs and report it back to the remote monitoring and remote control system. This mobile two way PFN could also accompany any one way PFN to give report back data for real time remote control of the one way PFN equipped machine whether it was stationary or mobile one way PFN.

304 Illustrates all the same functions that are listed for the two way PFN and states that it has only a physical retrieval accountability for any data stored. 305 is a block at the bottom of the page and its functions can be performed by both the one and two way PFNs. 305 is any special sensors section that will be gathering application specific data for these any applications e.g. environment, radiation counters that

transduce the number of Rads or particle strikes into an electronic signal for the processor software to evaluate through compare lists set up for an application specific PFN or as burned in firmware on simple device where a simple PFNs is set up as to sense an environment. If this PFN is at an installation or in a remote location it will be powered by solar cells to recharge it's batteries. 305 special sensors will be many different applications specific sensors that send an electrical signal to applications specific software programs in the PFNs . The TRAC system will be programmed special to handle specific functions for specialized sensing e.g. like hydraulic weight sensors . many of these peripheral devices and sensors exist as sets products and their are flexible software products that can be easily adapted to support these applications.

Another 305 special sensor is the nose. Which is a sensor that can identify odors 2000 times more accurately than the human nose and is capable of discriminating substances and matter at a molecular and even atomic level. This sensor already designed to deliver unique electronic signals for it's application specific software compare list library of known substances will serve well in high security applications to identify biological and chemical toxins explosives eg potassium nitrates ect, and leaks in regular chemical containers in any commercial or governmental installations airports. And when coupled to a mobile PFN TRAC system preferably a two way PFN on a host machine full accountable robotics can be provided for most any hazardous environment and or contraband search task. As mentioned earlier, the PFNs could operate electrically controlled weapons in unmanned equipment that was damaged or unmanned either due to the loss of life or to prevent the loss of life by using the machinery and equipment through remote control and or full robotics (based on the level of PFN computers and onboard programming). The options are vast and varied to improve security and safety for all facets of remote control protocols. To help world order and nation building by monitoring equipment and material movement, while robotically controlling terrain and

police an area for aggression, without risking mediating personnel any more than is absolutely necessary. (To help enforce treaties so that the assignees and their constituents are on the same dotted line with the non emotional objective cold hard steel equipment that stands fast to the terms that have been agreed upon- Once again, audio recordings would be in a native language which can be remotely sent as precursors to any physical intervention . First as a persuasive protocol e.g. water cannon, tear gas , rubber bullets and all the way to a final lethal weapon activation as a last resort to save lives and preserve a peace accord) . These PFN armored machines and or equipment would be all terrain like tanks, track vehicles, hum Vs wheeled vehicles, hover crafts. ect. And of course their peripherals could be all of the same and more in the military weapons categories. Eventually special peace keeping PFN controlled equipment would be created to help maintain order in an unstable area (This is a system of MM Network to develop a Real ROBO Cop in plurality, through this technology's Spider eyes program) but first as part of every piece of equipment networked and remotely controlled.

Basically all vehicles machines and equipment will be outfitted with a Protected primary Focal node that allows for universal plug and play capability of varied electronic components. These PFN control centers will be accountable control centers that self police themselves and their components and can report any improper or illegal or dangerous components or equipment operation to the appropriate authorities. These systems will allow the proper government agencies real time control through FACT software in times where public safety or national security are in danger. It will also allow for the quick conversion of commercial off the shelf products e.g. cars, trucks, ect to be specially out fitted with high security government and private components and aggressive remote and automated controls and or weapons in an easy, efficient and more secure manner.

Recently the "car plane" designed by Moller has been developed for future three dimensional transportation for the individual. The technology exists to day to set up a

guidance systems with the three coordinates delivered by the current GPS systems. Their is latitude longitude and elevation and when used with the military's accuracy achieved with an additional correction signal for the ionosphere distortion of satellite signals the GPS accuracy is within centimeters. So most probably this invention will see government use for a while before it is a general public individual transportation tool. In any case the FAA could more readily organize and develop the car-plane technology with this invention . And the PFN will be invaluable in consolidating the accountable black box, communication systems and locating equipment all in one concise system that is easily tailored for monitoring and controlling an ever increasing numbers of these car planes in the future.

Basically all the transportation systems will be coordinated in computer network to micromanage out collision possibilities in any plane or surface travel, and the PFN TRAC system is an ideal system to organize and initiate this effort for present travel and the next millennium . With the PFN capability to down load instructions from the out side (e.g. a control center for air traffic could control a plane from a remote location coordinating the air crafts actions and sensing it's environment and the air ports position and condition and provide the best glide path or course of action in real time aggressive controls e.g the auto pilot controls for any inexperience or compromised pilot through to safety land any aircraft either with human operational assistance or completely by computer control.

FIGURE 3A

This figure is self explanatory in the properties of the most generally used communication devices in the PFN/TRAC system. However a brief review of the cart can help to better understand the use of the devices and guide their use in application and standards consideration. The left side column is the communication devices them selves. In reading down this column there is one way paging ,one way radio frequency signal equipment, two way paging, two way wireless phones and land wired PFN's listed as

PHONE, two way radio frequency signal, and cordless phones which are short range radio frequency signals received and put out on land based phone lines. And finally short range radio frequency signals . However at the very bottom is a definition of letters describing the functions of each of the communication devices ,what they can do and therefore be used for in the PFN applications. Each PFN will have at least one communication device interfaced with a processor system and memory storage

R=RECORD

r= REPORT

O= ONBOARD

RR=REMOTE RECORD

me=MINIMUM CAPACITY

LD=LIMITED DISTANCE

Across the top are activities performed by the PFN such as Audio/Video data gathering, machine activity controls and telemetry, personal or operator telemetry, environmental telemetry. By using the letter key provided it is easy to see the properties, qualities and capabilities of the one and two way PFN systems and determine the best type of system for any particular application. This chart can be referred to when reading and reviewing figures Three Four Five and Six with all the different types of communications detailed. This chart will quickly provide the basic on board record and report back properties and data storage options that can be expected from any particular type of PFN by the communication devices they are employing

FIGURE 4

This drawing is of the simplest one way communication PFN and these basic electronics have already been prototype used and proven from and for the other related

patent applications. Basically with the one way communications there is data storage on board the host in the PFN at two separate locations, but they require physical retrieval of the data. This device in it's most basic form will not report back to any remote control and monitoring system, but can be sent messages, which will activate preprogrammed responses. This is the basic encryption of a one way PFN, but, as was earlier described in figure 3 these units when used in concert with the other two way PFNs can transfer their data and thereby have the two way PFN report the data to a remote location. It also should be noted that this can also be accomplished through a land line comports available to a one way mobile PFNs (provided it is outfitted with the proper DET data encrypted terminal as part of the land line connection or a one way PFN out fitted with DES chips. Of course the same would be true for secure commercial applications as well with PGP protocols. (this is for the high security applications)(non sensitive systems would need no encrypted technology) All that is required is the extendible and retractable connector developed as a variation of the tow bar coupler and electrical connector described in the third related provisional application 112756-300. RE. Interactive high way car towing, car trams or car trains which is the energy efficient individually private mass transit option for land based vehicle platforms in long distance travel.

Also another and more efficient transfer of this data from one and two way pagers for longer messages, which will not require expensive hardware is the infrared comports that have been extensively detailed in the other related applications and or light transmissions or the short range RF transceivers. These systems are used with law enforcement and or secured installations and or stationary commercial settings for industry, ect. for the PFN VTRAC system

To follow the flow of the one way systems in figure four, 300 block of boxes is the world wide sectional and local network gate ways to send data to the one way PFNs as indicated by the thin dotted arrow passing between the wireless transmission box and the security level 403 DES \ PGP box. The question mark in the 403 box is there because

it is optional security for one way transmissions into a secure installation as was discussed earlier.

Looking down from the top center block labeled 200-204 PFN containment is a series of boxes which are all components of the PFN. These components described here are all individual C.O.T.S. products that can be interfaced as separate devices or IC C.O.T.S. components integrated and connected or hard wired together or as combinations of devices and IC components to provide the hardware to support TRAC software. The invention has it's own proprietary configurations that are detailed in many different modalities throughout all the related filings. And the invention's PFNs and TRAC remote control system is capable of interfacing with many other already existing components and systems to enhance any remote control product with greater accountability, security and management. This invention was and always has been expressly designed in this manner to provide a secure physical platform and electrical interface to focus, organize and help standardize remote control functions for all equipment in every application. The TRAC software protocols are designed to continue this security and provide accountability to the system from the PFN to any network the system it is interfaced with. The invention's TRAC programs can be stand alone products or a set of interfaced devices which can be married to any existing system (modular) and add to both creating a better set of products and or better remote control, management and monitoring systems.

To the right 400 is the standard pager as one of the one way receivers and this circuitry is detailed in the first patent. 401 another one way option receiver could be any type of radio receiver on any frequency and all the frequencies are listed in the 60-108 related patent and also here as figures 9 and 10. 402 is a combination of communication and processor functions integrated and combined into one system and a specific C.O.T.S. product made by Motorola Corporation. called "Creat a Link. and is one product that serves as a prime example of the inventions versatile application in utilizing other technologies as part of the protected interface and accountable data storage components

rather than this proprietary pager technology and parallax mini computer if so desired. Of course the TRAC protocol would be programmed into the Motorola software or firmware to authorize software commands, authenticate remote control activity and store it in the appropriate storage. And for certain applications this might be part of an ideal configuration for some application specific PFN's if the functions did not require great amounts of report back data to remote locations.

The mini computer box directly below the C.O.T.S. receiver processor (Creat a link) or comparable device is for the traditional PFN computers either the Basic stamp computers I, II or the planned Euro- boards 188 , 386 and 486 or even those with Pentium processors, that were described in the earlier patent 112756-202. The choices of computer processors is once again application specific with the 386 or higher processor being necessary to support better quality video applications with reasonable speed, smoothness, and quality, for digital applications However. snap shot video applications can be achieved with smaller and less capable processors. The mini computer's the first sacrifice in any real time full video being jerkiness and or the time needed to process the digital image.

However the first prototypes are planned for analog video systems and simple processors to prove feasibility and the digital systems will accompany the more sophisticated minicomputers and special TRAC programming. This can lower video and audio cost for these applications but, will be more costly in the processor system in the beginning. These first video systems will document cabin activities and external activities, and then evolve as an intricate guidance tool for automated and remote control guidance To use video to aggressively remotely control a vehicle and or drive it through automated activity controls it will require extra sensors as to steering parts position speed and the activity controls on the acceleration and braking functions to effectively and remotely control a machine in real time . And other criterion is video quality and properties especially for the report back function which will determine the capability and

speed of the vehicles that can be managed through remote control operations. The on board communication systems e.g. cellular or wireless phones, two way reflex paging and other RF transmission equipment either on board the host equipment and controlled through the PFN and the accountable software TRAC that must manage the authorization of a signal and authenticate any command functions, as well as, process all the sensed operational and driver action data and store it in the two local memories under the proper circumstances with the appropriate time date and command string record.

As detailed earlier for the two way pager systems and limited remote data transmissions they will be assisted by other more sophisticated PFNs that can be utilized in conjunction as (shepherds or watch dogs to better provide visuals for any of these less capable PFN units that have limited, or restricted report back or video quality due to limited data quantity capability especially in reporting transmissions as is the present case for the two way paging system Create a Link II (a Motorola Reflex protocol) or as depicted here a total lack of any on board wireless report back functions , because this is only a one way (Pager) receiver as it is configured in figure 4

To the right of the Mini computer box is the little box GPS number 407 and it is the global positioning system or it can be any type of locating equipment either a separate hand held device interfaced with cables or as an integrated chip set circuit hardwired into the computer or processor, or as merely a chip set as has been described in 112756- 202. Or it might well be a cellular phone triangulation tracking system. All of which can also be in the form of IC cards with edge connectors that plug into the Euro-board 100 mini computers detailed in the second patent 112756-202 as mentioned above and incorporated herein by reference. These would be the hardware components to run the TRAC programmable authorization and authentication as well as, operate and manage the record storage and provide hot geographic coordinates and time synchronization data or confirmation for the local TRAC module clock

The HPC box to the left of the mini computer box is the Host machines Programmable Computer or control circuit and or processor. This can be the only computer in the secure interface or it can be interfaced with other control circuits or processors either proprietary and or other C.O.T.S. products which are coupled in the secure interface and made a more reliable , accountable monitoring and remote control device termed a PFN which stands for (protected) Primary Focal Node. The PFN is designed specifically with versatility to provide a physical platform with a universal electrical set of of plug and play interfaces and accountable TRAC\FACT software to develop a logical organization and manageability for remote control and robotics to meet societies legal needs for all these related technologies and their combined functions. This focal point (PFN) on each piece of equipment housing and linking all electrical control circuits with host peripherals and sensors to off board monitoring and remote controls provide the organization, security and accountability through TRAC software and memory storage for society to meet insurance and security concerns for the use of aggressive remote control and robotics. And above all the PFN and TRAC gives organization and structure to write a Standard to for remote control and robotics applications for all possibilities and applications. The PFN TRAC\FACT system combines and focuses communication control circuits and data storage in one safe and secure accountable local location so that DOD, DOT HIGHWAY SAFTY AGENCIES, FAA, FCC, FBI, CIA , LAW ENFORCEMENT PROFESSIONAL ORGANIZATIONS, E.G. IEEE AND THE MANY INDUSTRY STANDARDS AND WATCH DOG GROUPS can form a standards effort with the major auto manufactures and equipment and machine manufactures in every possible area. The invention has been expressly designed to help create a responsible organized modality to this emerging area of merging technologies and help to marry it well to societies laws and needs.

To the left of the HPC block there is the host equipment interface which would be merely a multi-pin interface connector from the box if the HPC is contained with in the

PFN. The lower blocks below 404 is the sensory or telemetry data gathered on the machine and or operator, and the box to the right represents the functional control of devices or accessories on the host equipment. With these two functions combined the Equipment operation can be achieve through remote control and monitoring all as part of an entire network.

Returning to the center of the page and specifically the lower center their is three boxes displaying the two levels of on board memory storage with three accompanying numbers 105 , 106, 107. These numbers are used to delineate the different types of memory storage devices and not the actual number of devices employed in any specific PFN system. The reason the numbers are used is because these are the present day prototype developments and are listed as present technology, however, due to the vast improvements in memory capacity with all the many different technical variations the invention does not limit its claim to these specific devices and systems that might be employed into this secure PFN , the secure and accountable TRAC and or FACT and or CEW interface and applications.

405 Points out that these data storage components and in fact all the PFN devices and components are detailed extensively in the previous patent 112756 202. However the planed universal prototypes in the security area will be detailed presently as to the proprietary devices components and system functions excluding application specific configurations (soft ware) TRAC for Trusted Remote Activity Controller and FACT Federal Access and Control Technology.

406 shows that the data retrieved from a one way PFN is done through physical contact unless it has an IrDA communication port or short range RF transmitter.

408 is TRAC the programmable and modular software and varies in structure and format based on the different hardware implementations weather it is COTS based, PC, Programmable Controller (Stamp); Or if it is custom, logic Sequencer, micro processor, FPGA (field Programmer Gate Array) or a

custom gate array. Even though these are not all displayed in the three figures in this application all of these hardware options will probably run some form of TRAC software especially to support FACT programs in all application and therefore should be included as hardware implementations for this technologies PFN TRAC\FACT systems, CEW is the commercial encrypted technologies on the inexpensive Web for the payment industry's activities and will accessible to FACT and be capable of accessing FACT to enforce payments on equipment . However these are software programs in existence now for bank card applications with no accountable aggressive remote control to date. So this use through FACT would be a new application and law regulations and rules must be standardized agreed to and legislated in a constitutional manner.

These TRAC Interfaces/Software will have algorithms for BANK/Stock Exchange Transaction--FACT\CEW Products . And many of these will be supported pre-existing COTS products running through the protected primary focal nodes TRAC software. There will be other accountable programs for remotely piloted vehicles RPV and this technologies proprietary PASSS software for the automated slow stop and securing of a vehicle in a stationary position. And this technologies PAGSSS software which has numerous variations but basically it is the proprietary automated guidance slowing stopping and securing of a vehicle through remote control as an evolution of PASSS. Other software specifications include the use of a Commercial:128/64 bit Encryption for web transactions. And for high security in government and military applications: DES the (Data Encrypted Standard)

The interfaces and connectors are named extensively in the related patents however , presently the Automobile industry is planning to start a standardization effort for electrical connect-ability of accessories. This standardization effort has

been the focus for all the related patent applications starting from the real time stop and control box with accountability through the further development of the PFN and this invention looks forward to participating in any effort to develop H-Rel universal electrical connectors, and can offer the actuators, sensor protocols, signal levels in the aggressive automated and remote control devices to reach deeper into a standards effort in this area. As always maintained in this technology the PFN has been created as an accountable organizational interface for all a host piece of equipment's electrical devices, audio sound, video, recording, memory storage processors, computers and communication systems. The PFN TRAC system can support on and off board security control and management for all PFN interfaced equipment This is an important quality to any standard proposed for the auto industry along with accountability and physical protection. Just the organizational platform has tremendous value to any such standards effort for electronic in the auto industry This technology will be constructing prototypes with these interfaces anyway and a collaborative effort is always welcome when ever possible. Telephony is another industry interface with Digital Cellular, PCS, 56K modem, Pager Technology as well as the varied RF signal and light transmission equipment so listed in figure nine and ten of this application and or detailed in earlier related applications.

FIGURE 5

This an illustration of the simplest two way communication systems and the necessary security devices to condition the signal for security protocols with encrypt technology. It is basically another flow chart showing the data from the remote control and monitoring network, as well as, all the data and control signals to the data storage and the peripherals through the many possible processor options running any form of TRAC ,FACT or CEW software programs. This for the most part is the same as figure 4 in structure, however, it provides two directional communication for remote control and

monitoring systems and there by creates the third accountable level of data storage with two onboard and at least one off the host piece of equipment (redundant data storage). The off board can be as simple as an application specific Email or warning flag detailing the PFN TRAC systems ESN electronic serial number to a privately owned or personal E-mail address or it can provide it's data to any number of more extensive memory record systems for any specified event or incident as might be mandated as a standard operation or function legislated by law or developed to standardize accountable real-time remote and automated controls or system management functions.

This drawing is of the simplest two way communication PFN and these basic electronics are planned prototypes from and for the other related prior patent applications incorporated herein by reference. Now with these basic two way communication capabilities there is data storage on board the host machine in the PFN at two separate locations that still can be physically retrieved; but, also the capability to report this data to at least one remote location (which is some what limited by this communication medium) This device in it's most basic form will report back 20 characters to a remote control and monitoring system, through a Reflex paging service in the US, Canada, South and Central America , parts of the Mid East, and Asia. It will also be possible in the future to accomplish this in Europe with the ERMES version of two way paging protocols in the near future. And these messages can be sent to E-mail addresses for inexpensive world monitoring management and control. This can be a privately owned and operated system of any size with a varying level of security through personalized COTS encryption products or part of a larger network of any size and scope and operated in an open fashion of data acquisition or also encrypted to protect personal data to only the authorized personnel.

And of course any of the two way pagers can be sent messages, which will activate preprogrammed responses as is the case with one way paging. This is the basic description of a two way paging protocol PFN, but as was earlier described in figure four

and figure three these units when used in concert with the other two way PFNs with more sophisticated) transmitters and or land line Data Encrypted Terminals or (DETs) can transfer more of their security data efficiently to a remote location. The onboard memory storage will still be as capable as the most sophisticated PFN/TRAC system even though the data transfer to a remote location is some what limited. Also, preprogramming in the PFN computer can send a series of 20 character messages to a remote location, where the monitoring software can reconstruct the whole message. Another option is multi-paging devices that can be combined to send a large data message with different carrier frequencies for each paging device. This would increase the difficulty in intercepting the entire signal or message being reported. (Motorola's Reflex two way paging protocols are being referenced here for all of these options basically, the ERMES products are still under development)

And to reiterate these two way PFNs can also accomplish data transfer though regular land line comport connections where ever available provided the PFN is already out fitted with DES chips or PGP software for it's wireless transmission capabilities.(if not it will have to send it's data through a local DET comport which will probably be hard wired to the local monitor and remote control station or network gateway) . All one and two way PFN's processors and or mini computers will be capable of generating dial up phone tones to connect to a phone node if so desired and deliver direct communication from the computer to any hardwired monitoring center. And of course if land line connections are available for HS and MS security they will have the necessary sending and receiving equipment and TRAC/FACT and or CEW software systems and programs to handle the encrypted signal. Of course the same would be true for secure commercial applications as well with PGP program protocols running as part of these application specific software programs to condition any digital communication signal. This could all take place in an automated setting as well. All that is required is the extendible and retractable connector developed as a variation of the tow bar coupler and electrical

connector described in the third related provisional application 112756-300. RE. interactive high way car towing, car trams or car trains which is the energy efficient individually private mass transit option for land based vehicle platforms in long distance travel. The same communication coupler that link all the PFNs in each vehicle to control which power plants will increase the collective power to increase the speed of the train. A variation of this physical connector to create a physical connection either with another PFN or a stationary installation connection port is an obvious development for anyone skilled in the art and familiar with this inventions technology and patent applications and devices. As also mentioned earlier infrared comports and or other short range light or radio systems could also achieve this same local transfer of data from the one way and limited two way pager and RF systems.

To follow the flow of the two way systems in figure five, 300 block of boxes is the world wide sectional and local network gate ways to send and receive data to and from the two way PFNs as indicated by the thin two directional dotted arrow passing between the wireless transmission box and the security level 503 DES \ PGP box. This 503 box is there because it is a necessary security for any two way transmissions out of a secure installations as was discussed earlier.

Looking down from the top center block labeled 200-204 PFN containment is a series of boxes, which are all components of the PFN and housed within the containment. These components are all individual C.O.T.S. products that can be interfaced as separate devices or IC- C.O.T.S. components integrated and connected and or hard wired together to form combinations of devices and IC components. The invention has it's own proprietary components and configurations that are detailed as many different modalities throughout all the related filings. And the invention's PFNs and remote control system is capable of interfacing with many other already existing components and systems to enhance any remote control product and or security system in many ways. This invention was and always has been expressly designed in this manner to

provide a secure physical platform and electrical interface to focus, organize and help standardize these functions for all remote controlled equipment for every application. The invention can be a stand alone device and or system of any size (or a set of interfaced devices systems and networks) or it can be married to any existing system and add to both by creating a better set of products capabilities and remote controls in any monitoring system as well as provide accountability through the TRAC/FACT and CEW software programs.

To the right 500 is the standard two way reflex pager as one of the possible two way receivers. 501 another two way optional transceiver, which could be any type of radio transceiver on any frequency and most all the frequencies are listed on figures 9 and 10.

However, the allocated and dedicated frequencies are designated and many of them are shown on the allocation chart . These of course would be the ones used for the Government and other high level security protocols however as has been stated the pager and wireless phones can be commercial grade frequencies accompanied with encryption technology for security. For this reason other low cost public airway can be utilized with these same security protocols. 502 is a combination of communication and processor functions integrated and combined into one system and is a specific C.O.T.S. product made by Motorola Corporation. called "Creat a link II". This all in one product serves as a prime example of the inventions versatile application in combining other technologies as part of the protected interface and accountable data storage components, when ever possible, rather than solely relying on the proprietary pager technology and parallax mini computer and other proprietary computers if so desired. And for certain circumstances this might be part of an ideal configuration for some application specific PFN's. This Motorola product "Creat a link II is different in that it employs the reflex two way paging protocols which are a necessity to achieve the report back function for this minimal two way variation

In the drawing the mini computer box directly below, the C.O.T.S. Receiver processor (creata link or comparable device) is for the traditional PFN computers. Either the Basic stamp computers I, II or the Euro- boards 188, 386 and 486 or even those with Pentium processors, that were described in the earlier patent 112756-202. The choices of computer processors is once again application specific with the 386 or higher processor being necessary to support full video applications with reasonable speed, smoothness, and quality, however. Snap shot video applications can be achieved with a smaller and less capable processors in the mini computer with the sacrifice in any real time full video being jerkiness and or the time space needed to process any digital image. This condition requires extra sensors to effectively and remotely control a machine so equipped in near or very near real time. And other criterion in video quality especially for the report back function is the level and capability of the on board communication systems e.g. cellular or wireless phones, this 2 way reflex paging and other RF transmission equipment either on board the host equipment and or controlled through the PFN. Or assisted by other more sophisticated PFNs in the network and or on location that can be utilized in conjunction as (shepherd systems or watch dogs to better provide visuals for any of these less capable PFN units that have limited or restricted report back or video quality due to their capability to handle the quantity of data required, especially in reporting transmissions as is the present case for the two way paging system Creat a Link II (the Motorola Reflex protocol) .which is best set up to report back in a limited snap shot of images, . However much other report back data from other sensors can be provided a good and reasonable form of communicating their data back to at least one remote location.

To the right of the Mini computer box is the little GPS box number 507 and it is the global positioning system or it can be any type of locating equipment Lorands, cellular triangulation, LoJack ect. either as separate hand held devices interfaced with cables or as a integrated circuit hardwired into the computer or processor , or merely a

chip set as has been described in 112756 202. The last two of which can also be in the form of cards with edge connectors that plug into the Euro-board 100 mini computers detailed in the second patent 112756-202 as mentioned above and incorporated herein by reference.

The HPC box to the left of the mini computer box is the Host machines Programmable Computer or control circuit and or processor. This can be the only computer in the secure interface or it can be interfaced with other control circuits or processors either proprietary and or other C.O.T.S. products which are coupled in the secure interface and made a more reliable , accountable monitoring and remote control device termed a PFN which stands for (protected) Primary Focal Node. The PFN is designed specifically with versatility to provide a physical platform with a universal electrical set of interfaces to develop logical organization and manageability for remote control and robotics to meet societies legal needs for all these related technologies and their combined functions. This focal point (PFN) on each piece of equipment housing and linking all electrical control circuits with host peripherals and sensors to off board monitoring and remote controls provide the organization, security and accountability to justify to society and meet insurance and security concerns for the use of aggressive remote control and robotics . And above all the PFN/TRAC/FACT/CEW system gives structure and organization to write a Standard (for remote control and robotics applications by focusing communication control circuits and accountable data storage into one safe and secure location . DOD, DOT HIGHWAY SAFTY AGENCIES, FAA, FCC, FBI, CIA , LAW ENFORCEMENT PROFESSIONAL ORGANIZATIONS, E.G. IEEE AND THE MANY INDUSTRY STANDARDS AND WATCH DOG GROUPS. The invention has been expressly designed to help create a responsible organized modality to this emerging area of merging technologies and help to marry it well to societies laws and security needs.

To the left of the HPC block there is the host equipment interface which would be merely an interface connector from the box if the HPC is contained within the PFN. The lower blocks below 504 is the sensory or telemetry data gathered on the machine and or operator, and the box to the right represents the functional activity controls of devices or accessories on the host equipment. With these two functions combined the Equipment operation can be achieved through remote control and monitoring all as part of an entire network.

Returning to the center of the page and specifically the lower center there is three boxes displaying the two levels of on board memory storage with three accompanying numbers 105, 106, 107. These numbers are used to delineate the different types of memory storage devices and not the actual number of devices employed in any specific PFN system. The reason the numbers are used is because these are the present day prototype developments and are listed as present technology, however due to the vast improvements in memory capacity with all the many different technical variations the invention does not limit its claim to these specific devices and systems that might be employed into these present day PFN secure interface systems. It is equally important to remember that the technology has been and always will be engineered for both backward and forward technology interfacing, as well as, provide the present day technical options 505 Points out that these data storage components and in fact all the PFN devices and components are detailed extensively in the previous patent 112756 202. And other related patents. However, the planned universal prototypes in the security area will be detailed presently as to the proprietary devices components and system functions excluding application specific configurations and any specific secret (software) protocols

508 is TRAC the programmable and modular software and varies in structure and format based on the different hardware implementations whether it is COTS based, PC, Programmable Controller (Stamp); Or if it is custom, logic Sequencer, micro processor, FPGA (Field Programmer Gate Array) or a

custom gate array. Even though these are not all displayed in the three figures in this application all of these hardware options will probably run some form of TRAC software in some application and therefore should be included as hardware implementations for this technologies PFN
/TRAC/FACT/CEW

These TRAC Interfaces/Software will have algorithms for BANK/Stock Exchange Transaction Products . Many of these will be supported COTS products and through the primary TRAC/CEW software protocols. There will be other accountable programs for remotely piloted vehicles RPV, and this technologies proprietary PASSS software for the automated slow stop and securing of a vehicle in a stationary position These will all be part of or have a FACT component to control these functions by the appropriate authorities in an accountable manner. And the PAGSSS software which has numerous variations but basically it is the proprietary automated guidance slowing stopping and securing of a vehicle through remote control as an evolution of PASSS will also be responsive to Federal Access Control Technology FACT. Other software specifications like the Commercial Encryption on the WEB include the use of a Commercial:128/64 bit Encryption for web transactions. And for high security in government and military applications: DES the (Data Encrypted Standard)

The interfaces and connectors are named extensively in the related patents however , presently the Automobile industry is planning to start a standardization effort for electrical connect-ability of accessories. This technology has been focused on this point or issue through all the related patent applications and looks forward to participating in any effort to develop H-Rel universal electrical connectors, and can offer Actuators, sensor protocols, signal levels in the aggressive automated and remote control devices to reach deeper into a standards effort in this area. This technology will be constructing prototypes with these

interfaces anyway and a collaborative effort is always welcome when ever possible. Telephony is another industry interface with Digital Cellular, PCS, 56K modem, Pager Technology as well as the varied RF signal and light transmission equipment.

FIGURE 6

Shows a system that can support the most sophisticated high security and two way communication capability for full real time audio \ video with either cellular or digital phone or any other comparable radio frequency equipment specially delegated for these purposes (either Military controlled and or operated, or a joint venture of commercial and governmental support e.g. COMSAT commercial and government satellite system. No matter what ever, even if the commercial wire and land based phone technologies are utilized all will be provided either EDS or PGP encryption protection for Medium and high security applications even if it is used on the commercial Internet, and today there is cellular system for the payment industry to transact bank cards wirelessly and these COTS products will be interfaced through the PFN or proprietary CEW software can be used. This most sophisticated machine messaging PFN is being proto-typed to support and report every data signal sensed and provide any aggressive remote control for any devices by previously described proprietary technology and or versatile interfacing with other technologies. However, the cost will be proportionate to the level of sophistication and the amount of hardware, firmware, software, and peripherals required or desired .

Even the least expensive one way PFNs can be ordered to activate or deactivate as well as control varied performance of what ever they are connected to. So the system cost can be greatly reduce by using the less expensive (page type) one and two way PFNs where sophisticated real time video systems to monitor and record are not required form the remote control unit itself.. However these costs will certainly be reduced with these systems being utilized in vehicles for guidance in automated highway systems. But the

present lower cost PFNs can still be utilized to wage an aggressive response where all friendly life has been removed from an environment, installation, machinery and or vehicle if the extreme need exists to take radical action. Any standard or specially installed accessory can be remotely controlled. From terminating the use of a piece of equipment by standard means, to energizing airbags on a terrorist, to totally terminating a piece of equipment in a hostile situation through extraordinary means (by PFN detonation's, of explosives ect)

As mentioned earlier just one mobile sophisticated PFN in most cases. (as the shepherd or watch dog unit can supply visual data to any remote monitor and control terminal). The more sophisticated the watch dog unit the greater the protection of the sophisticated unit.. This system can and should be armored and capable to support aggressive weapons e.g. surface high current capacitor shock equipment systems, laser and electro-magnetic wave weapons microwaves , sleeping agents, tear gas , water cannons , pepper spray, tazzor gun, net mortars, rubber bullets and convention automated machine gun, cannon and explosives for the extreme security scenarios. Of course the host platform will dictate some of the conditions and restrictions to support any of these devices as well as any real need for any of these aggressive protective defense devices. Identification systems can be employed to recognize friendlys when they arrive and can take orders directly form them on location if need be. This can be accomplished through any and all forms of the short range communication systems already described that can even differentiate friendly from aggressors during a security incident or emergency with the technology already described throughout all the related patents e.g IrDA, and or limited RF transmission devices other light transmissions and the phone system or any other RF transmitter (which will be personally coded device communicators limiting access by finger print or one of the many other Id systems previously detailed). In the third formal 112756-301 all the electronic devices that are to be controlled normally for accountable aggressive remote and automated control are thoroughly detailed. However,

this high security and medium security applications that involve police and military option will be developed in a collaborative effort with the appropriate government agencies and manufacturers of the weapon devices. It is sufficient to state presently that the PFN TRAC system will be capable of running the standard FACT software programs and can be easily adapted to run and support DES chips and or provide the same protected power, activity control hook ups and sensor array systems to provide police and military options as have be discussed above.

The PFN/TRAC system on any piece of equipment machine and or vehicle, will have a protected connector section that specifically provides the circuitry for these specialized security devices and protocols for the extreme aggressive protection and retaliation packages and options needed .

These devices will in many cases be part of regularly needed host equipment and naturally camouflaged and incorporated into their structures their appearance will be a natural and peaceful one, while harboring a great capability to provide varied levels of aggressive security with the least amount of friendly personnel in harms way. (This system for high security automated aggressive response will be known as the ("Trojan Horse defense System) (THS) And could have as a final option for every security PFN in the system a self-destruct order protocol to secure any violated security area where there are only aggressors left. And this final option can be initiated form any where in the world with the correct encrypted secure codes held by the responsible authorities. These TRAC /FACT/DES systems of course would have special considerations and guidelines set up for governmental and national security agencies, as well as, world organizations involved many of the most extreme PFN utilization's like TRAC's FACT/DES/ THS would be legislated policy and developed under the strictest security protocols. The invention is merely the organizational platform to physically secure and electrically secure and organize the appropriate components to provide the means to incorporate the public safety and national and world security options.

The Protected PFN data storage would support any reported record to justify any such decisions and their should be well established procedural protocols for these security scenarios for e.g. Embassies , military installations, nuclear facilities, and any special security risks or treaty refereeing ect.

All monitoring for every condition in these high security environments would be greatly enhanced and response time to any event or emergency would be almost immediate with accurate data and audio and video records on exactly what transpired to analyze and remedy any same negative situation in the future and or to prosecute any impropriety that transpired or review fairly any improper action taken

This drawing is of the most sophisticated two way communication PFN and this electrical configuration is the basis for all prototypes in every application no matter the level of security. The only thing that changes besides DES hardware is the specific TRAC –Application Specific Software provided for the normal host machines purpose these ASS programs will run normal operation and FACT and THS will be down loaded to allow for strategic command control of all available activity controls normal and specialized in real time as deemed necessary by the appropriate authorities. These downloads can be performed on standard manufactured equipment to provide security control through PFN TRAC/FACT/THS system for any rapid deployment need. All the components are and will be proven and in most cases C.O.T.S. products are in use presently. . Basically with this more sophisticated two way communications there is once again data storage on board the host machine in the PFN at two separate locations, that can also be physically retrieved . However, these PFNs and TRAC software will have full report back capability on their own for every data stream to any desired remote control and monitoring system. And they are also capable of retrieving data from any less capable PFN as earlier mentioned and reporting their data back to the monitoring and control centers. This is accomplished through physical connections or IrDA communication ports and or light or RF transmissions as has been detailed throughout the

related patents. Once again all that is required for the physical coupling is the extendible and retractable connector developed as a variation of the tow bar coupler and electrical connector described in the third related provisional application 112756-300. RE. interactive high way car towing, car trams or car trains which is the energy efficient individually private mass transit option for land based personal vehicle platforms in long distance travel . Of course the infrared comports that have been extensively detailed in the other related applications and or any of the light transmissions and or RF signal transceivers will once again reduce the hardware needed to complete the interface and any data transfer.. (But what ever the transmission be physical or wireless of any type; the modality will have to be assessed for it's vulnerability to access any signal and or transmission and the appropriate DES-PGP and or any other security Protocols will have to be in place at either end of any data transfer if deemed warranted) as part of TRAC/FACT/THS for the very high security protocols commercially but basically militarily. This focus on the high security protocols was done to show peripheral accessories attached to the standard sophisticated PFN/TRAC/FACT/THS system however the same PFN TRAC system will be used in everyday applications with out DES and all the other high security protocols and functions. This is what is both unique and necessary to provide cost effective controls ,protection and utilization of accountable remote and automated control and management systems for the future. And this is why the Protected Primary Focal Node (PFN/TRAC system is going to be essential in concept and function to write standards, laws, legal regulations and basically organize these merging technologies in a safe and fair manner for all.

Note: The more sophisticated PFN has been chosen to elaborate on the High security activity controls in general but this does not mean that these extreme aggressive controls are not available on the less sophisticated one and two way paging or RF or short range cordless phone communication systems. This may very well be the case and especially

when used in concert with one or two sophisticated PFN systems or or other security surveillance systems.

Not yet detailed is the TRAC's FACT program that will carry some high level security control encrypted Commands to allow the proper authorities to control any and all equipment, machinery, and vehicles in a state of emergency. This of course will be determined by the public and it's governing bodies and agencies. The Protected Primary Focal Node/Trusted Remote Activity Controller/ Federal Access and Control Technology or PFN TRAC/FACT system is designed to be accountable to all parties using and effected by machine use and it's impacts. Accountable Aggressive Remote and Automated Control scenarios and real-time control security functions is just two of the many real-time management task performed in an accountable manner by the PFN/TRAC/FACT/CEW system.

To follow the flow of this two way sophisticated system in figure six ,300 block of boxes is still the same world wide ,sectional and local network gate ways to send data to all the PFNs as indicated by the thin dual directional dotted arrow passing between the wireless transmission box and the security system box 603 DES \ PGP box. The 603 box is there because it is an obvious security necessity for any two way transmissions into and out of a secure installation as has been discussed earlier. With constant transmissions sent out of the compound it would be far easier to obtain critical data to remotely control these PFNs without the Data Encryption.

Looking down from the top center block labeled 200-204 PFN containment is a series of boxes which are all components of the PFN. These components are all individual C.O.T.S. products that can be interfaced as separate devices or IC C.O.T.S. components integrated and connected or hard wired together or as combinations of devices and IC components. The invention has it's own proprietary configurations that are detailed in many different modalities throughout all the related filings. And the

invention's PFNs and remote control system is capable of interfacing with many other already existing components and systems to enhance any remote control product and or security system in many ways. This invention was and always has been expressly designed in this manner to provide a secure physical platform and electrical interface to focus, organize and help standardize these functions for all equipment in every application. The invention can be a stand alone system or a set of interfaced devices or it can be married to any existing system and add to both to create a better set of products and remote control or management and monitoring system.

To the right 600 is the standard cellular phones (Digital (D wave) and analogue) as the two way transceivers and this circuitry is detailed in the second patent detailing all the modems and cable connections for all the possible C.O.T.S. hand held devices. And also all the PCMCIA cards were described as well as cellular phone IC cards that can be connected to the all the computers listed in the same second patent 112756-200.

601 another two way transceiver option could be any type of radio frequency unit on any frequency and all the frequencies are listed on figures 9 and 10. The government has a multitude of special application frequencies that might be a requirement for any application specific use, so this is always going to be an option in any PFN for any uses but most especially for high security applications.

602 can be a combination of communication and processor functions integrated consolidated and combined into one system and or a specific C.O.T.S. like the simplified switching device "Creat a link" but more sophisticated and capable. Some such products exist presently and were developed for the trucking industry by companies like, LA Guard and Prince, Highway Masters, now part Johnson Controls and the GM Onstar System. And of course these C.O.T.S. products will be easily accommodated and be enhanced in the protected and accountable interface with all the signal security (DES and PGP) in place and required for any high security remote control and or aggressive action. This is another example of a present day versatile application utilizing another

technology as part of the protected interface and accountable data storage components of PFN\TRAC. However, all these functions can be provided by the inventions proprietary technology and mini computers if so desired in the proprietary PFN and running TRAC/FACT software.

602 also lists the Complete PCMCIA Card which is a product that combines the Cellular phone technology and modem into one device with antenna for lap top computers to function in a wireless environment for phone data connections. This particular C.O.T.S. product has been singled out as one system that will be utilized in the security PFN prototypes and is mentioned here and will be totally detailed in the formal application. Of course in the DES security mode the modem section will have to be modified to accommodate the DES chip set. or this function of encryption will be accomplished in the mini computer through down loaded modular software which will also be able to accommodate any DES chip sets and or in the case of PGP encryption run any of the necessary software. TRAC/FACT. In many cases or applications of CEW commercial banking companies e.g. NCR, ect. will provide their own proprietary encrypted software algorithms however ,the PFN\TRAC\FACT system will be structured to support all COTS software and all COTS software must provide for FACT identification e.g. ESN and special access to their programs and hardware or firmware to be used commercially as part of a standard to be developed on operating regulation in remote control and data management applications systems.

The mini computer box directly below, the C.O.T.S. Transceiver processor option is for the traditional PFN computers either the Basic stamp computers I, II or the Euro boards 188 , 386 and 486 or even those with Pentium processors, that were described in the earlier patent 112756-202. The choices of computer processors is once again application specific with the 386 or higher processor being necessary to support full digital video applications with reasonable speed, smoothness, and quality. The other criterion that will give good video quality and properties for the report back function is

the on board communication systems e.g. cellular or wireless phones and any other capable RF transmission equipment on board the host equipment and controlled through the PFN. This system is the shepherd or watch dog to better provide visuals for any of the less capable PFN units that have limited or restricted report back or video quality due to data size, band width, and transmission time capability especially in transmissions from the two way paging system "Creat a liink II" (a Motorola Reflex protocol) or as is the case with the one way (Pager) receiver as it is configured in figure 4 which has a total lack of any wireless report back functions in and of itself .

To the right of the Mini computer box is the little box GPS number 607 and it is the global positioning system or it can be any type of locating equipment either a separate hand held device interface with cables or as a integrated circuit hardwired into the computer or processor , or merely a chip set as has been described in 112756 202. The last two of which can also be in the form of cards with edge connectors that plug into the Euro-board 100 mini computers detailed in the second patent 112756-202 as mentioned above and incorporated herein by reference. One important note is that any and all PFNs can be outfitted with GPS and of course the most sophisticated can provide hot accurate readings and give positions with the military GPS with in centimeters with their additional ground signal that in allows for the algorithm to adjust for the distortion that the ionosphere creates in the commercial versions of the GPS which are only within 30 meters as to an accurate location if so designated by the proper authorities. Also with the latest Cellular locating systems or other land based RF signals either more accurate or 4th signal convergence algorithms can be employed in the PFN software to increase the standard GPS geographic location coordinates accuracy to be more like the military GPS which corrects for the ionosphere deflection from the satellites signal.

So the importance of the GPS accuracy has great value to provide vital data for accurate evidence as a primary goal of the accountable protected primary focal node. It provides accurate geographic audio's and visuals, as well as, environmental telemetry to

asses any aggressive personnel, ordinance, and hazards that might be present and in control .in a rescue scenario or recovery effort of a lost security area. The pinpoint data reported from the PFNs will provide an important tool to evaluate a hostile situation and determine the best course of action. And as earlier stated the PFN s can help wage an aggressive war, when and if that choice is unavoidable. Or bring a hostile event to an early closure with the least amount of lives lost. Also the accurate locating systems consolidated in the PFN /TRAC hardware and software systems provide accurate geographic and time and date data for the every day situations of machine use that can be authenticated as evidence grade data with the ESN from the resident PFN and host piece of equipment ESN along with all active device ESN in a command string header for contact and response.

The HPC box to the left of the mini computer box is the Host machines Programmable Computer or control circuit and or processor. This can be the only computer in the secure interface or it can be interfaced with other control circuits or processors either proprietary and or other C.O.T.S. products which are coupled in the secure interface(s) and made a more reliable, accountable monitoring and remote control device termed a PFN Which stands for (protected) Primary Focal Node. The PFN\TRAC system is designed specifically with versatility and universality, to provide a physical platform, with a universal set of electrical connections and interfaces which are ideally standardized as much as possible. And coupled to TRAC authorization and authentication software controlling the local and remote event memory storage functions; to develop a logical organization and manageability for remote control and robotics to meet societies legal requirements and social needs for all the related technologies and their combined functions. This focal point (PFN) and TRAC software on each piece of equipment housing and linking all electrical control circuits with the host peripherals and sensors to off board monitoring and remote controls provide the organization, security and accountability through the TRAC system, to justify to society and meet insurance and

security concerns for the use of aggressive remote control and robotics in any scenario. And above all the PFN/TRAC/FACT system gives structure to write Standards to: (laws, rules regulations and code) for materials, interfaces, procedural use and or protocols to perform accountable responsible remote control and robotics by focusing communication, control circuits, locating equipment for time and geographic information, to accountable data storage through TRAC FACT software in a safe, secure location for the most part . DOD, National Security Agencies and public governing committees, political bodies and agencies, like; CIA, Secret Service, DOT, HIGHWAY SAFTY AGENCIES, FAA, FCC, WWW management agencies and organizations, The Justice Department, FBI, LAW ENFORCEMENT PROFESSIONAL ORGANIZATIONS, E.G. IEEE , Automotive manufactures and other manufactures, Intelligent Transportation Society, The Insurance industry, AND THE MANY INDUSTRY STANDARDS AND WATCH DOG GROUPS, as well as the general public input, should make up the groups that will deliberate and form the laws to be legislated on by congress, with the appropriate rules, regulations and protocols needed to plug the appropriate, safety for the individual and society in a fair and appropriate manner to be incorporated in legally approved software applications and commands utilized by PFN/TRAC/FACT systems, keeping the necessary secretive final aggressive commands protected, from the general public for obvious security reasons to only be used by the appropriate authorities; but always monitored and recorded for total accountability to society in general and each and every individual citizen.

(These should be basic criterion of any (MMN anywhere and most especially on the web or WWW) as part of any machine messaging network. interfaced. Often with the world wide web and or the Internet from and through the PFN/TRAC gateways will create more and more equipment, machine and vehicle monitoring as well as document more human activity.

So in this process of real-time accounting of equipment use and impact we have to respect one another and the use of our shared environment.

For this reason and others the invention has been expressly designed to help create a responsible organized modality to this emerging area of merging technologies and help to marry it well to societies laws and needs as it prepares data on the changes in the environment .

To the left of the HPC block there is the host equipment interface which, would be merely an interface connector from the box if the HPC is contained with in the PFN. (these connectors are all shielded and protected in the higher security applications any will enjoy as much protection as is application specifically needed). The lower blocks below 604 is the sensory or telemetry data gathered on the machine and or operator, and the box to the right represents the functional control devices, or the activity control of devices and or accessories on the host equipment, which will be standard automated controls for the machine and operator for the most part unless there is an application specific need. For example, some of these accessories will be the extreme aggressive defense weapons described earlier and in fact any electrically controlled defense devices can be remotely controlled not only by this sophisticated PFN, but even by the simplest PFNs, while viewed by the sophisticated PFN or surveillance video cam and controlled remotely. And with these two functions combined any and all equipment operation is achieve through remote control and monitoring all as part of an entire local network that gives greater security options. This provides tremendous back up and force to any security system with constant alternatives to regain control and stability in a threatened security environment and or situation with the least risk to all life, which will always be proportionate to the skilled personnel, controllable equipment available, circumstances and the choices they make, which what ever they are; they can always be accountable ones in local memory and in the system's network.

Returning to the center of the page and specifically the lower center there is three boxes displaying the two levels of on board memory storage with three accompanying numbers 105 , 106, 107. These numbers are used to delineate the different types of memory storage devices and not the actual number of devices employed in any specific PFN system. The reason the numbers are used is because these are the present day prototype developments and are listed as present technology, however, due to the vast improvements in memory capacity with all the many different technical variations the invention does not limit its claim to these specific devices and systems that might be employed into this secure PFN interface as the only modalities to establish accountability on board in the PFN.

605 Points out that these data storage components and in fact all the PFN devices and components are detailed extensively in the previous patent 112756 202. However the planned universal prototypes in the security area will be detailed presently as to the proprietary devices components and PFN\TRAC/FACT/THS/CEW system accountability functions. All the prototypes will be completed as detailed in this formal patent application 112756 401-and 501 The TRAC/FACT/THS/CEW plus any application specific programs for Home management , Commercial management, Controlled Security Technology, Mobile management for both surface and air transportation systems. All of these will have master control centers and multitudes of commercial servers interfaced and inter linked. This is only mentioned in this most sophisticated system of the PFN but all variations of the PFN's will be appropriately linked and functional through TRAC and FACT unless they are DES specially isolated.

606 is the physical recovery of on board data as has been described thoroughly in figures four and five and of course this more sophisticated communication PFN has the off board data storage in the monitoring and control system, which is limitless in the dial up services it can send it encrypted data to. This is not so with the two way pager systems they must rely on a specific page service provider. And all the two way RF systems are

only limited by the amount of transceivers able to receive a signal.

608 is TRAC the programmable and modular software and varies in structure and format based on the different hardware implementations weather it is COTS based, PC, Programmable Controller (Stamp); Or if it is custom, logic Sequencer, micro processor, FPGA (field Programmer Gate Array) or a custom gate array. Even though these are not all displayed in the three figures in this application all of these hardware options will probably run some form of TRAC/FACT software at least in some application and therefore should be included as hardware implementations or firmware implementations or even any form of modular software for this technologies PFN/ TRAC systems including FACT,CEW.THIS or any of the application specific software systems Home, Commercial, Control high, medium and or general security and or mobile control and management for either surface, land or sea or air and space

All TRAC Interfaces and their Software will have algorithms for BANK/Stock Exchange and all sorts of payment industry Financial Transaction Products . Many of these will be supported by pre-existing COTS products and managed through the protected primary focal node hardware and TRAC/CEW software 128/64 bit commercial off the shelf products presently, however, the full nature and scope of this invention is to support any security protocol that is a accepted financial standard and this up to date banking and automated wireless and hard wired payment industry capability is and always has been a most primary stated goal and purpose and most definitely falls with in the nature and scope of the invention and it's general purpose to receive real-time payments for fee for use applications or penalty assessments for improper or unauthorized and or abusive use.

There will be other accountable programs for remotely piloted vehicles RPV however, this technologies proprietary PASSS software for the automated slow stop and securing of a vehicle in a stationary position. And this technologies PAGSSS software which has numerous variations but basically it is the proprietary automated guidance

slowing stopping and securing of a vehicle through remote control as an evolution of PASSS. Other software specifications include the use of a Commercial:128/64 bit Encryption for web transactions. And for high security in government and military applications: DES the (Data Encrypted Standard) To be modular and programmable or even physically insert-able chips into PFN/TRAC/FACT COTS products for rapid conversion to high security and or military operations.

All the present interfaces and connectors are named extensively in the related patents however, presently the Automobile industry is planning to start a standardization effort for electrical connect-ability of accessories. This concept technology has been the major focus of this invention through out all the related patent applications to provide an accountable protected local control center that can electronically log, interrogate and inventory as to each components ESN and or it ESN software or identification designation into an operation PFN inventory of guest devices. This log is updated on every up boot of the system , new device installation and periodic inventory checks as a primary procedural function of TRAC and FACT software. The PFN/TRAC/FACT will report any new inventory components and check it against any National Registry Alerts compare list as a standard software function(understandable to anyone skilled in the art) The full application of the National component. device, part and equipment registry is detailed in this application extensively in figures 16, 17, 18,19 20, 21 22

This invention has been develop to organize and coordinate an accountable electrical interface for every type of electronic equipment used on any type of equipment and provide a tracking service to control any illegal unlawful, unauthorized and or dangerous use, misuse or abuse of equipment and or to help thwart any criminal or negative impact on society, it's economy, the environment and or any of societies infrastructures. This is accomplished through the TRAC/FACT system of identity tracking that will require legislated law rules and regulations to be applied to this great innovative technology's National part, component, device and equipment Registry that

can eliminate theft, misuse of property and make any and all components fully accountable for their actions in remote and automated control scenarios but also their impact on others and the environment. Of course the proper rules regulations and law must be constructed for this accountability tool and it must meet the real-life test of fairness to all, but ultimately product quality assurance, public safety, national security, and crimes of stolen property (all electrical components) can be handled through the PFN/TRAC/FACT system for normal life situations in the most fair and accountable manner

With all this in mind this invention looks forward to participating in any standards effort to develop H-Rel universal electrical connectors, and can offer actuators, sensor protocols, security FACT chip signal systems for use in aggressive automated and remote control devices which can reach deeper into a standards effort in this area to develop this National Registry detailed in figures 16, 17, 18, 19, 20, 21 &, 22. This technology will be constructing prototypes with these interfaces anyway and a collaborative effort is always welcome when ever possible. Telephony is another industry interface with Digital Cellular, PCS, and 56K modem, Pager Technology as well as the varied RF signal and light transmission equipment. Which are configured to run all the PFN/TRAC/FACT/CEW and or the high security programs like THS with DES chip insertion.

These last three figures have been taken from this technology's high security application because these are the hardware components that will support the Trusted Remote Activity Controller TRAC/FACT software systems for all normal PFN systems and in the prototypes. This technology has provided the security descriptions to maintain the versatile COTS quick change of standard commercial cost equipment in a high security application and to still provide secure integrity to this HS application. This technology provides general cost and time conversion savings and versatility from normal life remote and automated control systems to high security applications. This is

accomplished by creating an protected secure environment of accountable record keeping to perform automated and remote control activities for society and it's institutions with all the locked compartments seals and proper laws governing use and access to critical areas (to be determined in the standards effort and properly legislated into law for the local secure areas in the PFNs . The same standards effort would also create the governing guide lines and device use for the TRAC/ FACT system on and off the host equipment and help legislation to create a constitutional laws rules regulations governing the programs use and setting penalty and crime statutes for it's miss-use to insure the proper public safety, national security, and respect for the individual citizen's privacy are guaranteed.

To demonstrate the versatility of the PFN\TRAC system and it's uses. No high security strategies or specifics will be detailed here and they would be worked out by the appropriate authorities and downloaded into the respective PFN's or physically installed to perform their approved security and defense tasks. This technology is well aware that the military and their suppliers have developed much of the robotics system for combat today and combining, connecting and interfacing our standard protected PFN control center on normal every day equipment with it's FACT software higher security application involving DES/THS is our main consideration and contribution to the extreme aggressive conditions that might require police or military robotics options. Ideally the invention may serve as an electrical platform either added on or already existing to monitor equipment movement to track supplies and provisions in a treaty agreement ect. and or supply unmanned multi lingual policing in hostile areas with out having mediating military in harms 'way. The TRAC/FACT/DES accountability aspect will serve well to properly use automated and remote controlled force in real-time anywhere in the world and fairly review that use thereby keeping it at the correct level and help and to present the truth in any conflict area to aid in resolving mis-trust and paranoia and separate it from real threats and fear .These Protected Primary Focal Node

Trusted Remote Activity Controller software programs to perform accountable aggressive remote and automated control through PASSS (Slow Stop and Secure all vehicles and or equipment) PGASSS (second generation Guide Slow Stop and Secure) running Commercial encrypted payment industry on the Web CEW and all the application specific management PFN programs like HMS home Management System, Commercial Management Systems CMS Mobile management systems MMS Control Security Technology CST Federal Access Control Technology FACT or the high security applications Trojan Horse System with DES Data Encrypted Standard

PFN\TRAC\PASSS\PAGASSS\CEW\HMS\CMS\MMS\CST\FACT\DES\THS

Application specific software systems will provide for an organized development of this technology so that it marries well to a democratic and free society that has embarked on the technical road to mass data gathering management and memory storage, while it respects the individuals rights to privacy by providing accountable protocols for access to personal or privately owned data gathering equipment. Because PFN\TRAC can provide objective records in a constitutional manner for all, disputes it will become much more clear and easier to resolve disputes, and open the road for humanity to share control of all machinery with other individuals and automated control systems. The PFN\TRAC system can provide the means to value operation and system use as well as individual failures of man and the equipment, and in many cases provide fail safe systems as well or a least detect when a system has failed and become unpredictable and unaccountable. This invention is an ideal way to usher in the shared control scenarios of man and machine in the future in a sane and fair manner. Of course the use and the laws governing any abuse will be determined by the people and their duly elected governing bodies and appropriate government agencies police systems civilly and armed forces globally. Policy will be determined by the appropriate levels of governing organization for the strategic and or defense use deployment and protocols of the PFN\TRAC\FACT\DES systems with

COTS products around the world. The invention can help manage and or control and witness altercations and disputes to provide fair and correct review and accountability for the events and actions taken . And this invention could of course be coupled with world organizations and all involved nations to determine application and use whenever conceivable and possible. These areas would be legislated and laws rules regulations and all the appropriate legal structures can be addressed and put into place to preserve the best quality of life possible for the individual and their society. The PFN/TRAC systems can create a fair deal trust among all societies, but it still requires all the people to accomplish it.

This figure six was used to explain the total social impact and growth of this technology and figure 6a will show how the invention stays current with the future developments and still provides all the properties and qualities, while the technologies merge and consolidate together. This is done to leave no doubt in anyone skilled in the arts that the total impact and development of the invention has been visualized and is thoroughly detailed for it's full technical nature, scope and value but also, for it's total use impact on humanity and the environment for the present and long into the future.

FIGURE 6A

This figure is devoted to showing the future merging of communication technologies with micro processors and greater memory storage and conversely greater product capabilities and efficiency both in size and function. It has been created deliberately to detail out a good clear commercial evolution of consolidation of technology in the (PFN) so anyone skilled in the arts can easily structure the most cost effective combination of COTS products or components to create the best PFN for the present time and into the future. It also has been done to clearly show that all these developments were planned and detailed within the related patent applications to keep the invention current in the future.

or any other product control and ID data. Then when all components registered by their manufacturer in the National Registry at point of shipment to the commercial market and secondly confirmed when in use in real-time by a legitimate owner and at the point of installation through the PFN and uni-buss super modem at present completed automatically by the firmware fact chips install by the manufacturer and the FACT software operating in the PFN/TRAC system. This is detailed more extensively in this patent application

6A(UTU) The super modem also supports the uni-bus internal link in the same manner. This is not per/se a new Modem or modem design standard. But the integration in the PFN first level converting circuits to be incorporated and handle application programs from the host machines application specific activity controls and sensors. It will allow for standard connectables with special adapters and also provide for a control signal which is a modulated digital signal sent out on the power lead to individual activity controls, sensors, operator telemetry and to handle Audio and video digital signals.. The super modem 6A(UTU) is a universal transposing unit and will be able to handle analog to digital conversion, digital to analog conversion, all encoding, decoding and encryption processors either in it's firmware or in it's installed software running in the mini-computer section. This modem section can in the future be integrated directly into the communication devices and or combined with the mini-computer section or they might well all be integrated together in hardware and accompanied with the FACT main processor software (that is system or component failure sensitive with memory storage to confirm functional reliability and emergency power supply and charger circuit as one single protected and sealed protected PFN integrated circuit. If so this is still within the nature and scope of the invention and it's purpose.

Also fiber optics as was detailed in an earlier PCT patent application and may be used to carry control and monitoring signals. In this case the appropriate sensor and converter would be part of the super modem interface and any responsive peripheral circuitry.

In the Multi-Bus Comm Link there will be a universal antenna buss properly shielded grounded and or filtered to provide lower or no noise. Or this universal antenna will be run separately. Ultimately 6A PFN Core will incorporate 6A1 through 6A4 with memory storage 105 through 106 in one self contained protected containment and integrated circuit with a uni-bus internal interface connector link for any and all past present and future accessories desired.. 6A4 and 6A5 illustrate this present interface capability. It should be well understood through this figure that any consolidation and or combination of communication technology, computing, or controlling processors and memory storage that is used to monitor manage and control man and machine interaction and individual activities from a protected environment and provides accountability falls with in the nature and scope of this invention.

FIGURE 7

Depicts a security enclosure and in this case illustrates a nuclear scenario, which would require unique types of monitoring and remote control devices . This could be any security scenario for any installation with application specific requirements which would determine the specific peripherals with any variation of protected circuits. But with same purpose to. To monitor and control a restricted secure area with accountable remote control and or robotics from either a local, regional, and or a global monitoring network which is also maintained with secure communications.

700 is the gate into the secured or fenced in area with a PFN which will receive a signal from any vehicle \ equipment entering the restricted area. The signal will contain ESNVIN and/or SR numbers or any specific identification information for any vehicle and/or equipment being brought into the compound. Also any personal identification and or fingerprint and/or PIN verification will also be a requirement for any accompanying personnel. If the proper identification is authenticated for an authorized entry the PFN will activate any gate motors and permit entry , even in a un-manned setting if the environment is uninhabitable for humans or is part of a desired automated an or security protocol.

701 all the way up in the upper left hand corner of the figure shows a guard or observation tower that could also house the local computer monitoring and control terminal like the one represented in the drawing by the little picture of a man at a computer terminal 300L in the lower left hand corner. There is a dotted line that goes all the way around the entire compound which is a security fence and or any other access restrictive devices or barriers as indicated by number 705. All of these devices can be either linked or solely operational with long and or short range wireless communication technologies and or land lines if so desired and as has been maintained and detailed through out all the related patents. Just down from 701 is some trees just outside the perimeter fence and this is another PFN which can be application specifically designed to do a number of functions. To either control video surveillance systems, report on environmental impacts on the surrounding area of the compound, air, water, soil sensors for contaminants, toxins like radiation biological and chemical wastes. When these PFNs are not connected to a host piece of equipment that does not generate electricity or cannot be supplied a charging current for the emergency batteries the PFNs will utilize solar cells to maintain the power supply in adequate energy levels. This charging option has been described in related patents for automotive applications in remote areas where a vehicle has lost its power plant and the car storage battery is either discharged, disabled or removed. The PFN emergency battery would be recharged by solar cells aesthetically and stealthily placed on the top surfaces of a vehicle to retrieve solar energy and convert it to a charging current for the PFN to send out or transmit emergency signals. This same system would be utilized for the PFNs that are to report on the security environment where there is no standard means to re-energizing the PFN batteries. All PFNs are designed to have their own power supplies which is once again an added security feature.

702 shows either satellite reception and/or transmission capability from some security compounds and or government installations using high security DES and DET systems for direct satellite networking. These are special frequencies and if a necessity they would be the radio communication systems in the secure PFNs or they would use short range transceivers to the local monitoring gateway computer terminal and rely on a repeater function of the gateway to send the satellite the signal.

703 in the top middle of the drawing is a phone to indicate that the monitoring and remote control system is also hooked to land lines. These land lines in the high security

application will be D.E.T. Data Encryption Terminal in which chip sets will be in the gateway computer modem and or terminal hardwiring to send sensitive data encrypted and also on any computers networked with the it. Directly below are two PFNs one on any back up oil burning super heater or boiler for steam generation and the on the nuclear concrete steam generator and containment exhaust. These can be placed in areas that are difficult to access and rely on secure wireless communication and or be used as back up to any pre-existing sensing system already in place to monitor exhaust gasses, toxins and or pollutants. They can be used to activate vales as primary or secondary backups to hardware systems. And of course any hardwiring system would greatly benefit by the secure containment and multiple accountable data storage. The smoke stack applications for PFN monitoring are only suggested possibilities the PFNs can be structured and set up to monitor and control and functions , the equipment, personnel and environment.

704 shows a video camera that is part of the perimeter security or surveillance system and is either hardwired directly to the local gateway computer system and or controlled through the wires. Or it is reliant on wireless systems with the correct. level of a encryption technology (DES, PGP) to restrict any general access to the sensitive video images being broadcast from any interior secure areas in the installation or compound. 704 video camera can also be mobile as already described and claimed through out all the related patent applications. Most of the remote control mobile equipment will be outfitted with video cameras to keep accountable visual records on any and all remote and automated functions with the more sophisticated 2 way radio and cellular phone configurations in (fig 6) capable of reporting these encrypted signals back to at least one remote location thereby providing this same data to any network configuration if so desired. PFNs could be all that is needed for the controls of any electronic camera guidance control of servo motors and their relays and or any solid state electronic switch systems and or mini processors being utilized as the control circuit.; if the standard land line communication system and or main power was discontinued due to any difficulty or elevated expense in providing a particular camera in a specific location with these necessary component services to energize it and provide a communication path way. This could be done as a back up consideration or as the most optimum modality due to expense and environment. Once again these PFNs could rely on the same energy source that energizes the camera motors if they are hardwired or on their battery power packs

which will be recharged by camouflaged solar cells that would be application specific to the requirements of the PFN and camera demands for any electrical current or energy requirements per time of use scenario. This would determine the size of the storage batteries and the number of solar cell required to service any battery power pack and system use.

Directly below the camera is a chest or locker which represents a secure containment and or vault that will be housed in a underground pit or secure structure to store dangerous substances, e.g., radioactive products, by-products, and waste, Bio and medical products and waste, chemical products and waste, etc. There is around the locker a radioactive warning sign but their is also a bottle that is being used to represent the primary container for any of these toxic substances that would be stored in the special containment locker. The bottle could be medical, bio, chemical, and/or nuclear waste (As being developed by Westinghouse and others (theses special glass containers are to secure nuclear waste in storage.)

The beaker just above the box represents a sensor or set of sensors and in this case of either chemical and or bio sensor array with a PFN attached to it.. These application specific sensor arrays would be placed in the soil surrounding the containment and or positioned to sense the surrounding atmosphere and or submerged in any area ground water supplies, e.g., aquifer, lakes, streams, rivers, bays oceans, etc. They will be sensing devices and or device arrays capable of recognizing, delineating, discriminating and quantifying specific and different substances and the amount and or strength and or any concentration and or contamination and transduce this data into an electronic signal which then will or could be encrypted, generally modulated and transmitted over a PFNs communication frequencies and devices in the more sophisticated 2-way systems (figure 6, but also possible in (figure 5) the less sophisticated two way page protocols, e.g., REFLEX TM); and or merely stored in the data storage section of the simplest one way PFNs for physical retrieval by a person or another automated robotics mobile device with PFN control and the earlier mentioned connectable data extractor and extension coupling innovation and or interface for data transfer and retransmission to at least one remote gateway and any accompanying network system . Directly below the chest or vault is the equipment that would deliver the toxic substances and pick them up from their places of origin. Their is a PFN on the fork lift or any support equipment that would

be handling the hazardous materials from the transport trucks or rail cars or ships or planes. These pieces of equipment will have what ever sensor array that is application specific to complete their tasks appropriately. e.g Radiation sensor that can convert the amount of RADS present around a sensitive containment vessel or area. And convert this reading into an electrical signal (Transducer) so that the electrical signal will represent a level of RADS on the Rankin's scale that can be associated with safe levels, dangerous and harmful levels. These levels will of course be established by the appropriate government authorities e.g. Dept. Energy, EPA's National -----, -----,-----.

Special sensors Like the "NOSE" that can sniff, smell detect or identify substances 2000 times better than the human nose and its accompanying comparative software that discriminates at the molecular and the atomic level in some cases is an ideal application specific sensing tool to uncover explosives, biological toxins and dangerous chemical agents with as little or no human contact in high security installations around the world, and then to secure these dangerous substances and report around the world in a secure manner to organize and protect. safe environments and controls over much of the terrorist chaos without invading the normal citizens movements and maintaining professional courtesy and respect. for the individual while increasing security awareness for the real threats.

Of course all the metal detectors, phlorescopes, MRI'S and or x-ray scanner technologies can be employed and supported by the PFN proprietary computers and video cards as well as interface with any pre existing system to record and report and manage that kind of data if so desired in the manner in which has been described through out the entire group of related patents.

FIGURE 8

Illustrates the many varied high security purposes of the installation secure area system depicted in figure 7. It shows some of the governmental uses, and commercial applications for a secure installation , that are hazardous and can be enhanced by unmanned operational functions, e.g., oil, gas and chemical plants, medical waste and sewage facilities, nuclear substance use, and nuclear waste storage and a multitude of

other science , energy technologies as well as monetary processing either in hard currency or credit - debit data.

Figure 8 shows the same physical installation compound , but this could be any type of installation and employ any number of different type of physical barriers and electronic protection and monitoring devices and systems that can be part of any preexisting security system or controlled though all the varied PFNs in a networked system. 800 is a block of many of the high security government buildings structures installations and government agencies . e.g. military, political institutions, government branches and embassies. 801 represents financial and monetary operations and institutions, which can range from Fort Knox , the mint installations to banking operations armored vehicle tracking and travel path with time and place records in three places in real time along with real time audio, video monitoring of the entire operation. 803 is a satellite that could in some high security government protocols be solely operated by the military and have no commercial applications and or it could be a com sat or commercial and governmental capability with DES and PGP and even unrestricted general transmission capability. as was described in the number two formal patent application 112756-202 the world wide web can be utilized for the PGP encrypted security system and provide very good security of these PFN monitoring for phone , wireless and land line systems if the goal was to have a reasonably secure system very inexpensively. However most probably for any real high security and or restricted government protocols these will be isolated transmissions on DET Data encrypted terminals with DES data encrypted standard chips with physically isolated sides for sensitive and non restricted data in any transmission or transfer at any level . Either here on earth or in subspace through any satellites.

SECRET

At the very bottom is 802 and these installations can be operated by governments and or corporations and represent the chemical industry, medical field, fuel oil and gas industry and of course the nuclear industry as depicted by the figure 7. 300 w on the globe represents that the monitoring and remote control network can be set up locally regionally or sectional and world wide if so desired and have any and all capabilities to monitor and control as determined by the company wishes or security protocols necessary to properly protect the installation and its purpose as well as the would from any inherent dangers it possesses to the community.

The 700 figures have all been described and detailed in drawing seven as well as 300 L local monitoring and control station or gateway if networked from the local level., however any phone node that is capable of receiving and transmitting a conditioned PFN signal can act as a gate way to any desired network system combination . All that is required is that the proper encrypted hard ware and or firmware and or software be in place.

FIGURE 9

Is the first page of two pages listing the allocation of frequencies and naming what they are being used for these frequencies change from time to time but are being listed here to demonstrate that the invent can and always has been able to utilize any frequency receivers and transceivers in a PFN. However, as has always been maintained some digital and specifically those that are full video applications require enough band with or a conditioning of the digital signal through co-panding or compressing and decompressing through a chipset processor on both ends of the transmission in some case.

FIGURE 10

Is a second page showing with more frequency allocations and named purposes and descriptions.

FIGURE 11

Trusted Remote Activity Controller (TRAC)

First a review of TRAC operation and implementation which is the basis for the functional accountability of the invention, once again the :

OPERATION

The Trusted Remote Activity Controller provides all local vehicle or device control and event storage relative to PFN protected (Primary Focal Node) operation. It interfaces to an RF telemetry link, which may consist of a one or two way paging system. More sophisticated links could be used such as digital cellular or PCS (Personal Communication System). Typically, a Remote Management System (which may be as simple as a single page, or as complex as a controlling PC or Server) initiates a TRAC function, such as an automated slow, stop and secure sequence. The signal or paging command is received securely (via encryption) and decoded by the TRAC. Optionally, a local display or audio speaker may provide local status of the TRAC function being executed, with appropriate progress tones, voice queues or displays to provide a local operator feedback relative to the progress of the function. In performing the function, all Activity controls are initiated by the TRAC and monitored by the TRAC from start to finish. This is accomplished through feedback sensors. Feedback Sensors may be electrical, mechanical, fiber optic, infra red or other technologies. Since the function being performed requires a high level of accountability and trust that the sequence was in fact executed properly, every step of the process is monitored through appropriate feedback sensors to attain the reliability and trust required. This positive feedback in the TRAC is the key feature which distinguishes the TRAC from other electronic or software controllers; making it a fully "trusted" system for the task being accomplished. Additionally, all events and status relative to the function are recorded locally in the Local Event Storage Memory. This is termed the System Function Data. The level of redundancy in storage of System Function Data and the level of additional feedback and checking required in order to verify the Activity or function was accomplished properly, is directly related to verification requirements. These requirements may be regulated and approved by local or federal law, law enforcement or

CONFIDENTIAL

insurance agencies, World Bank, EPA, ICC, SEC or other regulatory agencies. Interim progress of the sequence, activity or function may be optionally transmitted back to the remote management system through a 2-way phone or paging link. This may occur as the function is executing or may be programmed to occur after completion of the sequence. In any event, local, redundant storage of the event is always contained within the PFN for subsequent or simultaneous retrieval of event information and proof for accountability purposes. The PFN enclosure and TRAC monitoring of tamper sensors guarantee the information has not been compromised. Other types of information along with the System Function Data may be stored in the TRAC Local Event Storage Memory. This auxiliary information may include digital or analog data not directly related to the function being monitored and executed, but important for evaluation and determination of liability, collection of evidence or environmental data. Examples of these include road condition information or surveillance audio and/or video.

IMPLEMENTATION

TRAC implementation may be accomplished in many ways, depending on space or funding constraints and level of integration required for the system. A PC-based system may be in the form of a desktop system, laptop or embedded system (PC 104) with a dedicated DOS or Windows based TRAC program, consisting of machine language, Basic, C, C++, Visual Basic, Visual C or C++, or other high level language which accomplishes the TRAC function through software control. Interfaces to the System Under Control (SUC) may be accomplished through appropriate I/O cards, either analog or digital. PC compatible Modems or Cell phone interfaces provide the interface to the Remote Management System (RMS). SUC and RMS interfaces may be in the form of ISA, PCI, PCMCIA, VME, Compact PCI, Future Buss, or other commercial interfaces compatible with the PC-based system used. More compact and custom implementations of the TRAC may consist of

dedicated state machine controller implementations in which TRAC functions are executed through embedded firmware. These implementations may incorporate multi-chip solutions using EPROM or EEPROM interfaced to Arithmetic Logic Units (ALU), I/O ports and discrete memory elements. They may also be microprocessor or microcomputer based. A large variety of board level products are commercially available for such an implementation. Single chip or high density implementations might consist of Field Programmable Gate Array (FPGA) or Application Specific Integrated Circuit (ASIC) based devices. These implementations may incorporate all sequencer, firmware, I/O and storage functions on a single device and would provide the highest level of integration and smallest size.

Display, Video and Audio (Auxiliary Data) for the TRAC can be in many forms and types. These may range from analog systems, in which tape or other magnetic media store the analog signal, to digital systems in which data is stored on hard disks, EEPROM or RAM. Data format may be modulated through FM or AM, compressed, packetized or otherwise encoded for reduced bandwidth or for transmission over the Internet (packet audio and video).

FIGURE 11 (detailing the other software programs running)

This figure of TRAC is a more detailed description of this technology's proprietary programs interfaced in the programmable and modular TRAC, for mobile management, commercial management, home management and the control security technology applications detailed throughout the related patent applications. In this drawing the cube labeled TRAC displays all these Application Specific Software programs (ASS). This software is programmable and modular. The TRAC software can be in the form of hardware with embedded software or firmware, or it can be modular software running in processors controllers and or computers.

The Software / Algorithms will accommodate Bank and stock exchange Transaction products, which will be supported by this technology's FTP Financial Transaction Program.

This program will do as much as possible to support run and route any C.O.T.S. products best suited to the owner of the host equipment and their choice of commercial servers, but eventually all programs will meet certain securities exchange and banking standards. This technology plans to utilize Commercial:128/64 bit Encryption for Web Transactions with the present proprietary software program to support and interface most of the secure commercial exchange products with all the pretty good protection PGP software C.O.T.S. products available today. This is labeled Commercial Encrypted for the Web. CEW. These transactions might be used for service billing for privately managed credit card account service companies ect. dealing with a specific clientele and their equipment. This system could provide inexpensive direct billing to personal and company E-mail addresses, rather than going through a large bank card programs with all their expensive costs. And the bank card companies would utilize the financial transaction products FTP product constructed to provide the adequate security protocols for a secure track able transaction record including identification for equipment and personnel, as well as, time date and location of any transaction. (Finger prints and pupil recognition hardware cameras and sensors, ect. would be employed along with the accompanying software algorithms to document and authorize as well as, authenticate any transaction. However, initially the key pad or any interfaced phone number pad will be utilized to provide personal identification numbers PIN numbers for the transactions)

FACT is the federally authorized control technology protocol and or standard. This program will take priority over all running programs on any PFN equipped piece of machinery equipment and or vehicle. It will be used by law enforcement and authorized government agencies for national security and public management and or crowd control in extreme cases such as, a declared state of marshal law. It will be a priority system over all host equipment functions including financial transactions to insure fair and stable pricing in providing necessities in a ravaged and or compromised area .The financial record can be reviewed later to determine any improprieties exploitation's, and or profiteering that occurred and is so prevalent in these kinds of circumstances.

CONFIDENTIAL

FACT will also be responsive to special reserved RF radio signals for police and official government access as well as be responsive to specific coded and encrypted messages sent and received on any frequencies. This is to allow immediate individual communication and control of a vehicle and immediate communication and control of all vehicles and equipment in an emergency. A standards committee will address the specific protocols for the utilization of this function and law, rules and regulations will spell out the guidelines. And with TRAC in a secure encasement with local memory and remote redundant memory at a triage level if not totally accommodated; accountability and analysis of any such event will be made easier and more instructive for any future events. FACT program will be accessible by the police, law enforcement, and or traffic enforcement system and police remote control command tools, that are capable of locally identifying a vehicle and controlling a shut down of that vehicle in the manner well detailed in the related applications for this technology's proprietary "spider eyes program" or for any smart car and or interactive highway programs. Of course law has to be legislated and rules and regulations made and well understood as to the manner of engagement and the procedures to use these devices and systems to preserve respect for the legal rights of the individual as public safety is being served and provided. The laws are clear and exist today. Only the rules governing the use of this technology have to reflect the true intent and provide accountable record for the law.

FACT will have varying degrees of security protocols all the way up to and including DES data encrypted standard at certain levels for any and all equipment if so determined necessary in the legislative process. And this technology provides for the use of such broad government management and control through a modular modality to be deployed physically in chips and or activated as pre programmed software in any processor, for special situations as authorized and agreed upon by the appropriate governing bodies for domestic civil situations and or world peace to insure fair treatment and management in these hostile situations.

FACT has been designed to be set up and governed by the United States democratic process as a master control standard for this technology's machine messaging network and to include the world wide web to comprise an MMN on the WWW. However when this system

is operated around the globe each stable nation state, would possess their own encrypted control code for national security and also have their own security protocols for any sensitive data processed by a PFN through TRAC software system and or communicated on the MMNWWW .

In hostile areas of civil unrest the same world organizations could address and mediate with any warring parties in the same manner they do today to negotiate a peace settlement . However with this technology any agreed upon accords or treaty measures could be written into software programs and downloaded into PFNs with this TRAC software to monitor and remotely control and or use robotics to referee the terms of any agreement. The PFN TRAC system can be installed and or activated in any and all equipment to help in the processes of nation building to insure fair exchange between the warring parties and to insure any aid efforts are guaranteed to be utilized in the fashion intended. Also the management and control systems can serve to better follow the actual behaviors of the agreed upon hostels with out interfering or intervening or introducing any other new groups (Troops, ect.) or societies directly into a localized conflict.

The PFN TRAC system can be given a progressive array of tools to help safe guard any agreed upon peace. This technology can give audio instructions in the appropriate language and repeat or site the agreed upon terms when they are violated. This accomplished by the monitoring of improprieties with the hostile parties and or persons. The technology will record incidents on location and in the remote monitoring and control center. It can then aggressively intervene from the authorized monitoring and control centers with varied levels of deterrents all the way up to full lethal weapon deployment and use. All these actions are tracked and stored in memory systems both on board the PFN and redundantly in a plurality of remote locations. Accessory deterrent systems

FACT, CEW, FTP, are all the primary programs that are a part of TRAC's secure communication links to any remote management and memory storage computer gateway or node that can network with any host machines ASS sub-programming modules. This primary programmable TRAC module software will prioritize communication from the comm. links as determined by the standardization efforts for accountable remote control as per application

specific protocols and real life social economic and environmental circumstances in real time. Local memory storage and time are both kept as part of the TRAC programmable Module as well as, the application specific programs for management and control of society and it's equipment.

The Mobile Management would have application specific programs for remote piloting of a vehicle. (RPV). And most especially this technology's proprietary PASSS program, which stands for proprietary automated slow, stop and secure the vehicle. And the secondary modality of the this proprietary automated shut down PAGSSS proprietary automated guide, slow stop and secure. This of course can in part be accomplished through remote control if so desired. M-ASMP stands for mobile application specific management program. This is any number of basic programs that are now completed by OEM PCMs that will be monitoring vehicle sensors and operating activity controls, as well as, accessory sensors and additional controlled devices made accountable through an interfaced TRAC equipped processor in a PFN. These standard mobile application specific programs will provide service data analytical and repair data, environmental testing and feed back of the equipment

Commercial Application Specific Management program C-ASMP is designed to provide specific service data and remote analysis functions, as well as, control any machinery or equipment from at least one remote location and or to shut it down for emergencies or in accordance with any financial arrangement. leasing , taxing, ect.. Also, monitored is any environmental data, or any application specific data like fuel or energy use or resource use water, air, ect. Some other general application specific areas for the commercial management areas are; industrial, agricultural and construction.

Home Management Program H-ASMP is another application specific set of programs that can offer home nursing telemetry for specific physical conditions

FIGURE 12

Figure 12 is an illustration showing the world and all the possible networking of systems that will make up this complete interactive data handling communication and control system , or create the monitoring network of the present invention the

(MMNWWW). Figure 2 shows satellites that surround the world and triangles denote commercial or private servers and government providers; the servers \ providers are gateway nodes in most cases to land based phone service for computer net works for the government agencies commercial service companies, and/or the WWW. (ps) means phone system hard wired; (lg) in a circle is local government; [E] in a square is the emergency response; the little man is a lost child or convict; and also depicted is a tractor, boat, plane, bulldozer, factory and a car.

The radio towers are, for example, cell phone, digital and/or pager towers, and/or RF systems and the capital of the US represents the national government and the stars are other national government around the world. The triangles are servers in other countries.

This figure is meant to present the simple view to establish the concept of a world wide monitoring system to link all forms of communication networks through the inventions PFN's to create the Machine Messaging Network the (MMN) which when it's data is presented on the WWW as informative accountable web pages completes this task. Society once again will have the means and knowledge to use this monitoring and record keeping system to control functions either indirectly or directly with remote control in real time. But this will and probably should be done with caution and consciousness.

The reason that this world monitoring and control system is feasible and not just some inventors dream is because it is based on smaller networks which are presently emerging and already perform meaningful public desired services by combining telecommunications and vehicles together. These are not at present true remote control, automated control or any real robotic set of systems for machinery. But most definitely the invention is what the future will need to make these emerging systems better for all society . It can provide for fair revenue practices and assessing at the same time through accounting for material use and waste products with the operation of all humanities equipment and technology. And without any doubt the timing is correct to create this type of accountability to better help humanity to manage it's technology economically and environmentally.

FIGURE 13

Figure 13 is a list of U.S. Government Agencies. And in fact it is actually a U.S. Federal Government Agency Directory prepared by LSU in a search engine format web page with hypertext and or mosaic or gopher software architecture so that the browser can click on any under lined department or agency and go directly to that specific departments home web page.

So obviously the agencies already exist and they are set up on to enter data on to the net through their own web pages. Many of these agencies already prepare data by regions if not states and local jurisdictions or geographical boundaries. Some even provide this data presently to universities ,corporations and or governments. for their research and knowledge as well as the general public. Most importantly the areas dealt with in this application as to watch dogging the environment is well saturated with governing agencies. Those dealing with the environmental, law enforcement and transportation as well as all taxing agencies and revenue mechanisms and government spending or disbursement of public funds for the local state and national levels are also available on the Web already. This makes the goal of setting up Web Account pages for local state and national very easy by maintaining a structure that will interface with the government agencies and financial markets supply it's information to this format. The purpose is to develop a public product for rapid awareness of one's physical and economical environment from the local to the national level to greater insure the wise use of technology investment and create a more politically interactive public that can voice its views economically and by public comment through electronic polling in the most efficient and clear way.

Some of the national environmental agencies that would supply data to the web account pages are on page 3 of figure 13 NESDIS,EIS,NCDC,NODC and the coordinating agency Office of satellite Data processing and distribution. Some more are NMFS,NOS,NWS. As well as the office of Global programs, The office of Oceanic and Meteorological Laboratory, Air resource lab, Climate Diagnostic Center, Forecast System Lab, geophysical Fluid Dynamics. Many of these would be coordinated By EPA and the data would be presented in clear accurate packets framed to current issues if appropriate, as well as, given as raw data hyper links that the individual can click back on and find the agency and person responsible for posting a specific data framed for a issue.

Along with posting data to the web page many of these agencies would be gathering data from all the PFN's through either their area local phone nodes or networked commercial servers that transferred data to their local nodes .The agencies would then share it and store it and post it on the web account pages. They would be retrieving this data was mentioned earlier from their regional phone nodes and or commercial servers that would be passing this data on to them automatically through special software structured by these agencies. It would therefore be a requirement of any commercial server or any provider that acted as a gateway to any government data management for a agency that they be running the agency approved software to be licensed operator Commercial servers e.g. cell phone service, ect.

On page 18 of the Directory listed half way down the page the Federal Department Of Transportation has all it's divisions listed and of course these too would be responsible for the gathering of Data in their traditional way as well as through the inventions (PFN) data transmissions, especially in the interactive highway systems for all vehicles.

However, all agencies record their activities geographically but some don't report their issues and/or activities to the local level and the public is forced to track down this information. Ideally with the local state and national public account web pages on the web, these regional agencies can post local data and issues they have collected and are working on as they prepare their data for reports to the regional or state as well as, national level through hyper-links during the gathering and preparation state through basic programming with any sensitive data restrained. Because, there may be a need to pass some of this information through a security protocol program first and then post the data in a clear straight forward manner for the public with FAQ's.

Other areas to retrieve data from the PFN and post data to the Web account pages will be The Department of energy, and all their projects and programs starting on page 9 of this register, ultimately all agencies in their mass data management and storage programs would structure there software to support their representation on the web account pages so they can account to the public for their existence and their activities. And of course the Justice Department starting on page 15 along with all the earlier mentioned FBI programs in related patents incorporated herein by reference would be an important part of this technology's proprietary spider eyes program in reporting criminal incidences that are under investigation so that the general public can

also help locally and nationally in the process to jointly police our society to provide a more democratic policing process.

These would be posted locally as described in earlier patent application incorporated herein by reference for the San Antonio Police Department, etc. as well as supplied direct FBI regional and national Data for all 4 levels of the web account page) And of course this is a main objective in providing these web account pages to the general public. If the individual is going to be ask to share some of their rights of personal privacy, but intern will be treated with personal, respect, discretion and full accountability for any and all levels of indiscretion respectively. Both criminally and civilly. These are the proper ingredients necessary to advance these present data acquisition technologies to improve public safety, national security and the individuals free and secure lifestyle with a healthy respect for privacy and thereby help to delineate social paranoia from real fear of social control of an individuals life or cost of life. The PFN accountability can keep a fair environment for all and all must relate their data to their source in any inquiry or lose their claim or position.

A better, safer and more informed society with fair play to insure all have as much freedom and security as legally possible with gathered information and for all gathered information the PFN TRAC/FACT system can insure this life condition, but it takes all of us to make these practices constitutional and proper and it takes all of us to maintain this machine messaging network and all information technology in this manner.

This sharing of data can more easily be achieved through the advances in fiber optic land lines and internet routing systems like those developed by Cisco Systems and Cerent Industries for data systems and the Internet. For this reason these government agency and their systems can be capable of much more management functions of their mass data and can support the Public web pages and other local government hyper-links to maximize the presentation of critical real-time data to the appropriate people in the shortest time with very little increased labor effort after the original programming. The next figure will detail out the PFN uses and illustrate how this machine messaging network (MMN)+(WWW) can function with our present information technologies and

CONFIDENTIAL

add greater control and management to our equipment use and environment resource use.

FIGURE 14

Figure 14 is the entire inventions control system from the Primary Focal Node and Trusted Remote Activity Controller on every piece of equipment to all monitoring, accounting processes and or control and management systems from public government and every agency and commercial interest desired to the general accountable presentation of this Data to the public in general via local state and national accountable Web pages. This is the PFN.\TRAC\MMN.WWW providing general data as a social economic and environmental technology accounting system for Democratic Governments through a responsible free enterprise and free communications system with all the security controls necessary to provide accountable remote and automated services world wide and monitored by everyone for general knowledge and data.

At the very top of the page is a group of ten icons symbolizing where the PFN's would be utilized. These few representative icons are by no means to be interpreted as the only places that PFN's will be utilized. They are intended to be used in some form on all pieces of equipment and or placed any where it is determined their needs to be monitoring for public safety, trust and national security after meeting any necessary legal and constitutional requirements for their installation.

PFN's can have more than one purpose e.g. they can be used to bill (through CEW applications) for commercial service or for specific service of a machine and simultaneously be gathering data on any incident or accident event or provide additional controls by off board control and or management systems in an emergency or in the case of a compromised operator in real-time. In fact, with the development of this PFN machine messaging network into vehicles and equipment it can provide responsible good governance and organize all machine systems in an accountable manner to insure that any abuse or miss use of these automated systems are accounted for and available to the individual citizen for public protection and retribution. Data on individuals will always be secluded and at least one step away from public review. If any individual data resulted in legal review for liability or criminal activity it would be handled in the same manner as evidence is handled today through the proper authorities and representative lawyers with the protected PFN evidence equally presented to both conflicting parties

CONFIDENTIAL

during the discovery process prior to any civil legal proceedings. Of course this is a section and set of procedures that will be appropriately legislated for the PFN by dually elected government bodies in a constitutional manner .

The icons from the top left are trees with a (PFN) box to monitor the environment, weather, air pollution, etc., either sensors or video camera or any number or types of sensing devices will provide electrical signals to the in house PFN computer or processor, which will in turn provide discernible data via varied forms of wired and or wireless communication to either a commercial server if contractually employed by the PFN owners or to a phone node gateway to the appropriate government agencies and then on as area prepared data to regional or local web sites for the public to review (General public, educational and research institutions, commerce and industry, and all levels of government, ect.. This box is given a zigzag line to indicate a wireless transmission in a remote area but just as easily could be hard wired if available. Once again some of these monitoring devices are in existence presently, so the invention will add communication, local memory and many other assets to them if they do not have them and return their data in real time to the agencies for processing that are to govern them and any private or commercial operators that are licensed and contracted to monitor and operate this equipment and accompanying software. If these are self policing operations by commercial interests they can be given a tax rebate and assistance in their problem areas in recognizing their genuine cost of doing business in real time, but they must be licensed and adhere to any and all legal rules regulations and or laws governing the use and handling of data as it is categorize. These governing agencies can then pass the data on to mass data management for individual alert postings that can be cross referenced for closer observations and correlation's .This would be accomplished by earmarking this gathered data by the specializing agency as identified as a possible or high co-related area of interest and or impact to other known fields of study looking for this kind of mass data input. This may be accomplished as easy as an automated E-mail and or redundant internet CC command or be part of a sophisticated mass data management and storage facility capable of handling and processing all types of query's and or it maybe a combination of both employing hyperlinks from agency commercial organizational, educational and even individual web pages. This general data will allow the public to review data and read individual findings and even arrive at their own conclusions with all the data and tolls available. The local PFN will provide the first

stage of accountability for the acquisition and distribution of data and the performance of local activity controls and system management.

Any posting or CC-ing from mass storage or data management be they private, public or government agencies under the design of this invention will require total accountability for substance issuance and or any authorization by responsible party's acceptance and records of activity and use on demand to complete total accountability for any acquired data. This data will be gathered in real-time processed and presented in as close to real-time to all if it is not sensitive (containing personal data or national security data or monitored for public safety and proper policing procedures) So, any proper storage, management and or delivery of data will be determined by the appropriate governing agency and their demands in software for their authorized and or licensed commercial contractors, or for their phone node gateways or any other government agencies listed or individuals listed or known to handle any same-such data. The PFN's software will be configured to retrieve the data in an easy to handle format to simplify this process. Part of the accounting system is to be able to support this mass data acquisition system with out breaking anyone group, e.g.. the individual, the governments, and or any commercial enterprises. So to be fair and because every action is electronically traceable in the message headers if anyone's vehicle or equipment is used to capture video for the publics business they can be credited for those services and if a news or commercial enterprise wishes to use or tap into their systems to show, e.g., a traffic tie-up then they must pay the owner of the vehicle or not use the data gathered unless the owner complies with a request. The owner would be notified if their system was being asked to use its data link or sensors for any commercial request or the owner could call in and offer location viewing to the news agencies. This provides real-time news and insures accurate pay for the advancement of this extraordinarily large monitoring system to all the individuals that will support and provide it.

The next icon up on the left is a generating plant and it shows a direct black line going to the commercial server's semi circle. This is a land line phone link and also a squiggly line is present to indicate a wireless transmission if needed as a back up or for a more cost effective modality, etc. The invention could list here all the standards for air quality for SO2 point source standards, particle point source standards, NOx point source standards, all the green house gas CO₂, etc. However, there are government agencies and private watchdog groups already involved in monitoring this and they have

CONFIDENTIAL

established standards which can be used as a starting point. The invention will house all the appropriate sensor arrays to detect these toxins or most probably just utilize the "Nose recently sent into space by NASA . This sensing device can detect odors so insignificant that they are microscopic in origin and minuscule in volume. With the nose attached to the PFN computers running the nose software identification library files either locally or downloaded on an automated request or provided to all government agencies to insure real-time compliance for safe and lawful substances and or matter handling providing real-time reporting of any violation in real-time to increase the proper response by the appropriate personnel and equipment in the most expedient time frame to insure public safety, national security and provide the most latitude for truly free and safe individual activities movements and freedom in the safest manner. These PFNs or industry provided units would report to the general public on a local web page and also regionally and also nationally so the public can respond knowledgeably to the information gathered and presented. Commercial Governmental, Educational and even individual citizens can respond and post discussion for hyper link and text spots on the web pages for review by all.

Many data acquisition systems exist today and they are not accountable at all and the systems are basically unregulated. Though the PFN/TRAC system structure accountability will always be provide for the use of the system with base anonymous individual data query and action unless it embarks on the rest of society's critical data. and or use. All of which(excluding personal identification data) will be available and prepared for the web on public account pages. This will let society help in the governance process of it's private , commercial and governmental decisions with out looking at anyone individuals particular conditions.(unless as apart of free speech that individual wants public recognition for any particular political reason) (self choice)

The next piece of equipment is a bulldozer and most of the time there is a limited amount of construction equipment but because they are forced to work in dusty environments and therefore are incredibly susceptible to clogged air systems which causes an increase in rich unused fuel being partially burned that deliver a great deal of pollutants into the air. Farm equipment as well, is inherently a dusty environment and also these pieces of equipment are in many cases working with food products and should be monitored for toxic fluid loss as well as any storage tank facilities for fuel pesticides and or concentrated fertilizers. Both construction and agriculture equipment will be

serviced in the most part by wireless -pagers with small short range fm transceivers and processors as described earlier. The RF transceiver is for networking all monitored farm equipment to one land line, transceiver where ever possible and the pagers will be used for inexpensive longer transmissions, also this will provide for the repeater function of a short range signal to a long range transmission or telephone communication line, e.g., people locator (Child find) (another proprietary device of this invention). With every land based line so outfitted with a transceiver an emergency network could be developed making every land line part of the repeater net system coupled to all vehicle PFN's. The short range transmitter would have the same one tuning crystal the same as the (tot spot) system mentioned earlier (other related patent application) this would be a specially dedicated frequency by the F.C.C. (possible from one in figure 9 or 10. Also figure 13 has 26 pages of all the government web pages already existing and these web pages would be hyper-linked from the local state and federal web pages addressing data in the order of the hyper link and interest.

Also other crucial Agricultural Data gathered can be sent immediately to the government agencies to monitor and advise the farming area. some GPS systems are employed by Archer Daniel Midland (ADM) for the governing of irrigation and crop monitoring from satellite systems. Along with the equipment and ground monitoring these systems could be interfaced and updated to return accurate crop data back to the government and to send aid and services to help a farmer or farming district in trouble due to weather or blight ect. When this was done the farmer could be given a tax break with respect to crop investment and loss. Also if the data gathered in a specific area was used for public use or commercial use the farmer could be reimbursed for the access to their electronic gathered data. For example speculators and investors in the market could best figure what to invest in .

The next icon is a factory and depending on how many pieces of equipment and the proximity they are to land lines these pieces of PFN equipment may also only have a short range radio transceiver that is in communication with a secondary node with in the company (land based line)and reports directly to a company control system in which these machines are monitored and recorded for their operations, but can also be provided instructions from plant management directly to their operators or are operated with robotics without operators. This in house PFN TRAC network system could provide a data link for service contractors and show a history of operational readings which when

run through their software diagnostic programs and or those programs owned by the factory would limit the repair choices and suggest the materials needed to effect an appropriate repair prior to arriving on the job. This would be a great time saver and money saver. Also personal calls could be routed to the operator without them having to leave their machine or work station to answer them.

In the material handling industry many robotic order picking systems already exist and converting them to collect emissions data toxic fluid loss as well as gather performance data and perform more and greater tasks would be relatively easy. As well as, store the data either on board each PFN or (in existing converted remote control systems) which would be able to store data either on board the machine or in the secondary company node or the commercial service company or any government monitoring agency or any or all of the above.

12 O'clock on the drawing there are icons for a boat and a car. The boat would have sensors on all toxic fluids and in the bilge to determine if the fluid had been passed back into the environment or to catch it before it was if deemed safe and possible . Having the PFN on board would be a great way to increase safety and to know navigation location at all times. In areas where cell phones and beepers were unable to communicate either a satellite or global digital phones might serve as a replacement. And also marine band radios would be used. And in this case the radio receiver station for the coast guard would receive a data link transmission along with any voice transmissions Data signals would provide the boats ESN and or full registry and a full report as to it's mechanical condition along with any SOS broadcast automatically sent or initiated by the boat occupants or automated equipment.

The car icon is very well described in this whole application and is used to describe most all the PFN's properties and qualities in all the other industries.

This is also true for the trucking industry the next icon at 1 O'clock. However, just a moment will be taken to point out that the intense concern for air pollution due to the trucking industry Commonly referred to as the colors of smoke blue, black and white. These smokes could be monitored in real time as well as the charging and paying of all fuel taxes and highway tolls. This could be paid electronically without creating toll plazas and the traffic tie-ups that accompany them. merely have a standard signal sent out by the highway computer that requested every vehicle via short range transceiver to broadcast its ID ESNVIN back or to call it in on a cellular highway node

system. The ESNVIN would also have a special tariff smart card number already swiped into the cars PFN which was bought earlier. This national card only pays for tolls and gas or use tax or commercial cards can be used when they are accompanied by encrypted transmission and reception for security. And, of course, for the interactive highways or any smart cars to be a reality for society they will need to process all their remote control instructions through a secure PFN that can record and account for all the robotic actions for any legal decision involving a driver accountability and an automated systems liability. Trucks will be provided with sensors on their tire pressure that will translate into axle weights and only drive through check for accuracy scales will be in place to check this equipment by contacting the PFN and receiving the PFN\TRAC for trucks data on each individual truck. Any tolls or charges will be automatically accessed and billed to the correct E-mail address or paid in real-time through credit card or debit accounts. The truck however will not release the brakes on the trailer if the weights are over the legal safe limit at the time of loading. A warning sound will be sent while the truck and trailer are still at the loading dock. This is only one's safety check for commercial trucking but all vehicle will be self monitoring the physical conditions of the mechanical components and give adequate warning to the operators before shutting the vehicle down in a stationary position or in real-time if deemed necessary either automated and or by remote control through this inventions PASSS and PAGASSS software programs and remote control activators detailed in the third formal patent and incorporated herein by reference.

The railway trains and subways, etc. already have many monitoring systems or networks. These systems would be tied into the all inclusive network system to account for energy use and environmental impact as well as monitor manage and control all surface and air transportation the specific local regional and national controllers. With PFNs on every piece of mobile equipment the exact location condition and possible collisions and or impacts can be accessed and the appropriate real-time warnings and help can be provided as well as maintain the most accurate record of the entire event if need be. So trains and even planes might carry these PFN systems in addition to the systems they now employ to provide more services or they will use them as a back up to all these systems (failsafe). The PFNs will be universalized and only be specific as to the jobs they perform. At 2.30 on the drawing there is a picture of an airplane with a radio signal from the plane and a land line signal to the tower. Here pertinent data from the

CONFIDENTIAL

plane could be logged into the MMN from the traditional FAA black box set up to down load on landings and during service or this data could be downloaded as is discussed in servicing equipment in the third application for the automobile. The tower and or airport facility is normally well endowed with environmental and weather sensing equipment and all this data would be also segmented by agency protocols and CC for the proper mass storage and also presented in the public account web pages. Also at 8 o'clock on the MMNWWW local node gate way protocol is a icon for the interactive high way and in most cases this will act as a primary local node to down load any PFN data that is standing ready for data transfer in the PFN Buffer an has been CC to it's PFN's unit storage. (either a commercial licensed carrier or government DOT or High way Safety government agency supported phone nodes gateways to area vehicle controllers via the TRAC/FACT software and any number of communication mediums .

There are in the upper portion of the page, eight concentric semicircles, which are layered protocols established by government standards for the data acquisition into their systems for processing. Their could easily be added more layers and most definitely will, but these eight will suffice to demonstrate how the system will process the data.

The first ring is the commercial communication server and MMN gateway via Land line systems . More and more in the future standard phone systems are going to have faster switching and for any one to operate a commercial node they must have all their phone support lines be Asymmetric Digital Subscriber Lines (ADSL) at least. The second ring in and the first ring provides any emergency service if the PFN did not call or was not able to reach an emergency service phone node for some reason . In this case the commercial server will maintain any and all contact e.g. voice and data links till the customer is served or connected to the emergency personnel, otherwise the second ring can provide any number of services from making web connections to down loading entertainment packages for the board driver. The next three smaller circles are for energy accounting and environment, transportation and traffic, and the criminal incident based reporting system.

It is important to remember in all these systems used in the MMN for the most part they are two way capable in communication and definitely all those used in the spider eyes program are two way. This means in the protocol for reporting crime all reports will be time and geographic stamped and will be reported in real time if certain

COPYRIGHT © 2000

software is triggered in a PFN or local law enforcement will be able to remotely activate any number of vehicles or PFN's they have recent reports from or any that are in use and giving out a signal to a local cell so that law enforcement can activate cameras and appraise an area in which they have just received an incident reported. Of course all these protocols have to be approved by the public and decide on how the billing will be assigned and credited and the priority of use in real-time. Many of the PFNs will be driving camera and video systems and these operating systems could be programmed to respond to a specially coded TRAC/FACT command from area law enforcement to provide the spider eyes service in real-time if they were not already involved in a crucial service (e.g. remotely guiding a moving vehicle). These PFNTRAC/FACT systems could be activated on a piece of equipment not being used. However a driver notification would be given to the operator on start up to provide on location accountability records and they could be reimbursed for that service as a credit for their next vehicle registration.

The voting node will allow for the public to vote on the road or in the home with their special pin Id, fingerprint verification. Originally configured to respond to issues as they drive home to let their representatives know how they feel on the issues that are at hand and proposed for input on the four web pages and or hyper-linked to the appropriate representative. They can view the issues ect. in their cars on LCD screens or see by hologram wind shields, and hear data delivered by voice. (Not Radio) This system would be developed to sanction a vote with a positive finger print ID and or an accompanying pin code. Also a driver could send a voice mail that converts to a written message to address an issue on, e.g., area roads and specific conditions time and geographically automatically encoded.

The two inner circles will be a continual running account of commercial and public cost and gains so an area can judge how well it is doing and also to determine where best to invest or create its finances and use its resources. This data would primarily be gathered over land lines and this accounting system could be used to make cases commercially to communities to lower taxes or provide support aid in a lean time or help to retrain workers in an eventual lay off. This is not the way business is done to day but it should and could provide a better way of life without stress for all in the future. Business would learn it's local community can help guarantee its survival even if it has to change the way it is doing business. Also in this function retraining programs

from the government and state and local educational extension programs can be offered through auto-tutor programs being developed by Cisco Systems so that every PFN can either be a educational node to learn current job skills or be a way to pre pare an employee for new tasks or employment do to the down sizing of a current labor market. This would prove to be an efficient way to use labor and supported partially by government would be welcome for any and all commercial interests to update their equipment and facilities as well as their personnel.

The inner center of the top semi circle is local government and all the way down through the center of the drawing is government with three pegs interlocking the local government the state government and the national government with the local account web pages that are displayed as local, state, national and international web pages. The pegs have letters in them and they spell out REPS for representative or the elected officials. With the public and commerce much more interactive with government at all three levels; all officials in all three levels of government will have to become much more interactive on all the issues and their perspectives and this is why reps is spelled out interlocking the levels of government as another medium by which decisions will be condensed and justified to the public. Basically the objective here is to integrate the process of individual power and responsibility for any one representative to be directly responsible to the empowerment structure held by the public's individuals.

At 3 O'clock in the center is the state government and below that the national government which are inter locked with the mass data management and storage network. To the left side of the system is data input for the state and the federal government. All the eight semicircles feed data that is presented to all citizens in the same manner unless security protocols have dictated a different path. The two inner circles provide in real-time the financial cost and gains and representatives and citizens can view this information and the representatives can make policy on taxing or crediting back or providing aid and the rest of the public will have the opportunity to completely see this transaction and voice there opinion in real time.

In between each section of government is an accounting process all the way to the federal banking commission. All the data is accounted for so that the financial and economical controls can be better balanced to meet the needs to provide for its society while stimulating growth.

The lower section semi circle is the delivery of data to the web account pages with government numbers on money spent and received locally, in the state, and nationally, Stock reports and financial reports on the local commercial companies, the regional companies and corporations, and the national and world stock markets.

60176818 . 01.1900

In the bottom semicircle there are four web account pages that anyone can access from commercial servers communication data links, the world wide web or mass media. Most all of these support response back systems even cable TV with a web box, although there is still a lot of problems getting service to all citizens so access could would and should be provided at any responsive PFN that supports a video display. And in public places as well like police departments and libraries. The four web pages would list issues plainly for the public to view and respond to. And their would be a section to frame issues in which the public could start a question. Also there would be a Yeah and Nay section on issues that were up for a representative vote. Also, there would be data given on the environment, the highway systems, the recent crime and much more vital information. This would be determined by the issues and events that were current first and then anyone, who wished to have data to explore their theories, e.g., on global warming would have it at their finger tips all the data and expert opinion as well as an auto tutor to learn understand and relate their informed opinion back to the rest of the world.

The figures from left to right at the bottom of the page are agriculture being remotely controlled. The highway systems being monitored and ultimately remotely controlled, The car is receiving remote service and the house being monitored and for it's energy use, all kinds of home management including in home automated nursing to reduce health care cost for the growing elderly and to allow them more liberty freedom and self reliance. PFNs will perform physical telemetry and even administer automated medications through the protected primary focal node and accountable monitoring system that will allow remote and automated medical care under safe inexpensive and more secure delivery systems.

The computer with it's a web access will be able to view all the web pages and act as another terminal to the web pages as usual, but will be provided all the automated PFN data as well. The TV at 6 o'clock is mass media with a web response box as another means to have contact with the Internet and all the PFN/TRAC data and to also respond to and cast opinions and votes in the future. With a PFN ?TRAC/FACT factory all activities can be reviewed privately and all that is displayed on the Internet all that is

open to public comment regarding the public's opinion and government policy will be totally accessible . Even the world could receive all the data from every where and all the world populous can see how the planet and any other humans are faring around the world. But for this to take place all the national governments agencies must clear the data to be freely posted. Some of this can be accomplished rapidly but corporate law , national security will have to continually participate in this process . And of course some data will just be considered to sensitive. The TRAC/FACT programs will allow the national registry to check any and all operating hardware and PFNs located in high security rated areas will report their data encrypted and or on separate terminals if need be. However, in the spirit of the Internet being an open area to exchange ideas and better ways of improving life and understanding these PFNs TRAC/FACT data input can increase the efficiency and proficiency of how people can do their government business, commercial business, and their personal business

FIGURE 14A and B

These two figures are composites tables taken from the Internet of the ISO-OSI models to illustrate the many and varied accessible interconnections for the PFN MMN. on the WWW .They are being used to show how to develop a secure individual and independent level seven FACT communication through the IP transparent com-links for increased National Security with the Invention (PFN). This application will discuss a inter communicative level seven to each application specific protocol with the final (A keys agency specific at a level 8 security involving all the constitutional check and balances, insured by PFN and remote Accountable memories available for review through the freedom of information act and or all necessary protocols . This will provide automated watch dogging of machine activities . As discussed through out all the patent applications the checks and balances will be legislated and the software written to laws rules or regulations for each branch of governance and for PUBLIC approval and or AUTHORIZATION in the -U.S.

Once again drawings 14A &B are two pages of charts and descriptions that were taken off the Internet detailing The International Standards Organization or (ISO) Reference Model. And with a basic discussion in reference to the Open System Interconnection or the (OSI) of networking including the seven levels to creating net

work communications between computers. This ISO reference model was created back in 1980 by the organization to create a standard for computer networking and the Internet. This Open System Interconnection is the actual standardized protocols that people use to communicate with computers. Because there was so much proprietary software in each computer manufacturer, the ISO developed a seven layer model which would provide a common basis for the development of standards that would allow different systems of communication to be connected.

This standard will be applied to the invention as well in all the present ways for transporting data. The PFN as a machine messaging system of communication will seek to universalize at the application level (level 7) encrypted technology that can be individually personalized and accessed by secured random synchronized encryption through the TRAC software programs and more specifically the FACT and or CEW sub programs that can run many of the existing COTS software products, which are encrypted and at the application level on both ends of a communication data exchange already. There are many security hardware, embedded software or firmware and software encryption products on the market today and many very good products. The invention does not seek to compete or develop any such new application products in level seven for any product manufacturers that can achieve what the invention prescribes as a level of acceptable performance for accountable aggressive remote and automated control of equipment vehicles and machines hosting a PFN and communicating to a national registry for ultimate accountability management and control. However, there needs to be a standard set just for this application level of activity where automation and remote control or shared management and control with local operators of a host machine can be accessible to the registry control apparatus for vital control and management functions to insure greater public safety and national security by the appropriate authorities. As one possible modality to achieve this unified access to level seven proprietary application systems might be to create an additional level. An 8th level in the OSI protocol stack

where coded access entries are provided by a manufacturers software and securely chosen by the National registry and governing authorities to be assigned and changed through random timed code selections on a synchronized clock system which also requires authorized pin codes to reset these access keys. This technology exists e.g Systems Link "Delivery Key "and can be applied to the PFN/TRAC/FACT registry and part of any sub programs like the commercial Off The Shelf bank card and payment industry applications NCR, ect. to be Run in TRAC/CEW applications or FACT for criminal activity. The review of commercial Encrypted Web products for the payment industry should run automatically through the registry if they are flagged for fraud and illegal use anyway at the application level both in the PFN/TRAC system and from the bank card supplier or supplier of the payment industry software e.g NCR ect.. .

Recently in the telecommunication field The National Security Agency and President Clinton pushed hard for a chip with federal encryption called the "Clipper" chip in all cellular phones so tapping cell phone for the government was as easy as wire taps.

This technology ran into much conflict from the ACLU, and the fact that a physical hardware chip could be replaced with a bogus or criminally constructed one or the firmware could be re burnt in the chip with some other Electronic Serial Number (ESN) and or Mobile Identification Number(MIN). These points are all well taken and prove the draw backs to the hardware chip like "Clipper", however this invention still claims all forms of programmable modular software as FACT capable if the manufactures meet the standards.

Another governmental effort has been to force the wireless phone manufacturers and commercial servers to develop the technology to pin point a cellular phone unit's location as is possible with land lines and physical addresses. This technology is already in place and offers the PFN/TRAC system another modality to tracking of a mobile units by cellular tower triangulation which will ultimately run software algorithms with GPS

technology NEMA to perform more accurate automated and remote control activities as well as pinpoint device locations for fee for use and impact on specific geographic locations, handled through area traffic controllers and the registry access for detailed information. And CEW access for proper billing and taxing a specific PFN/ESN vehicle in travel

The most important point being that FACT software has to be part of any level seven application or separately created communicative 8th level unified security protocol established in any device and or component or piece of equipment that is going to be responsible for PFN/TRAC/FACT/CEW control and management functions no matter what other applications are cohabiting any transmission. Both in the PFN and received in the remote location. Accountability for broadcast and use of all data is the key to making FACT a reality in this democracy. As stated throughout this invention all data collected must be performed to management protocols that follow the Constitution. For example, all Government agencies will be able to access the PFN/TRAC system through their own encrypted codes via the registry's controls to access data to freeze data and or to retrieve data as part of the National Registry detailed in later figures. However, the first two purposes access data or freeze data will notify the operator in a local display and voice message and asks for consent (as well as notify an absent owner if listed in PFN/TRAC/FACT inf. header) and or the second scenario will allow for control by public safety officials which still notifies the driver through voice and display and takes aggressive control of the host equipment and is capable of placing a freeze on local records and memory with a PASSS program or PAGASS program. At this point legal constitutional procedures must be followed for the people, equipment and the handling of any records both locally and remotely (e.g. Discovery laws , Miranda Rights , etc.)

The third control level is with no notification to the driver or owner and can only take place through a judicial order or Executive? order that is not obtainable normally through the FACT Registry program alone Most likely over seen by the Justice

Departments FBI. This Judicial order is obtained by a second random time clock of identity pin numbers and it creates three memories two in remote locations to all obtained data. The first locally with the standard PFN/TRAC two levels of memory (unless deemed not wise by the proper authorized agency) the second at the proper requesting authority's surveillance location and the other remote location under the supervising Judge issuing the tap and control and invading order on an individual's rights to privacy .

This is how the technology can work. However, the laws, rules regulations all require a joint effort to construct the right protection for those using this technology in these manners, both for the good responsible and professional civil servant and for any and all good citizens, and or criminal's exposed for their illegal acts and behaviors. Also, this process should include a respectful procedure with the unknowing individual citizen and an official representative of the authorized investigating organization and judicial branch in a private conference to return all gathered data anywhere to the individual. Or with lawyers present e.g for proper motions concerning evidence.(Evidence Discovery LAWs) for those allegedly involved in a crime. Upon the completion of a surveillance the suspect citizen will be called in and given all records and data obtained during the court order from both the policing authorities and the Judicial second data storage. Protection under the law for the Policing and judicial authorities should provide with no tort recourse by the citizen unless the data was improperly handled and that any personal injury was incurred . There should be no existing copies once the citizen has been returned their data and the data should be destroyed. (this is of course only a hypothetical protocol. And legislation would have to be drafted to be constitutional and fair to all parties involved. Of course the software programs would be structured to insure this legal structure and at this time it would be easy for anyone skilled in the art of programming to first construct a flow chart like the ones in figure 20 and 21 detailing simple software in the PFNFACT operation and in the main Registry. From here any programmer for any manufacturer can right the application specific commands for level seven access to their

systems and the appropriate preprogrammed responses of their components and devices interfaced in the PFN

FIGURE 15

PFN/TRAC/FACT/ESN Operation

Basic to the concept of operations of the TRAC and PFN, is a unique Electronic Serial Number or ESN, which may be either installed by a device manufacturer, or programmed at the point of sale for every component, device or subsystem within the accountability matrix (Local PFN). The ESN allows each element within the matrix to be securely and accurately tracked, inventoried or controlled, either through a local control loop or remotely, by an authorized application or agency. An example of a remote application might be local law enforcement personnel disabling a vehicle being chased by police officers. In many ESN applications, proper security measures would obviously need to be taken to prevent replication or copying of device or system ESNs for the purposes of fraud, unauthorized control or interception of data, or other criminal or terrorist activity. The FACT ESNs would also be the basis for digital encryption of information passed between the PFN device and the controlling entity (A National Registry) with local network processing nodes through public communications channels such as the phone lines or Internet initiated in many cases wirelessly from mobile PFNs accompanied by their Mobile Identification Number(MIN). This technology is nearly equivalent to that used in today's wireless systems and will incorporate many of the COTS encrypted security systems at the application level. Therefore it will require little research and development to implement; only modification of currently used commercial technology is needed to expand these applications of ESN/encryption technology to other areas (components, devices, equipment) interfaced through the PFNs. The adoption of standards that allow multiple vendors to inter operate is of primary importance and should be pursued in appropriate standards organizations such as the American National

Standards Institute (ANSI), International Standards Organization (ISO) or others such as the Institute for Electrical and Electronics Engineers (IEEE) Electronic Industry Association (EIA) and Consumer Electronics Manufacture Association (CEMA). As well as all the industry specific manufacturers and their associations e.g. for Automobiles.

The importance of security in these systems cannot be under emphasized. While communications privacy within the PFN matrix is a concern, it pales beside the threat of spoofing of such systems. This has been a great concern in the Cellular phone industry where spoofing (also known as cloning) is the process where a person provides false identification [about a cellular account] to the cellular communications provider with the intent to defraud. PFN systems requiring the highest degree of security would include transaction based systems; that is those systems which charge fees, perform billing or taxing functions or otherwise redistribute or charge funds.

NEW FACT CHIP

General purpose possible modality to prove feasibility

Component FACT chips are a micro-controller chip and or smart chip that is integrated and or interfaced with a silicon switching relay in every power regulating circuit or send the necessary data signal for any and every electronically controlled piece of equipment, devices and or commercially available circuit. The FACT system will be able to interface into any control circuit and restrict operation through a chip or software and direct all input signals to a designated onboard memory that is also provided time, date, location and the author of command (pin finger print ID or iris eye) as well as the command strings and all responses there to; be they automated or due to human activities.

The individual software will be capable through PFN interface communications to provide their stored data (firmware or flash memory to the National Registry upon a new

installations and will be able to immediately in real-time report this data. Once the data is receive and processed it will be checked to see if it has tripped any alert flags. If there is no criminal or suspect security flags the registry will record the new FACT component installation with accompanying (PFN operating inventory)to the appropriate PFN file in the main registry and apply the appropriate taxes and fees for the product installation.

This will be accomplished through a publicly provided registry phone none or a licensed and bonded commercial server that is registered and periodically inspected and reviewed to have and provide a secure Data Base Connection or encrypted Web connection with the appropriate government agencies (the National Registry, FCC, FBI ect.). This is all part of the Trusted Remote Activity Controller System. This FACT program will provide a secure command string and access path from the origination to any mass memory storage system that is search-able from the National Registry by any appropriate authority or agency. Some Fail safe security for the system is provided by the component software of FACT at the application level establishing a handshake with local memory in the PFN and legitimate remote registry equipment and a secondary integrity check from prior legitimate registry contact data. (possibly a Random code number established in the last contact with the PFN and Registry.

The registry will provide all public providers and commercial servers with the alert flag data so any receiving system will be able to inform the PFN of national security alerts for potentially dangerous devices (terrorist altered components that could be used to activate explosives, chemical, or bacterial or viral microbes contaminants) through the commercial (PFN) remote and management control systems. Of course the appropriate authorities would be alerted to any of the national security high risk installation attempts in real -time. The immediate action could be performed by either predetermined

automated protocols or by real-time commands handled directly by the appropriate authorities. Because, the exact piece of equipment can be ID by it's FACT chip along with all it's Original Equipment Manufacture OEM's firmware (Lot No. and any security codes, ect.) and of course this would be updated by any additional or subsequent use such as re-sales, retrofits or re-installments .An accurate record shall be provided with in the chips firm ware or flash memory and in the national registry(mass storage to be either provided by public government or commercial servers licensed). This process will be readily supported to provide tracking for commercial trading of legitimate products (new and used) giving government the economic taxing tool for real transactions and real-time product use for new and used devices components products and total equipment packages such as (cars).

This will also allow for immediate component analysis for any criminal activity and a clear record of component ownership and use through PFN /TRAC/TRACS/FACT programming. TRACS/FACT programming will be issuing Stolen alert bulletins, and or any security alert flag at periodic times for PFN's to do internal integrity and security tests as this information is reported or becomes available . Otherwise, any device, system and or component will be assessed for it's legitimacy and real-time use at the time date location of installation along with the PFN ESN and what ever other data is determined to be applicable. At this time it will be appraised and billed to the responsible party for it's use and impact on society, it's infrastructure and the environment. Obviously it is necessary to identify the host piece of equipment, and, any and all components the new installation is interacting with, as well as, all interactions from communication devices, control circuits, actuators, and responsible monitors, control an or management centers all

of which is recorded in the PFN secure memory (recording devices) for (accountability) and in at least one remote mass storage facility for accountability.

- The primary purpose of this singular identity component chip is to track any and all use of the attached device and or component that it has been incorporated into and to report any and all data in a complete and integral fashion, as prescribed by any code, regulation, law, and or standard decreed by any sovereign or governing authorities.

Number 2 in Fig 16 is the SMART CHIPS and or a magnetic strip can be provided as part of the components unit packaging and or a bar code so that an immediate check of the component can be search either by a OCR scanner or a hand held magnetic strip reader. With the more extensive amount of data handled by smart cards and chips this is another inexpensive modality that will help in tracking and reporting stolen materials. A hard or plastic card would be issued to the purchaser of any TRACS/FACT device so that they could scan their stolen property data to the National Registry.

Number 3 is the universal plug and play buss inside the PFN containment that create the electrical interface platform for all the components. This buss will carry the appropriate power connection and control connections from the PFN/TRAC/FACT controller to activate, deactivate or specifically control any and all components. Power can be cut off to a specific component through the BUSS or it can instruct the individual component's FACT CHIP to intercept power (power input or regulator circuit).

All the electrical connections in vehicles and equipment are need of standardization and I have written to this in all my previous applications and these are areas that will be a standardization effort in each industry and or application specific use of accountable remote and automated control. I have addressed how to complete these functions with present hardware connections firmware and software and have created some new

modalities to interface all the present devices. However as shown in figure 6a the components and technologies are merging and this universal plug and play BUSS in the PFN is an ideal way to make compatible this electrical interface platform.

#4 of 16 is just pointing out that the individual component FACT CHIPS must provide firm ware or stored data of identity, OEM data, last application, ect to comply with any standard or regulation developed for a national registry or any such security system. Because FACT is a major part of the main operating system in TRAC it's software is also modular and can be in any form or hardware application. The hardware chips and firmware modality detailed in this application should in no way be considered the only modality to create a nation wide security and management that is capable of real-time control of individual components, devices, and equipment. However, any other modality should be considered within the nature and scope of this invention. And this is area #6 of figure 16. The chip also can perform activation and deactivation of the component and that is what is meant by saying it "must provide control"

Note: While in the description of the FACT component in this invention is described as a chip, this does not have to be the case. And the best form of data management for security is open to each individual manufacturer's best options with their particular products to provide this function so long as it is approved by any governing standards for this use. It is obvious that a physical chip could be replaced or compromised in it's firmware so additional means will be utilized to insure security

Such as the random code exchange discussed above at the last legitimate contact or string of contacts with the Registry allowing only appropriate one way communication at the time for the PFN compare list or component compare list is

running to validate a legitimate registry contact or vice versa for the registry computers being accessed by a new PFN component application.

FIGURE 16

This is a general flow chart of a self contained PFN TRAC/ FACT management system that will be utilized by every piece of equipment. PFN's may have all the listed components or any number of them,; however no mater what is electrically interfaced it will have to be approved and registered as it is activated or deactivated. The very first triangle at the top numbered 4-500 refers to the one and two way pager systems detailed in the figures 4 and 5 of this patent application. These pagers as is true with all components will ultimately be provided FACT software to identify their activity and especially for those technologies that are responsible for providing communication data for remote control.

The second triangle is for cellular phone systems and is completely detailed in figure 6 as a more sophisticated communication system capable of handling and delivering very good data signal in volume and quality for applications needing such quality such as real-time video, ect.. The 3rd triangle 0- infinity frequency refers to any and all kinds of Radio Frequency equipment (including cordless phones and high quality and high powered RF equipment equally capable of providing large data streams modulated on their signals .

The 4th triangle with the word locate can be either cellular phone poxcimetry tracking, GPS, Lorands, LoJack or par of any interactive highway controller system or master surface transportation control net work and system receiver and or transceiver. Along with this locate system triangle the 5th triangle is a miscellaneous communication receiver and or transceiver that is responsive to light, sound or any discernable electromagnetic wave or transmission.

All of these PFN communication triangles devices or modalities shown as upside down triangles are not shown in figure 18 as having a FACT chip but they would also be

provided with FACT software to report their activation and any specific role played in any remote controlled event as either as a receiver and or any type of transmitting device. As is evident in the drawing they are connected to #1701 which is the uni-buss connector to the PFN/TRAC control system and accompanying memory storage units. 1702 is the Trac software with it's resident FACT software program. This fact program can be updated and it is capable of storing and retrieving data back from it's accompanying data storage. As detailed through out earlier related applications these PFN control circuits are sophisticated mini computers with extremely efficient processors in the for of euro 100 boards. . And as explained in figure 6 all these technologies are merging an the improved capability and speed of processors is in the major reason for such enhancement. For this reason I am claiming that these improvement fall within the nature and scope of this invention to provide accountable remote and automated control for society and it's institutions. TRAC is of course the Trusted Remote Activity Controller a modular based software program of which FACT the Federal Access and control Technology is an intricate part. These programs are run by the PFN min-computers and they send their commands and direct the data received by the uni buss to the appropriate data storage. Either a hard drive or the specially preserved non-volatile FACT memory that can either be down loaded or physically removed to be used in a court of law in the proper manner as determined by any rule regulations or laws governing evidence and it's acquisition, preparation and presentation for a society.

Both on the left side and right side of 1701 uni-buss is all the interfaced controls Accessories personal items and electronic possessions and alternative data communication devices. These devices are coded in the upper corners with the initials or first letter of the words that describe their boxes as examples of connectable interfaces employing the individual FACT Chip. This becomes more evident in figure 18 where the bottom of the page supplies numerous octagon stop sign shapes filled with these same initials indicating FACT applications and tracking. Also before leaving figure 17 it is

important to remember that in the ram memory of the mini computer the Fact ESN will be stored for all memory devices and the memory will always require the processors ESN or any comparable ID technology for any further or final review by the appropriate authorities or to comply with any legal proceeding.

It should be also understood that this universal Buss can extend outside any protected area with the immediate electronic protected capability to recognize and protect against any deliberate shorting or questionable interface. At the bottom of figure 17 the universal buss illustrates it's capability to handle power as well as in put and output control transmissions . It is also important to make clear that this involves a universal secluded antenna buss or reception will be provided for by certain types of physical structural elements in the PFN's structure to allow for patch antennas or physically small profile antenna structure to function with in any standard regulation or legally prescribed manner.

FIGURE 17

At the top of figure 17 there is a box to the left called the National Government Activation and Check System. From there - there is an arrow showing a Data Base Connection (DBC) or a world wide web Internet connection (encrypted if applicable) with the number 300 above indicative of any local and regional network as is evident between the left national box and the box on the right side of figure 18 which is termed Local Government Activation and check System. These most generally are the primary sources to supply data and or to act on any data receive that involves National security , Public safety other than individual input which in most cases is provided to either one of these node as would be any international requires , which will always first be edited through the appropriate national authorized channels. The National Registry will be a large routing system for mass management with only a system processing storage protocol and system that will handle data in a prescribed and secured manner through any and all of the 6 transparent IP layers to the appropriate seventh application layer detailed

earlier where it is transposed by the application encryption to insure security. This will be the same for all forms of communications wired and wireless as they are processed through their respective communication nodes and gateways (licensed Providers and Servers) to land lines, fiber optic cable systems or land cable systems.

The center three blocks are the facets and functions of the national and local registry for government, to develop security for all in the nation and to provide better public safety and to build trust within all of humanity, because of accountability and fairness. This is a safe guard system for man and machine messaging that is accessible by all of a nations society first individually through internet connections and if not accessible at least by any portion of humanity accountable to all involved parties through comment or constitutional procedures provided in the TRAC/FACT software. Internet dialog and media awareness for all types of media (mass and individual) as well as responsive and public access and input will spawn a much more involved individual citizen and functional democracy.

The first center block is termed **AUTHORIZED INSTALLATION REGISTRY**. This may be a network of secured computers in different locations or it might be one system in none location. The inventions purpose is to create realistic functional modality that can create this national and local registry level of accountability presently out of existing computer systems and to project some future consolidations of local nodes for related activities and data to help structure efficient data communications for all the government agencies an commercial services. The Actual structure of course will be part of a large standards effort and civil legislative effort.

Total purpose goal:

This is the base system to create a national directory of all products sold and re-sold in a country to better track their impact on economy, resources, environment, health and infrastructure all around the world and at the same time to allow nations to have a FAIR frame work to develop and use imported products, which are needed. The PFN system

can help to develop trust to insure an accountable answer to all of Societies legitimate concerns first for individual survival and then to be part of a mutually healthy co-existence with all of humanity , and all forms of worldly life.

The Authorization Installation Registry function is to record and make available by request and or to recognize any PFN use of an electrical device in conjunction with the PFN and first run a compare function to any and all legally known produced , and legitimately marketed products in a legitimate sovereign locality through local and or toll free telephony or RF or MISC. communications technology employing isolated network connection and or the Internet (IP).

The authorization installation will require a complete OEM specification and description that can be used to specifically identify individual devices and or components (Requirements to be determined by the sovereign authorities). This data will provide depreciating value levels and integrity checks that will be beneficial in tracking use and varying performance for securing public safety. Also the depreciation schedule will enjoy a diminished cost of operational tax relevant to the products prior use and or time of use. This provides a use tax not a sales tax for governing structures to apply to real time use. This frees the Internet to trade and free communication for general transactions and allows for the legitimate taxing structure for actual impact on society's infrastructure and environment by machines and the work they do

The second block is the Restricted Authorization or Crime Registry. Once again this data is supplied by everyone and anyone but primarily cleared and reviewed by the national and state or regional governing agencies. The really great part of this section of the system is that the private individual can in real-time participate in a personal injury theft by telephony with scan data or through personal contact with law enforcement agencies. With total accountability all parties will have to face their own actions in the proper legal settings. And basically there will be no use or miss - use of stolen property.

Of course this can be done for resources and all things needing monitoring to insure any fair deal is lived up to and or is humanly reasonable.

The third center block deals with the communication capability. Ideally this will be accomplished by toll free telephony or RF nodes for the public in using the public's privately owned equipment and PFN link ups as a hospitable commercial service with all other gained accessible service options and provided free by government or public providers for the tax and public interest provisions.

The 4th block in the center of figure 18 is the centerpiece of my inventive technology for each individual piece of equipment in this machine messaging net work. It is the Protected Primary Focal Node or PFN created as a protected electrical interface platform to merge, focus all host equipment's accessories and component's power and control circuits into one local accountable control and communication center. This PFN on every vehicle or piece of equipment is then linked, coordinated and managed with all other machine use and activities by a greater mass communication and management set of computer network systems (through RF, telephony and nodes or gateways) either for surface (land and sea) coordination and or for aviation.

However in this figure we are concerned with developing an understanding of the FACT software in the PFN and or possibly individual CHIPS that are at the bottom of the page as octagons or (mini-stop signs). Once again these might well be in the form of physical hardware and read only firmware or they might be integrated software programs interlaced and inter-reliant on the PFN/TRAC/FACT security encryption both in the PFN and in the National Registry system. Through out this entire drawing figure 18 there is two way communication from the individual chips or FACT programs to the national government activation and check process. However, the PFN gives the commands to the individual chips via the universal plug and play buss. And retrieves their essential operational data e.g. ESN, and or MIN and production Identification and seventh layer application security instructions from the ISO OSI networking Model. If

for example a stolen audio or sound unit is connected to the uni-buss of a vehicle. The PFN computer will signal or request information from the individual FACT chip in the sound system (SS-ESN-F). This can either be sent by isolated control hardware (wires, ect.) or by sending a modulated digital signal on one of the power legs or it can be accomplished by short range transmissions if this modality is employed in future wireless vehicle and equipment control systems to ease plug and play capability and reduce the need for so much hard wiring. No mater the means the PFN will inquire for an individual fact chip as soon as it senses current draw. If there is a change in current from a normal operational level the PFN will request and or review vehicle conformations for any trouble codes logged in the charging system or any battery draws or charging problems . This is performed by a TRAC software algorithm

And standard current sensing micro chips in the uni-buss and in the host equipment's electrical system, which can generate either analog or digital signal that the PFN/ processor can receive and recognize through any of the above in vehicle communication modalities. This current sensing system is part of an anti-tamper system of the PFN. It will give driver alerts to the abnormal draw unless an individual component FACT chip sends an ESN and data signal that is recognized for a specific authorization or security protocol. At the very least all components can be individually judged for their current draw and reported to the display or checked against their OEM manufactured specifications (Data delivered by the individual FACT CHIP to increase security that a component has not been altered after manufacturing. Even a individual resister chip like that used in the present vehicle keys could be installed secluded in the board with the FACT Chip to add even greater security and integrity checks. While this idea is creative and new the technology to make these combined innovation are available as electrical components and any one who is skilled in the art could from reading this section create the necessary circuitry to complete these security tasks. All the components are listed through out my related patent applications for the trickster circuits and the security seal

activation switch. The universal plug and play Buss as always stated will have to be a standardized effort for the most optimum development. The little octagon stop sign FACT chips at the Bottom of the page have letters on the top of the sign like AC-F which means (Activity controls- function) . These correspond to figure 17 left and right blocks. Once again all the components operating in or through the PFN will have to have FACT chip identity capability, communication processors, data storage as well as all these listed that access the uni-buss,

FIGURE 18

This figure depicts a universal PFN system with some usual device applications and varied hardware hook ups to communicate with the remote locations and physically perform the Accountable Remote and Automated Control for society and it's institutions. The bold black line with universal PFN enclosed is to indicate that this is a protected area not just physically but legally. In the enclosure 1901 is a commercial off the shelf COTS cellular phone it show one modality of connectability through a PCMCIA modem connection to the processor and internal TRAC\FACT software. In this application all the software is commercial off the shelf supplied by the cellular phone company and or the PCMCIA modem card interface. Obviously this preprogrammed software would be downloaded and the appropriate dial out phone numbers installed in the command string. These would be for commercial servers and or public providers as illustrated by the little man at the computer 300C, 300 L and the whole 300 networking system.

Below the PCMCIA connection block is the block called Complete Card. This is a desired modality for cellular phone use in the invention. It employs a commercial off the shelf COTS product a PCMCIA Complete Card TM. The complete card also supplies its own software and hooks up in the same manner as a PCMCIA standard modem card. However this system also incorporates the Cellular phone system and antenna. The

appropriate hardware is known in the industry and the appropriate configurations can be accomplished by anyone skilled in the art to link up the euro100 boards with the PCMCIA connections. The bottom box is modem and can be part of the top box PCMCIA connection when used with telephony or with any application from the lower box 1908.

Number 1908 box shows all the different types of communication devices employed in the PFN's. 1 way Radio, 2way radio, 1 way paging, 2way paging, light or sound and GPS or locating systems. These different communication devices are well covered in the in figures 3,4,5, and 6 and will not be revisited at this time. However, as this drawing illustrates they would process their data streams through the modem and on into the processor to be handled by the TRAC/ FACT/CEW programs ect. The modem would be capable of converting the applicable data steam and communication source to be used by the PFN processors. In this same block light and sound as well as any other electromagnetic wave that can be used to transmit wirelessly or hard wired to a converter or modem to deliver control signals to the PFN system are hereby included by reference as another modality of communication. In earlier related patent applications traffic control devices were described for authorized personnel to control in real-time a particular vehicle by pointing such a tool to a specific target vehicles receiving plate and to control a slow guide stop and secure sequence for a suspect vehicle.

1907 is the uni-Buss connector that has also been discussed earlier. However, ideally an accepted industry standard will provide a universal plug and play capability and the TRAC/FACT software and TRACS management system will insure accountability and real-time control as needed. All possible present connectable hardware was detailed in the related application docket No. 112756-202. However as stated before the plug and play capability for power, control signal is part of this technology as described in figure 6a as natural evolution of this invention. whether it is for a mobile application (car) and or a stationary devices the control power and signals to the

processor can basically use the same kind of plug and play Buss. 1903 is the mini-computer containing the TRAC/FACT programs. The round circle is for the CEW program Commercial Encryption on the WEB . This software program is provided by the credit card companies and will have a special modem capability and handle 128/64 bit. 1902 is a card swipe or reader that is connected to the processor either through the uni-buss or the old R232, TTL, or PS2 type of connections. These three are shown here as the present standard connectable modalities known to present industry. However the uni-Buss connector would be a more ideal modality for space greater data flow, and efficiency. These old standard connections are shown to be available to other components interfaced in the PFN and can be employed to give forward and backward engineering versatility. These would be limited in number as time went on and would have separate software command strings, with the appropriate drivers to access this different Com. Port and coupled device to complete the interface with the PFN. The device would still have to have an electronic FACT ESN or identity system or would require special registration to be interfaced. 1902 the credit card reader would be able to handle commercial credit cards and driver licenses and FACT SYSTEM identity cards.

1905 is the hard drive on going memory storage. For size reasons in this drawing the FACT application specific event memory is not shown but it is a redundant memory to the continuing running on the hard drive. The event recordings are controlled either automatically by resident PFN programs, remotely activated and controlled by an authorized external source (Logged command string) or by the resident operator or occupant. In any event all machine and man actions and interactions are recorded and logged in the FACT Memory preserved in the protected restricted access area as depicted and detailed in figure 2C , 2F and 2G.

1909 is a big dotted line which is the uni-Buss going out of the PFN and going to activity controls video cameras (or Digital) microphones and activity sensors as well as generic host control connections. Some of these sensitive control and sensor leads will be

provided PFN protection special and or utilize the host vehicles strongest architectural structure (e.g. the frame) to protect these critical transmission lines. This should be determined application specific and as part of a standards effort. I have gone though a great deal of effort to detail all the properties and qualities and give modality examples to provide a standards effort a good clear organizational system structure and electrical interface platform to provide Accountable aggressive remote and automated control for society and it's institutions.

300C in figure 19 is the commercial server who can be any gateway node the customer picks or can be a service provider for the OEM host equipment or an energy provider or a bank card provider or a communication company or any type or number of these commercial servers. However they must be licensed and provide enough mass storage to handle all critical TRACS/FACT data to operate in any geographic area. They also have to be able to handle it in a secure accountable manner. For simplicity purposes the 300C have been placed at the bottom of the 3 basic different types of present wireless communication. To the right cellular phone system ,to the lower left of figure 19 is the present one and two way paging systems and for the lower right is the Radio frequency systems. All of these systems connected to land lines (fiber-optics, ISDN, ect) to perform any hardwired Database connections they are computer operated and act ac gateways to isolated computer networks and can provide web access on the Internet. (if need be encrypted). A sample of the types of commercial businesses that would utilize each type of communication technology has been listed under their respective areas. This is in no way intended to represent all the possible commercial uses as the PFN will ultimately be on every piece of equipment.

In the middle right the rest of the 300 system is illustrated by the large computer stations manned. The one with L.G.A.&C. SYS. Stands for Local Government, Access & Control system. And the one labeled N.G.A.& C. SYS. Stands for National Government Access & Control System. In all communication areas and in the extreme

lower right hand corner is satellite and a satellite dish connected to land base phone lines. This is to show that the national registry can provide complete critical TRACS control and FACT data to it's entire geographic area and is also capable of transferring Data internationally at the proper authorities desecration. Some of the proper government agencies are also listed but all government agencies could access and create data as could even the general citizenry for total accountability. of course specific data on individuals would not be obtainable or used unless authorized by the individual or as the result of some legal action as is the present case. Any such mis use or access would be reported to the individual and alert the authorities and the person violating a persons individual privacy would be criminally charged and subject to civil action as would any agency or commercial storage area. This means total accountability. This system has been designed to respect individual privacy. Which means that the individual has to release any licensed storage facility public or private no mater if they provide the service free of charge or not. However, Gross non descriptive data can be sold and discriminated as long as an individual can not be identified or compromised in life the pocket and the pursuit of happiness. The exceptions to this rule is that if through the course of operation a piece of machinery they endanger others (public Safety) then the proper authorities and commercial insurance agencies can access these personal records. However an individual can give permission electronically in real-time if so desired with a signature of a PIN number for consent or a verbal voice recognition or the fingerprint steering wheel, video snap shot, or a signature on an electronic pad or the iris reader and voice recognition or any combination of the above. Free service can be provided and personal data can be acquired and used if this is agreeable to the individual.

FIGURE 19

This figure will detail the registry system in general. At the very top of the page is a small box that says World Organizations. This is the present state of World affairs that the national government agencies should be in control of the data involving any and all mechanized civil and industrial uses of equipment and the impact data. Ultimately the PFN TRACS system can help to develop trust and fair play in the use of the worlds resources and equipment as well as free humanity in an efficient manner. When humanity matures past survival paranoia to address only the real fears of peaceful co-existing the PFN management system will serve it's greatest function. However now it is best used and developed in the individual nations. As communication and understanding is increased the natural sharing of data will take place and is already transpiring on the Internet. For the present all government agencies will serve to clear all PFN data that is earmarked for their attention through the National Registry and be responsible for it's dissemination world wide. This is why the big black triangle ends up with National Government Agencies. Of course any data request generated by state and local agencies or pertaining to same agencies will be notified and enjoy all the same rights constitutionally guaranteed to day in their governance, but over this new technology.

This is the means by which taxation can be performed directly from every PFN (Sale and or use tax) for the state and National government as has been depicted and addressed in figure 14 of this application. Also credits can be applied back to the user or citizen for any community service performed by their equipment. Also aid can be applied with re-education programs carried out through PFN terminals for defunct industries and old jobs that have resulted in lay offs. This has been detailed in figure 14 .

The bottom of the triangle has LOCAL GOVERNMENT in big bold letters. This is done for two reasons. First local node and gateways will keep cost down for Registry network and second regional state and local government is the agencies that impact the individual in most cases. As has been detailed earlier in figure 13 all the government agencies are now maintaining web pages and data phone nodes and through basic routing

using ISDN of Cerent Industry new fiber optics and Cisco systems routing capability these agencies can be given an efficient data management for local regional and national Data base connection and inter agency connections as well to allow for the fast local discrimination of data as well as provide much of this general data on the web for the public on or through the media

Below the local government registry are the FACT Management & Memory for commercial servers. And to the right side the same FACT Management but provided by public provider nodes. The difference being that individual commercial servers will be providing more fee for services from emergency service to computer down loads and the public nodes basically will be for government services. Basically the PFN will use both systems commercial and public. It will do it automatically if it is pre programmed by the owner or it will do it as a directed command either given locally or remotely. An important note is that both these TRACs systems will provide accountable memory as does the PFN at the very bottom of the page which is responsible for activities performed and authenticating the activities. As shown and discussed in figure 19 land line wireless and satellite communications can all be used in the system

FIGURE 20

This is a flow chart to detail FACT software in the PFN on a host piece of equipment and also the interaction in TRACs/FACT software programming in the main registry. For a new install the process is started by plugging the component in ideally to the Uni-buss. As illustrated by the second block down the PFN/TRAC/FACT software recognizes the Components Fact chip and calls a predetermined number. The call in number can be a commercial server or a public provided node that access the national registry detailed earlier. As shown on the right half of the page is the TRACS FACT software in the main registry system. This is the national and state government registry system . The call in received by the PFN data from the new component check compares the ESN and manufacture data to OEM supplied registry lists and known crimes of stolen

property registered in the registry. If all is clear the registry approval is given and the transmitted back to an approved registration program in the PFN. The component is listed as it's appraised value is taxed and shown on the display for the operator and or owner of the host piece of equipment.. The same redundant data is sent to the appropriate governing agency and a tax bill is prepared, unless the operator decides to pay in real-time with either a credit card or bank debit card in the card reader on the PFN. In any event the entire transaction is timed dated and the run status is added to the inventory list of the vehicle or piece of equipment. If hard copies of the transaction are required a return E-mail address can be sent to a home unit for printing or memory storage or printed on location from the PFN or down loaded to a Lap top..

If a component is flagged with an alert it will be accompanied with specific software commands or additional alerts depending on the severity of the situation. A simple theft protocol might activate the unit normally with out notifying the user and alert the appropriate local authorities to the location of the stolen property and then regain custody of the stolen property and inquire as to how the person in possession received that property.

If there is a Terrorist alert to a particular component as soon as the person install the unit the alarms will be activated in all emergency responding agencies and even kill all power to the PFN and or set off alarms and warnings. This depends on the nature of the emergency and will allow for on the spot real-time commands to augment any response. As mentioned earlier FACT can provide a stealth eves dropping mode so that operator owner and occupants can not tell that they are being monitored and or recorded but this access mode will require a signed judges order and his personal access codes that are changed by time mode to send this command. Once again any miss use or abuse will of this mode will meet with serious criminal and civil penalties for the individuals involved and or any agency private or commercial entity. Freedom of information act will apply to any legal own of their PFN controlled equipment and they will be able to

download their individual memory that will show a complete access and use of their system coded with the agencies ID (local and national as well as for commercial access

The only exception is the court ordered stealth surveillance :

All other contacts must first announce their access, be recognized and agree to the process or it must be a time of national emergency, marshal law or a crime in progress. In any event all will be recorded and accountability will be part of any process to use or not use the PFN record as evidence in a court of law. The exact use of recordings and the preceding announcements or Maranda rights will be part of a legal standards effort.

Also a redundant record will be kept in a remote location either in a licensed commercial FACT server or in government mass storage. These systems are detailed in earlier related patents. As the spider eyes and green eye software programs. The Fact program will basically be operated with the Justice Department the FBI IBSR incident base Reporting system and The UCR the Uniform Crime Reporting system and it will be part of this technologies Spider Eyes system and will be totally accessible to local law enforcement and even the general public through national state and local agency editing as justified.. However all crime activity will be given ID's either IBSR-UCR or local and all data can be retrieved from the mass data in any discovery to make everyone accountable for all decisions and use of data including editing from the public.- MS is the mass storage in the TRACS/FACT system. Basically this drawing is self explanatory and I have outlined in writing what would be incorporated in any software algorithm as well as how humanity will be able to legally use this technology in a constitutional way

FIGURE 21

Although there will be many different software programs in TRAC and in the TRAC's system. Fact is being used here first to handle National Security and High Security Situations and to create more aggressive remote and automated controls with useful management systems, while helping to insure National Security, Public Safety and

maintain respect for the individual citizen all though TRAC accountability. The software flow charts in this figure are being used to illustrate the detail and capability of the PFN/TRAC system. Not all software applications will be detailed in flow charts here or in the related patents however from this detailed FACT software flow chart anyone skilled in the art of computer programming will be able to read all the written discussion of TRAC software programs and easily duplicate a software flow chart to write a program and or algorithm to perform and complete the functions described in my writings. To write and then to flow chart all these software programs would be impractical and unnecessary after several software programs are so illustrated much would be a redundant exercise. So for this reason any software, programs and algorithms developed to perform even the written described functions in all the related patents are considered to fall within the nature and scope of this invention and or technology.

Presently a more extensive discussion will take place on the Federal access Technology FACT which is being used as a model for the programmers and engineers to develop and manufacture the numerous products with norm skill and understanding in their respective arts.

In figure 22 this software flow starts in the TRAC's System or in the main registry. Here alert flags are generated with the correct FACT ESN and case number for fast cross-referencing in the IBSR or the UCR operated nationally by the FBI. However not just law enforcement and other government agency will be able to innate an automated crime re port or alert but also the general public will be able to file an automated report through area government operated web pages and Internet PFN access as well as in the traditional manner with the area police department. FACT cards held by the legitimate owner will allow for rapid scan in or card swipe by a magnetic reader. These encoded cards can be prepared and programmed at the time of a legitimate purchase and any and all identifying data will be available to complete a crime report

with the exception of listing the geographic location unless the theft was automatically reported by the PFN as it was being tampered with.

The second long box below for restricted authorization and crime registry will process the crime alert report. As stated earlier if it is a theft it might require on type of automated and remote control responses, and if it is an emergency (public safety or National Security scenario it might require another type of aggressive remote and automated control options. And of course if the first box above is processing the normal commercial registry of products and product information the normal install sequence would access this data and activate the unit and prepare any tax information and pass it on to the appropriate accounting agencies.

FIGURE 22

Track a Con.COM This system would allow for parolees to be back in society while their movements and activities were monitored and governed by an automated computer system that would track physical movement through GPS, or LoJack or Cellular and or RF triangulation on a personally carried device that monitors body temperature, pulse rate and provide for positive Identification e.g. Finger Print or eye iris evaluation The device would be controlled by the master controller and support local Web page access and hyper-link capability. Tactile and galvanic sensors would be capable of detecting chemical changes in perspiration and determine the chemical equivalent for a specific person drinking and provide a specific electrical signal that is transmitted back to the parole center for a con beep and direction to either report in or take a skin prick check or a breathalyzer. Locations of area liquor dispensing or known drug activities and be plugged in as trail markers on the GPS and flag a convicts questionable activities or ask for the above checks.

Prior victims of crimes that an Ex-con is convicted will be notified of the TRACK A CON.COM and the Con will be given a reasonable distance to stay away from the victims. Once again the appropriate trail markers will be posted as GPS, ECT.

FIGURE 22 GREATER DISCRPTION

Track a Con.COM This system would allow for parolees to be back in society while their movements and activities were monitored and governed by an automated computer system that would track physical movement through GPS, or LoJack or Cellular and or RF triangulation on a personally carried device that monitors body temperature, pulse rate and provide for positive Identification e.g. Finger Print or eye iris evaluation. The device would be controlled by the master controller and support local Web page access and hyper-link capability. Tactile and galvanic sensors would be capable of detecting chemical changes in perspiration and determine the chemical equivalent for a specific person drinking and provide a specific electrical signal that is transmitted back to the parole center for a con beep and direction to either report in or take a skin prick check or a breathalyzer. Locations of area liquor dispensing or known drug activities and be plugged in as trail markers on the GPS and flag a convicts questionable activities or ask for the above checks.

Prior victims of crimes that an Ex-con is convicted will be notified of the TRACK A CON.COM and the Con will be given a reasonable distance to stay away from the victims. Once again the appropriate trail markers will be posted as GPS, ECT. Geographic coordinates and will notify authorities and victims of flagged improper movements. The convict will be alerted as will and warned to report in and move out of the area. Also the victims can be outfitted with a mobile page and or Track system a warned directly of a past ex-cons close proximity. Additionally the victim and community can track the parolee on the system by contacting the web pages. 2201 is a bracelet or belt to attach the ersonal PFN or tracking device to a suspect criminal or child or anyone for that matter 2206 is the unit itself with a fingerprint thaw that can insure that the correct person is wearing the unit. The system could have an iris

159 B

recognition device, pulse sensor galvanic skin sensors, contactor for skin prick or breathelizer system that can monitor the wearers activities and body reactions. There could be any of the different communicating devices as listed and a processor and memory storage all application specific but basically taken from all the technology contained from all the inventions related patent applications. And the power source could be a battery or the electrical power could be provided by contrasting metal inserted into the body of a human and basically use their body as the power source. Ultimately an intire micro transmitter system could be place under the skin in another modality with no belt at all.

To continue with the figure 2202 is the antenna 203 the antenna lead would be incorporated in the belt. And 205 is the battery. This is being brought up with a new drawing presently but numerous modalities for this separate invention has been detailed in earlier patent applications.

CONFIDENTIAL

Geographic coordinates and will notify authorities and victims of flagged improper movements. The convict will be alerted as will and warned to report in and move out of the area. Also the victims can be outfitted with a mobile page and or Track system a warned directly of a past ex-cons close proximity. Additionally the victim and community can track the parolee on the system by contacting the web pages.

Claims

- 1) A claim is made for a any programmable and or modular software and or firmware that provides accountability and is used in and or with any hard ware as a trusted remote activity controller for automated and remote control functions and or robotics.

on a vehicle

on a machine

and or on any equipment

or as a piece of remote control equipment

either packaged in a physically protected environment

or used without physical protection (but especially with physical protection),

either having local memory storage and or a plurality of local memories, and or without local memory,

Either with remote memory storage and a plurality of remote memory storage , Or without any remote memory storage.

- 2) A claim is made according to claim one to refer to this programmable software and or any other accountable software program that performs automated and remote control and or robotics functions as a result of programming that can authorize, authenticate and preserves commands and save feed back data as a TRAC software program and proprietary to this technology and it's nature and scope, TRAC stands for Trusted Remote Accountable Controller

3) A claim is made according to claims one and two, that TRAC software is provided at least one non volatile memory storage and that TRAC controlled events are in secured environments so that it is highly tamper resistant through physical means and equally protected through electrical means and tamper resistant software programming to become an agreed upon standard for accountable reliable and trusted software commands and record keeping for passive and aggressive remote control and robotics to analyze, judge, evaluate, value, appraise and monitor, manage and control

Vehicle use

Machine use

Equipment use

Facility or installation functions

Perform financial transactions in real time and in stationary and mobile settings

4)A claim is made according to claims one, two, and three for TRAC software programming as proprietary in providing any accountable data to any E-mail address web site and or through the use of the World Wide Web and or Internet Protocol (I P)either for financial purposes, governmental uses, service providers, social purposes, environmental purposes, and or undetermined purposes.

5)This claim is made in accordance with claim 4 ; there are to be two basic sub software programs either modular and or programmable as determined by the existing hardware and operating system firmware or software for any application specific manufactured PFN\ TRAC termed FACT for Federal Access Control Technology and CEW Commercial Encryption on the Web that are responsively connectable through any communication medium in the PFN/TRAC system to a National Registry that provides protective surveillance as a clearing house though the FACT sub program to insure Public Safety and National Security, by

quarrying each component device attached through a PFN/TRAC system and or piece of equipment to determine if said connectable component is legitimate and cleared for safe public use.

6) This claim is made in accordance with claim five, that a FACT National Registry be created incorporating any and all applicable government agencies (national to local government) with their own access to the Registry and or network with encrypted codes and Identity command strings which are communicative and (Transparent in I P lower layers),

also access for the general public and their Private Encrypted Identity codes (PINs etc) access to same said registry (also transparent at (I P lower layers) for the purpose of reporting criminal use or activity involving devices and or components used, so that The Fact Registry Software system can continually perform around the clock searches for these illegal, unauthorized and or dangerous components, devices and or equipment through the PFN/TRAC system or any other connectable systems or networks thereby performing real-time interruption and interdiction legally, electrically and physically as part of accountable aggressive remote and automated control and management.

7) In accordance with claim 6, The FACT National Registry will be accessible by all Manufacturers on a world wide scale with National security protocols for FACT in the marketing of component, devices and equipment and the manufacture must provide an acceptable FACT program along with a Depreciation schedule for their product to be given authorization for sale in a country or PFN/TRAC /FACT. Registry will not activate either the component device and or piece of equipment,

Resale of the component device or piece of equipment will be requested upon each connectable to another PFN TRAC

owned system and or if it is being loaned by the previously owner or sold from the recorded PFN inventory of another owner both parties will be quarried to respond to the nature of the new install as the registry is contacted and requested to activate the unit in it's present PFN/TRAC system

This provides all governing bodies local and national to apply their tax structure and removes the need for a tax structure at the point of sale and puts it on at the point of use and real-time impact on the environment and societies infrastructures .

NOTE:

(little more difficult for the manufacture at the start but frees the market up for commerce) (it also allows better tracking of components to retrieve damages for stealing technology once the point is proven and the accounting process will be needed to determine damages) (globally) (can also be extended to music and Cinema with the appropriate encoding and home devices tied into home management PFN/TRAC systems and computer networks All components and software drivers would be running FACT protocols and would only allow for one illegal run after automatic Registry check and then the bogus disk would be unplayable on the same FACT protected equipment . Devaluing the illegal product and making an account of the number and use of the illegal copies.

8) In accordance with claims one, two, three and four a special claim is made for the Proprietary TRAC program with and or without this technology's proprietary protected primary focal node PFN's physical and electrical interface system to be an industry standard in all industries and certified and endorsed by the insurance

industry, governing agencies, professional organizations, the general public safety and commercial interest groups, and industry and commercial research groups and organizations as the legally acceptable system for accountable remote control and financial transaction technology for society,

In accordance with the FACT registry CEW this technology's Commercial Encryption on the Web will support any and all payment industry software (bank card's ect) and report the use of a bogus credit card or automated payment device to the FACT registry as it is reported by user and or Commercial company and alert in real-time the closest local authorities to investigate the use if so determined as the appropriate FACT response for public safety otherwise the commercial credit server will just disallow the use of the credit card.

9) According to claim five TRAC software record keeping requires terminal and or device electrical serial numbers and personal identification numbers as part of it's authorization and authentication program with the time date any geographic location coordinates or address of all the equipment and systems participating and or performing entries and or accessing any application folder or event file in storage at any location or part of the Registry.

10) A claim is made for an electrical seal system to detect tampering and to provide a water resistant seal protection for any containment for adhering any two surfaces with sophisticated authorization energizing systems without sophisticated authorization energizing systems web page Internet data

11) The PFN /TRAC local control unit is constructed to allow for the installation of a High Security PFN system that will operate strictly on Data Encrypted Standard or the highest level of military and National Security Agencies encrypted application levels simply by entering the high security PFN and

inventory the host machines FACT components and re command them to the High security PFN. This can be done through component or chip insertion in a standard commercial PFN/TRAC system or it can be a total PFN exchange, however the host piece of equipment will not operate any of it's accessories unless it is provided the correct signal from the FACT Registry or the High security DES network. Point of claim is that this provides Commercial Off the Shelf (COTS) products immediate and cost effective conversions for high security applications in there controller packages. E.g. standard cars chanded to be controlled in the most aggressive manner (out fitted with weapons in hostile environments) e.g. Embassies

12) The Fact registry will be a connectable service available to all types of communication systems as detailed earlier they are part of the PFN/TRAC management and control systems and will be made accountable locally and remotely through memory storage as part of a Machine Messaging Network on The World Wide Web The MMNWWW that has it's main purpose to provide Public Safety and National Security by monitoring the use and impact of machines and their components on the environment and societies infrastructures as well as human interaction, the system may be isolated from the internet through transparent lower level (IP) communications and or be totally physically separated at times and places, however the major purpose of the PFN/TRAC system of a Machine messaging Network is to provide free information to all to better plan and use shared resources, even though it may be necessary to protect and control some data and equipment management for Public safety and National security so that is provided for in the isolation of data and contact but it still falls with in the nature and scope of this PFN invention.

13) An independent claim is made for a personally worn PFN tracking device that can be worn by an individual and report their location to at least one web address

through a public server gateway node, or publicly owned provider node using any type of communication system,

an additional claim is made for the networking use of any multi-communication capable PFN to relay or repeat shorter range signals for personally worn PFN devices.

XX

ABSTRACT

This is No. 4 Abstract

ABSTRACT

This application is the detailed description and construction of the PROTECTED PRIMARY FOCAL NODE (PFN) when it is utilized for High and Medium security (HS) and (MS) remote control applications. The invention was always designed to remotely control the security and use of machines, equipment, and vehicles through various levels of monitoring and remote control systems and networks. And all of the technology has been designed to marry up to preexisting devices and systems to develop cost effective enhancements at the very least where ever possible.

However, these HS and MS (PFNs) are evolution's from the already secure protected interface known as a (PFN). The PFN designs were described in detail to further the monetary and environmental accounting system for all equipment in remote control applications. The PFN is the combination of the Black Box and Billing Box which detail more explicitly all the functions of the protected Stop and Control Box from the earliest related patent application). The different Boxes (Stop and Control, Black Box and Billing Box) were terms used to give explicit understanding of the functions and commercial meaning of the secure protected and accountable remote control interface.

This application and the earlier applications have been submitted to expound on the protected stop and control box, which was initially designed to restrict unauthorized

COPIES OF THE

use of equipment, machines and vehicles and or to limit their use and functions proportionally to the amount of receivable monetary remuneration for that use and or impacts on the environment or any environmental resource use for commercial and/or economic applications. The earliest applications name and describe all the various modalities of remote controls, peripheral devices interfaced and communication devices that will be employed to accomplish any necessary remote control or to secure any piece of equipment.

006770" BFBF09

So this application focuses on the high and medium security protocols named in the second formal 112756 202. Basically this application will focus on the protective packaging for the containment and any specialized modification of the electronics for extreme environments (Application specific modifications). Also on the security of any data signal, transmission and/or land line data transfer from a secure area and to a secure area, either from the PFNs or any derivation of the monitoring and control embodiment and/or combined systems and/or integrated networks for, e.g., government installations and sensitive commercial compounds where security, remote control and robotics are the best and/or safest mode of primary and/or of backup operations.

The physical containment of the PFN will be detailed further with the application specific variations of the proprietary protective wall and structure. Also the security protocols for the two basic secure signal conditioning for encrypted signals (DES and PGP) will be described and detailed as to how they will be implemented into this technology for government and commercial uses in high and medium security applications.

Finally, the three possible secure recorded memories for data storage make this accountable protected remote control technology an ideal fit for any and all security applications. It is especially well adapted for the specialized environments that demand restricted or limited access due to the hazards they pose to human health and or for protection from hostile forces anywhere around the world. The secure PFN and system can help identify problems, analyze situations and witness or even supply evidential data as proof for legal and/or public opinion of an event and all related actions. This can be accomplished from a multitude of audio and video angles and further substantiated from other recovered data sources that are timed and dated in a synchronized record. The final option can provide for aggressive remote control actions, if so warranted, and necessary to eradicate most threats in real-time or very near real-time if so prescribed, designed and needed. The technology exists for this scenario within all the related applications if deemed necessary and warranted.

This number 5 abstract

6375618-01400

Abstract

This application also details an accountable modular and programmable software termed TRAC that authorizes and authenticates commands from wireless and land line telephone and or RF equipment and or light transmission technologies to remotely activate and confirm automated controls and functions through processors controllers and or computers. As TRAC processes this data in a secure manner it stores it in a protected storage on board a piece of equipment in this technology's PFN on location and in the two way transmission PFNs it reports back to at least one remote location a redundant memory storage.

This TRAC system was designed to distribute communicated commands to their appropriate application specific preprogrammed protocols while authenticating the authorizations and preserving and accountable record on both sides of the remote control communication scenario and through out any redundant transmissions or data storage. The TRAC system of software has been designed to develop a Trusted Remote Activity Controller for all of societies needs regarding accountability and liability as well as to preserve an organize secure modalities to mange and control automated equipment, and financial legal transactions.

With the advance in electronics, communications and computer processors the automation of equipment is rapidly aggressive remote control and robotics and needs to be made as accountable as the owners and operators who have been solely responsible for machine control in the past. Because, control responsibility will be shared at first between man and machine and might very well always be this way; accurate telemetry of both will be essential to provide organization and proper management and legal control in this scenario. This technology's PFN protected primary focal node and The TRAC software system has been constructed to provide the means to accomplish these control and accountability tasks and to serve as an electrical interface, physical platform, and software control center to write standards to

Abstract 4 25 COMBINED FINAL

This application has been developed to advance this technology's Protected

Primary Focal Node PFN, which is a secure accountable electrical interface platform of communications, memory storage, management and controls on every machine, equipment, vehicle and or any management or control application that requires accountability; into a cost effective high security convertible system for extremely aggressive functions including military operations and policing in hostile areas. This application also re-introduces for an earlier filing a software program called TRAC which stands for Trusted Remote Activity Controller. This program has been developed as an accountable operating system for Public Safety, National Security in normal everyday use of aggressive remote and automated control and management. The sub security system responsible for accountable security is termed FACT for Federal Access Control Technology . FACT is software run in each PFN /TRAC system on every piece of equipment and is linked by every communication medium to a gateway system that is responsively connected to The National FACT Registry. The National FACT Registry is responsible to all governing agencies and their software protocols in the approved use of all equipment and their components in use as well as their impact on the environment, and society's infrastructure e.g. functions are to (to approve, activate and tax equipment and components as well as retrieve essential data assess and value all machine and resource use as well as monitor PFN inventory and react in a constitutional manner). In providing these secure accountable services TRAC software also supports CEW which are commercial encryption products on the Web like (bank card transactions and other payment industry products like NCR.) and provides the hardware devices to process and complete these activities. The PFN/TRAC system is designed to be a modular and programmable device of software and firmware supported by any composite and or all types of hardware, components devices connectables and interfaces from proprietary innovations to commercial off the shelf (COTS) products, but all made accountable on location and in the remote registry and structured by law, rules regulations codes and standards. This is the PFN/TRAC Invention. Accountability for aggressive remote and automated control and management scenarios involving man and machine and or total robotics.

SECRET - 01390

details an accountable modular and programmable software termed TRAC that authorizes and authenticates commands from wireless and land line telephone and or RF equipment and or light transmission technologies to remotely activate and confirm automated controls and functions through processors controllers and or computers. As TRAC processes this data in a secure manner it stores it in a protected storage on board a piece of equipment in this technology's PFN on location and in the two way transmission PFNs it reports back to at least one remote location a redundant memory storage.

This TRAC system was designed to distribute communicated commands to their appropriate application specific preprogrammed protocols while authenticating the authorizations and preserving and accountable record on both sides of the remote control communication scenario and through out any redundant transmissions or data storage. The TRAC system of software has been designed to develop a Trusted Remote Activity Controller for all of societies needs regarding accountability and liability as well as to preserve an organize secure modalities to mange and control automated equipment, and financial legal transactions.

With the advance in electronics, communications and computer processors the automation of equipment is rapidly aggressive remote control and robotics and needs to be made as accountable as the owners and operators who have been solely responsible for machine control in the past. Because, control responsibility will be shared at first between man and machine and might very well always be this way; accurate telemetry of both will be essential to provide organization and proper management and legal control in this scenario. This technology's PFN protected primary focal node and The TRAC software system has been constructed to provide the means to accomplish these control and accountability tasks and to serve as an electrical interface, physical platform, and software control center to write standards to.

CONFIDENTIAL

XX

Thought junk pile

THIS IS THE 14 FIGURE FROM PRO-5 AND MUST BE REVIEWED FOR THE FINAL FIGURE 13

This is a self-explanatory chart to show the accountable data storage for on board in the PFN and off board within the monitoring and remote control system. This chart can be referred to when reading and viewing figures 3-4-5 & 6 with all the different types of communications detailed. The chart will quickly provide the basic report back properties and data storage systems to expect form an individual PFN by the communication service it is employing.

Figure 13 is a interior block diagram as to how a card swipe or card swipe cell phone would be connected to one of the billing box or PFN computers and would then process the magnetic data stored on a card through the software provided by the card swipe manufacturers, as well as any credit card company proprietary security software used by the PFN computer. An electronic signal with a preprogrammed dial up number to a credit card approval service company with any proprietary software to process the data in the remote location would be partially and or either held on the card or in the PFN software package depending on the type of cards and devices chosen to complete this remote billing and payment procedure, e.g., smart cards vs. regular cards, etc.

This data because, in most cases will require a radio transmission should be sent as an encrypted algorithm to protect against any criminal hackers pirating legitimate credit card information out of the airways. Most credit card strip reader manufacturers design them to meet standards and protocols such as ISO 7811, 7811/1-6 and or comply with DMV format for driver licenses. They are also all CE, FCC, UL, CUL certified. These devices were all discussed earlier in the devices that could be interfaced with the PFN's as peripherals section of this application to provide mobile remote services.

It is important to understand this mobile paying function of the billing box currently shown in figure 8 as a add on devices for cabs, Limousines, automated rental equipment and vehicles, etc. is only the after market version of the PFN's total function

FOR THE

to provide a means to pay for equipment use and any and all services surrounding vehicle and equipment use commercially. This card swipe is another peripheral that will be on all manufacture vehicles in time as part of any PFN's to allow for a vehicle \ equipment operator to pay for any use fees, uncontested tickets, or to log driver license information, and or pay energy fees immediately, rather than having to stop the vehicle to stay current monetarily for use of the vehicle or services. They can card swipe at any time, either while taking on any energy provisions or at any convenient time in the comfort of their vehicle out of the elements while using the equipment / vehicle simultaneously.

As was mentioned earlier personal identification equipment e.g., fingerprinting, papillary ID, voice recognition, pin number from key \ number pad, ID transmission bracelets, etc used as either additional ID conformation peripheral systems or a future primary personal ID credit device component to a remote or PFN personal credit data storage accounting system will be connected and interfaced in the same manner as illustrated in figure 3a. Or these systems will employ any of the interface technology shown in figure 7 . In the case of the transmission bracelets of course the on board PFN universal RF receiver section will receive the signal and have a serial data conditioning of the signal encoder or this will be a function of the PFN computer processor and software through a special IC decoder \ encoder card part of the computer hardware.

Also for security the transmitted data will be recorded in the PFN memory systems e.g., hard drives, buffers or flash memory devices or MO drives or CD write drives, etc. as well as any remote location credit data management and storage system. Accompanying the credit data and amount request will be the ESNVIN number of the sending PFN along with time date and locator coordinates for the billing, charging , ticketing and acceptance of as well as any acceptance criterion for these transactions. e.g. electronic signature or hard copies generated by on board printers etc. which are turned in with a transfer of memory at the end of a shift or use of a vehicle or service

In drawing 13 1302 is a cell phone that can either be inside the billing box or outside and only electronically connected. 1302 here is out fitted with a card swipe slot that can read the magnet IC strip of a credit card or a driver ID, etc. There are two electrical connection shown coming from the special cell phone 1320 and 1321. 1320 goes to a PCMCIA modem to support data communication by a cellular phone for the PFN computer. (these actual connectors can be serial RS232 connections or IC cards

configured into the PFN computer hardware mother board, Euro-board or done with edge ribbon connectors etc. 1321 illustrates a direct connection if the special cellular phone is already out fitted for data delivery in its circuitry and therefore would connect directly with the computers RS232 with a mere cable or utilize the new 1394 universal bus system or utilize any connection to handle TTL or the standard serial port PS2. For this multi tasking phone to both send and receive data through the cellular system and to process the digital data retrieved from the magnetic strip a function switch will send a firmware stored signal to the PFN to process and store the card swipe data in it's hard drive if on board or in it's processor buffer to be retrieved and sent via the PCMCIA modem to the cell phone and to the remote location. As stated earlier this function could be manually contrived with the button first processing and then in another position sending it as data through the cellular protocol. Or this data could be performed through soft ware commands stored on the card and PFN or even in the cell phones firmware e.g. D-WAVE phone protocol from Sony and its multitasking capability out fitted with a card swipe. 1301 is a plain card swipe possibly one of the ACETEK series mentioned earlier as this invention's experimental prototype products. It connects directly to the PFN computer either serial PS2, RS232, or simple transistor to transistor logic TTL. 1306a merely depicts these interface options as well as shows the special cellular phone could supply its card data in this manner in one modality. 1311 is a PFN computer and is one ideally with at least a 386 processor as was described in the processor and computer section of the PFN's described earlier. 1311 would also be programmed with all the necessary and proprietary software to complete these security billing procedures. In the lower left corner of 1311 is a small square with the letter [B] this stands for buffer or hard drive in the PFN computer.

The number 1319 has lines that go to the little square [B] on 1311 and to the horizontal square to the left. The horizontal memory square is additional memory to keep a record of credit tans action most probably done with Sony memory sticks, how ever any of the memory systems described could be utilized and then erased by the proper procedures after any reasonable tie had past on questionable charge entries.

1323 with a lighting symbol signifies a wireless cellular signal conditioning device for data transmission to and from PC's. [PCMCIA] in a square. 1313 is a two way data modulator for any RF transmitters, receivers, or transmitters, used to down load data from the PFN or in this case the card swipe protocol to a remote location or

gateway, etc. 1314 is a two way Motorola reflex protocol to down load data to a remote location. (this would involve PFN software that could break up the data into 20 bit segments and transmit the data to a remote location that could reconstitute any lengthy multiple transmission into a complete secure text transmission if it is determined necessary to develop a secure algorithmic protocol for credit card data transfers. However Motorola is very protective of these transmission signal protocols already and this might prove a secure system if practically capable of handling the quantity of data in any commercial transaction.

All these different data communication pathways `are being discussed presently for the use of the card swipe billing to demonstrate the connectability of all the previously described peripherals and to demonstrate to anyone skilled in the art the ease, feasibility, practicality and obvious reasonable development of this inventions interfaces to organize and control the process to combine all types of communication e.g. wireless, and land based, into a protected focal center that is capable of processing and controlling, recording reporting and billing for the use of equipment and related services in an accountable modality or protocol.

1322 is a new product that adds so much to ease interfacing of cellular technology to the PFN and that is why it is mentioned here directly . It is a complete data hook up of modem transceiver and antenna with a PCMCIA III connectability to any of the PFN computers. The last square is a standard telephone data modem for computer data transfer, the little circled (H) stands for hard wired to land phone lines; and is listed hear to demonstrate that the PFN will be used with stationary equipment as well as mobile equipment and vehicles to value use and service related to use as well . 1318 shows the connectability of all these data conditioning and transmission devices described above and in figure 7 and within this application and all related applications. 1318 also shows that the memory 1319 will store any crucial down loaded data to a remote location on board the PFN as well.

FIG 1

MONITORING AND CONTROL SYSTEM FOR PFN'S

DATA BASE CONNECTION OR WWW.

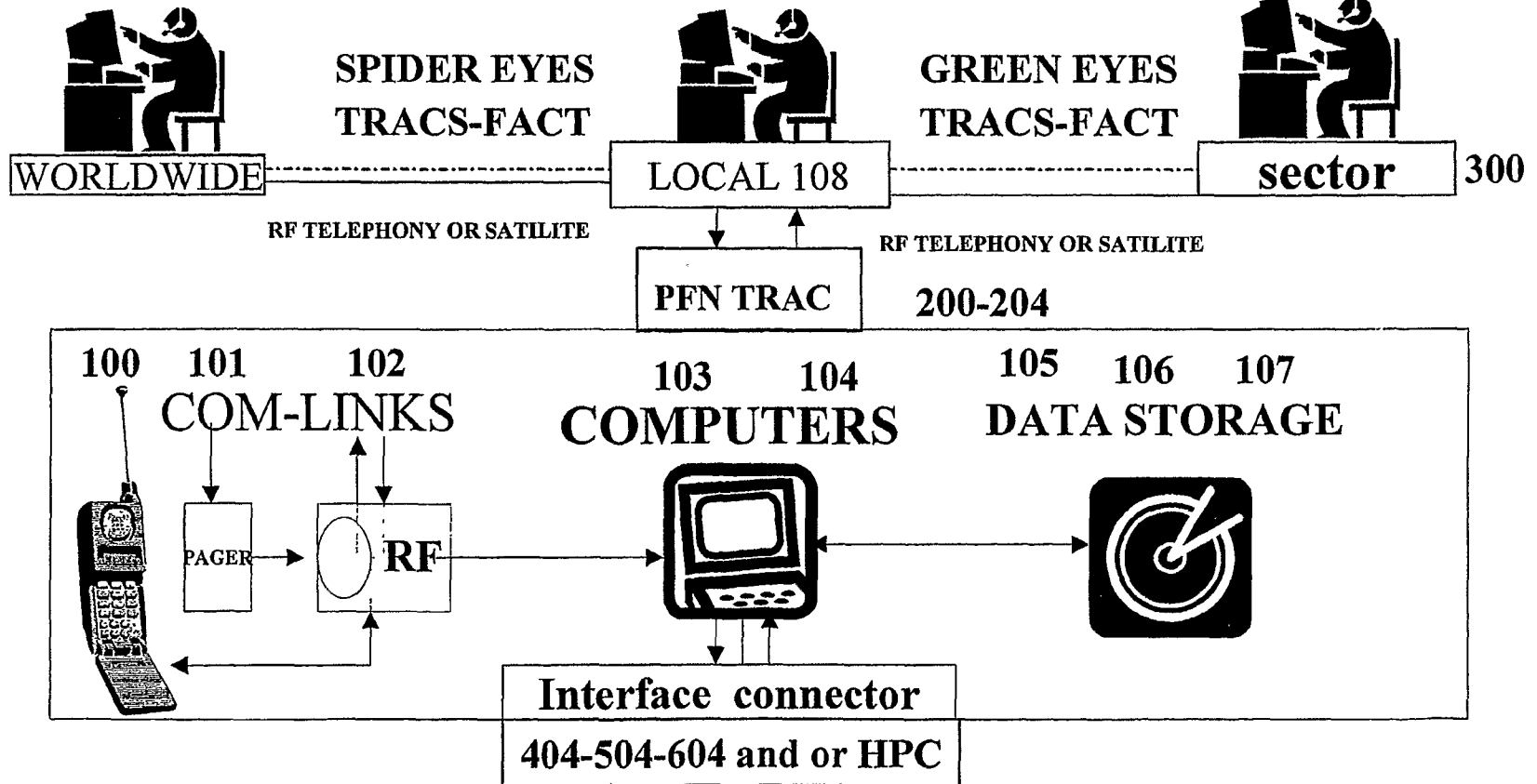


FIG 1A

TRAC

Trusted Remote Activity Controller

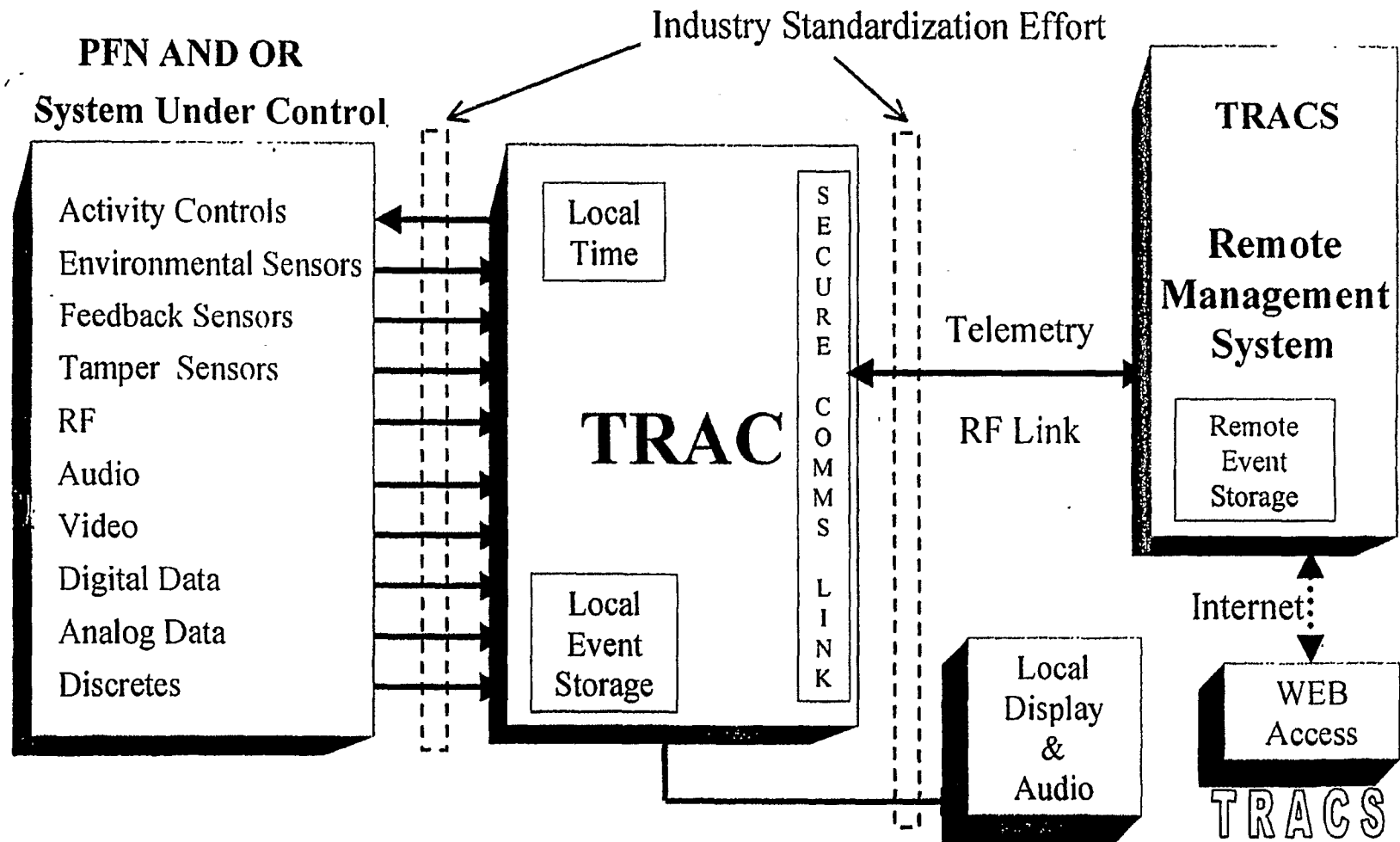


FIG 2

Application specific wall structures for PFNs

NOTE: THIS APPLICATION SPECIFIC WALL STRUCTURE DEALS WITH EXTREME ENVIRONMENTS OTHER WALL STRUCTURES WILL BE ADJUSTED TO MEET ANY APPROPRIATE NEED TO SECURE MEMORY AND COMPONENTS

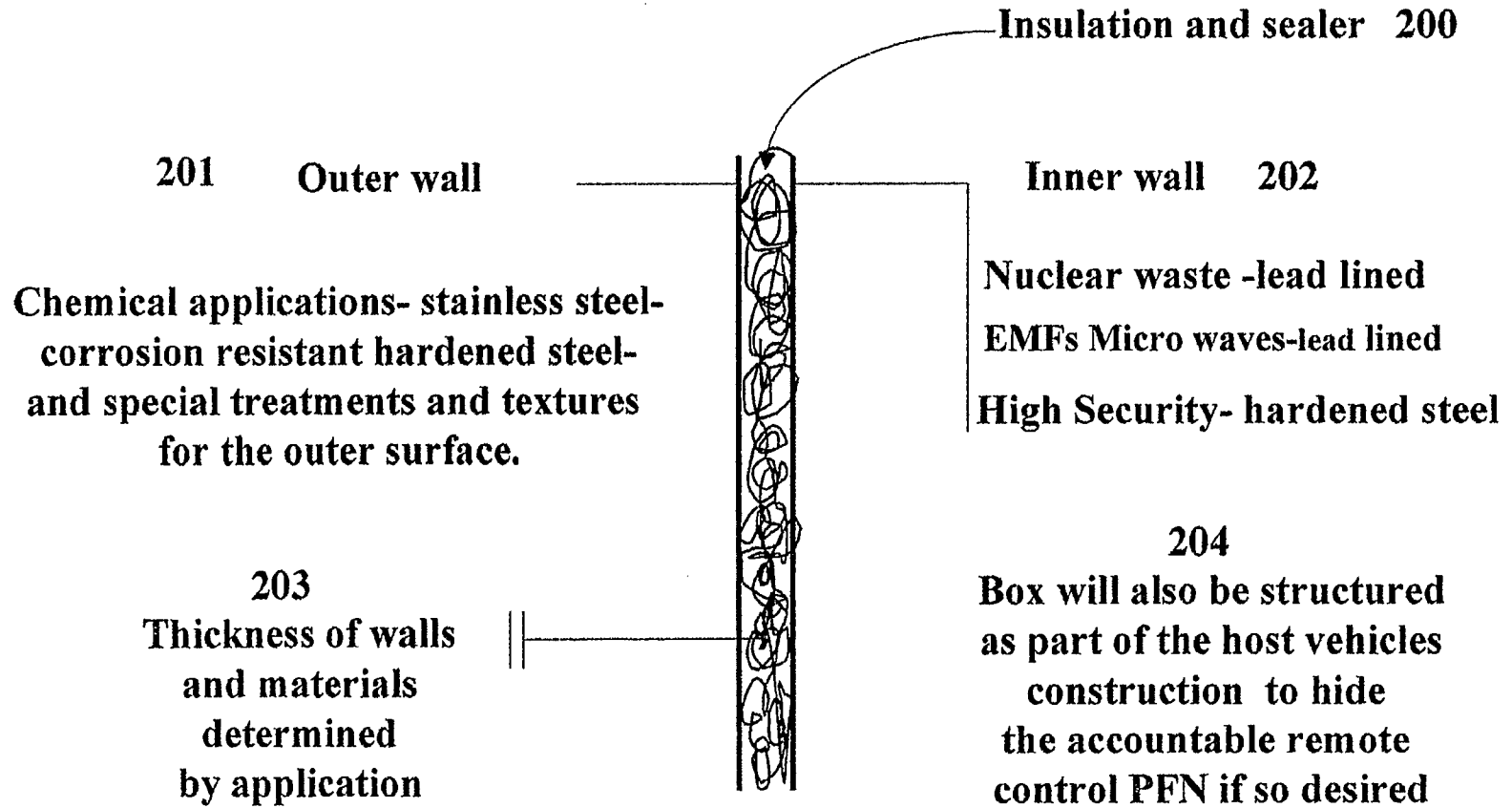


FIG 2A

006FTD BT892F05

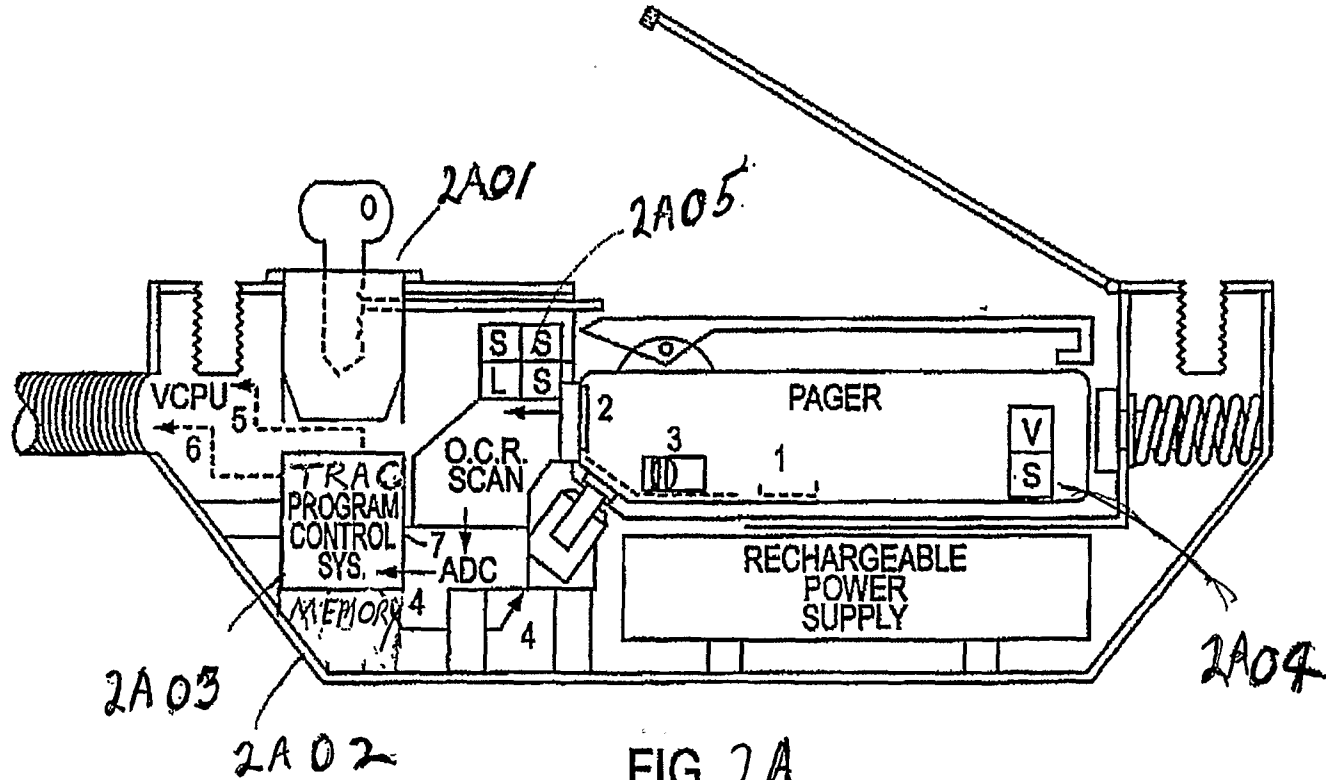


FIG. 2A

FIG 2B

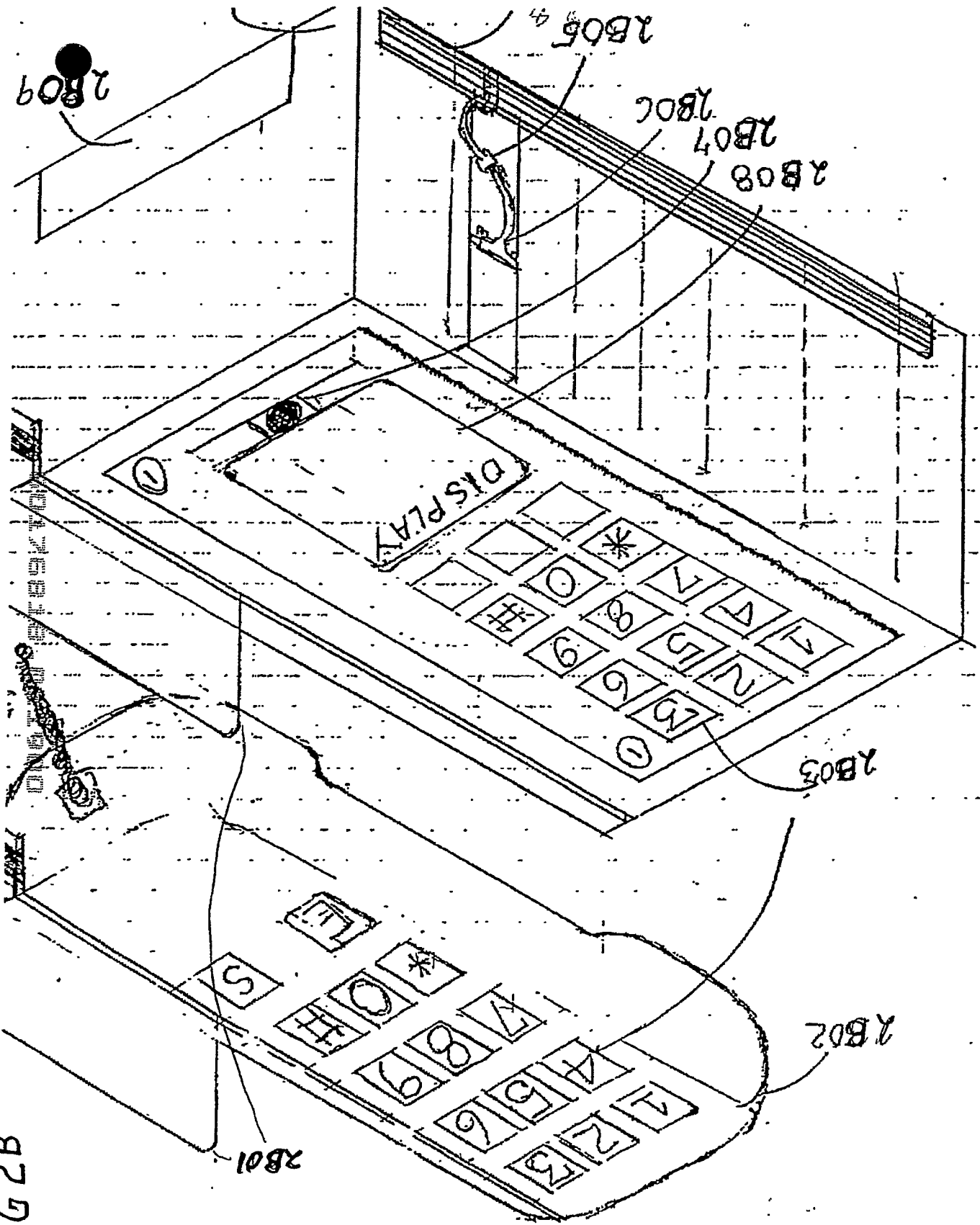
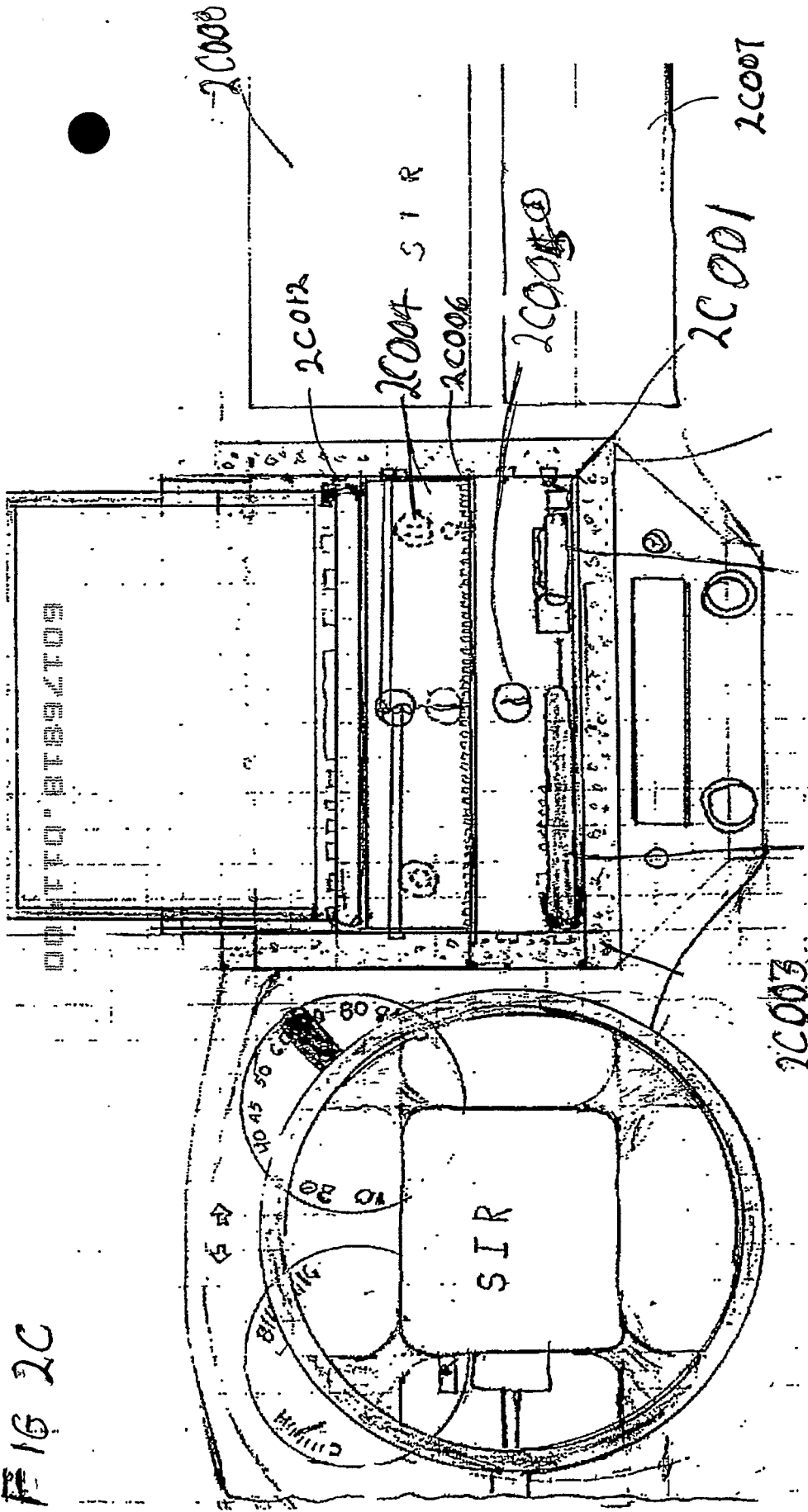


FIG 2C



2C000

2C012

2C004 SIR

2C006

2C005

2C001

2C007

2C003

PFN AND DASH MOUNT
INTERFACE SECURE BOX

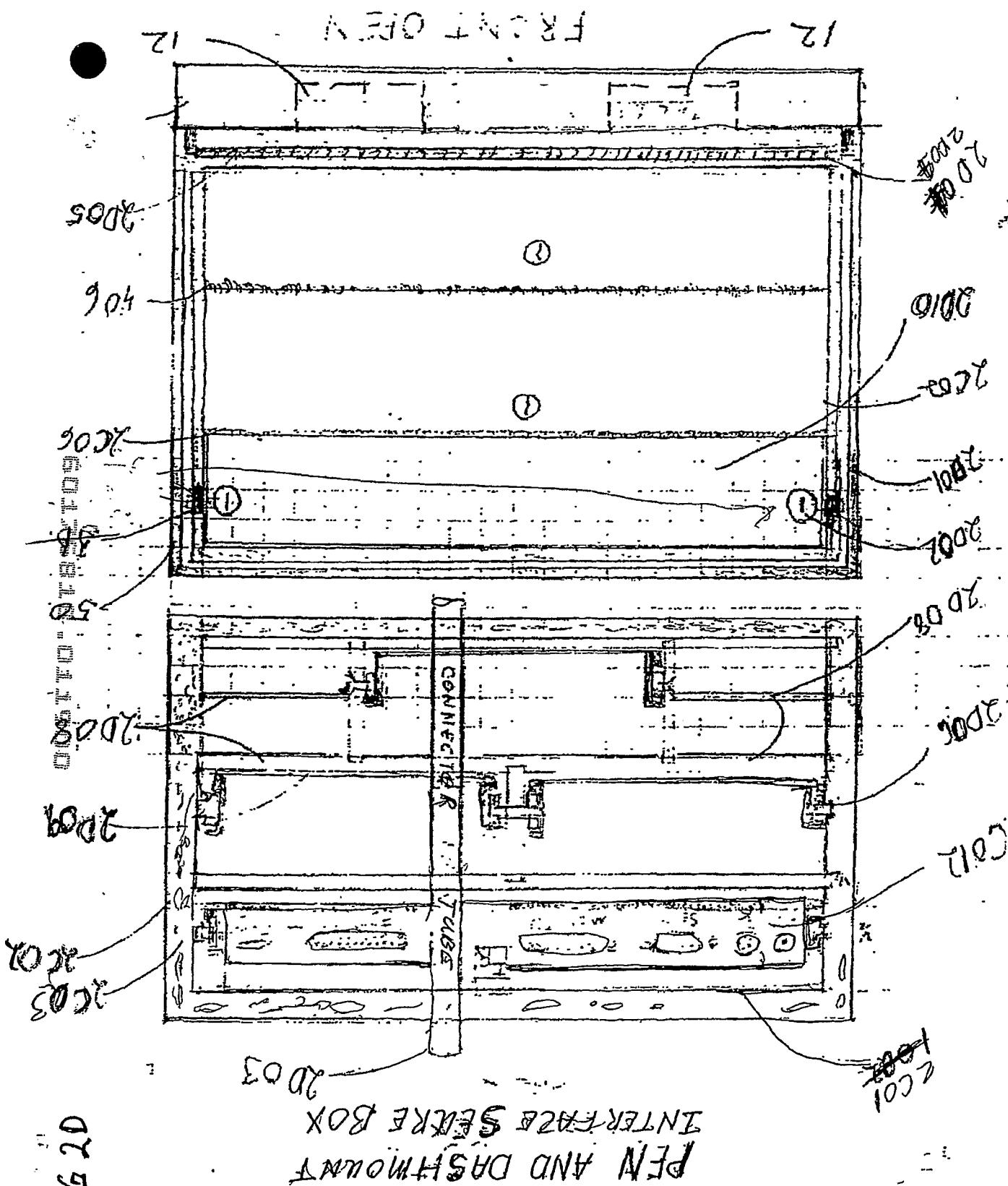
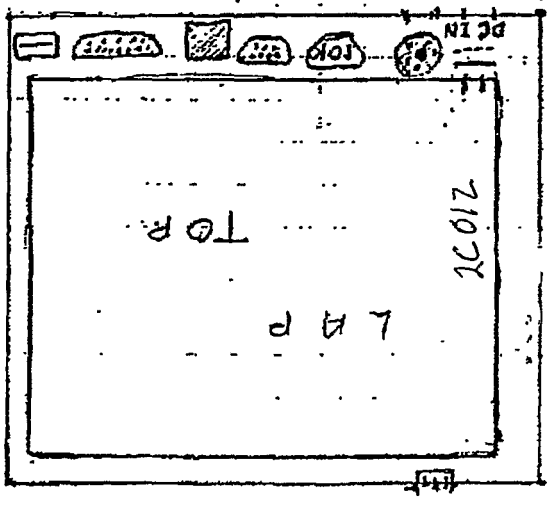


FIG 20

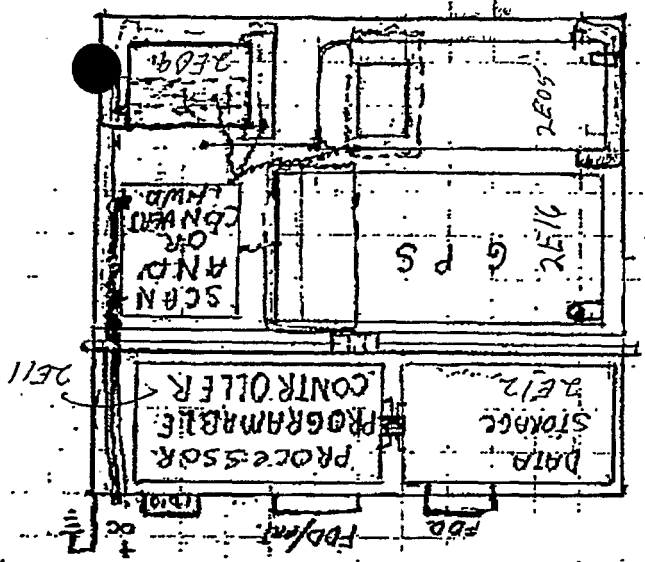
PEN AND DASHMOUNT
INTERFACE SECURE BOX

PEN AND DASH MOUNT
OF SECURITY BOX

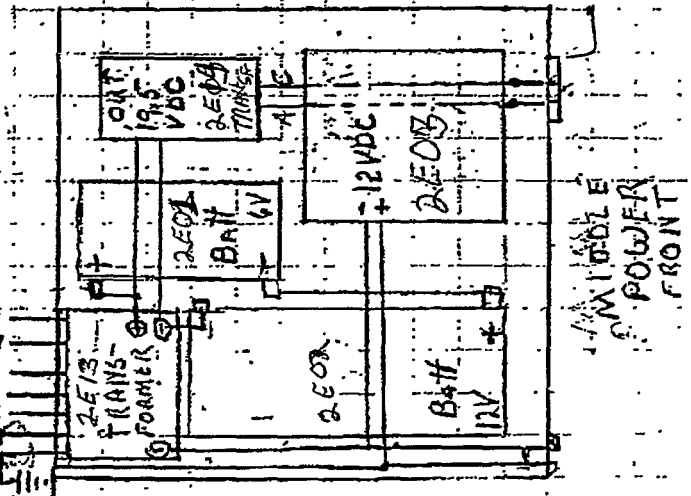
FIG. 2E



TO P
LAP TOPS
PALM TOPS
ORGANIZERS
PERSONEL ITEMS



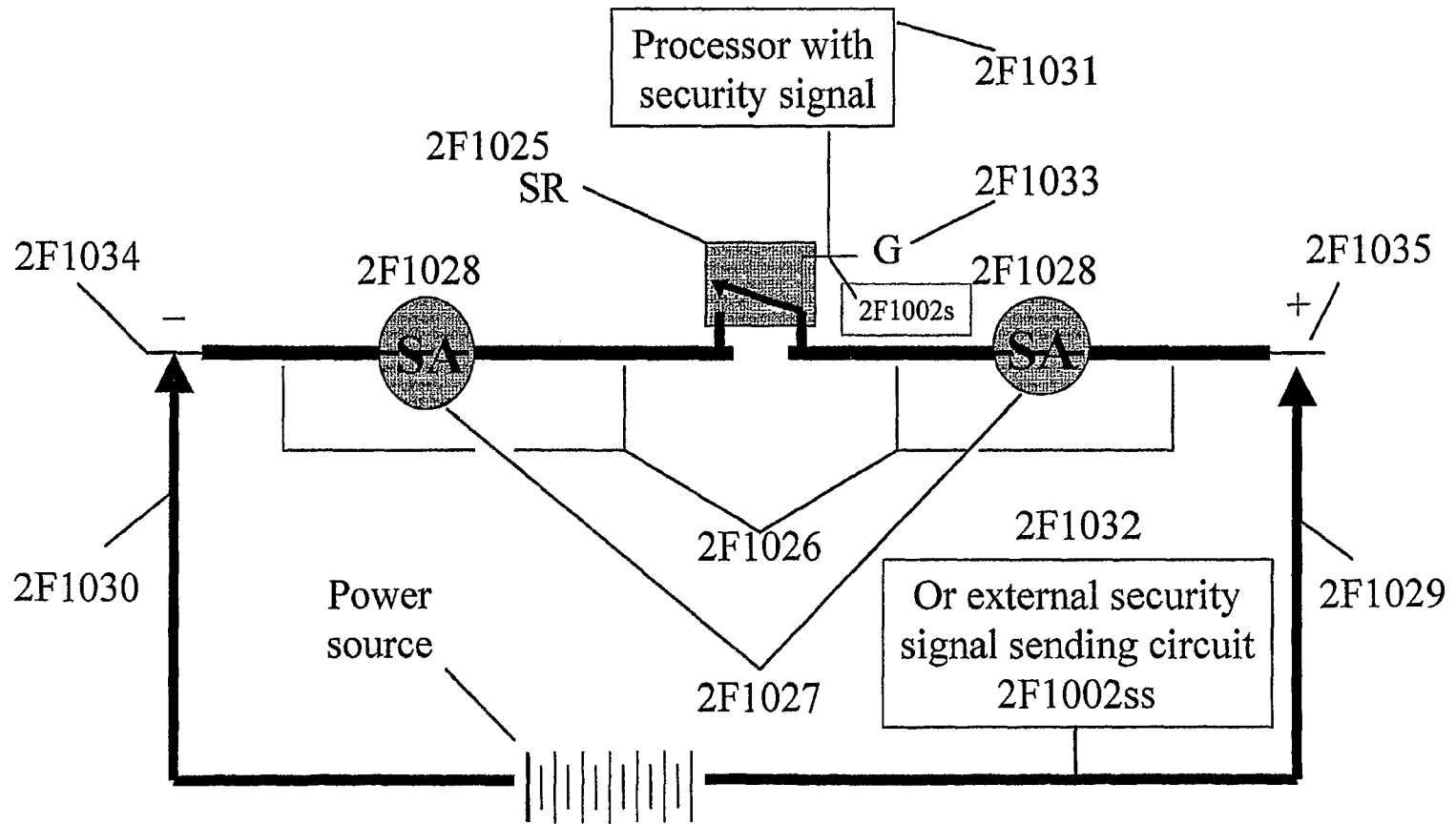
BROD DRAWER
OTHER RADIO
EQUIPMENT



AVAILABLE
POWER
FRONT

Electronic Security Seal

FIG. 2F



Security Sealed Area For The PFN

FIG.2G

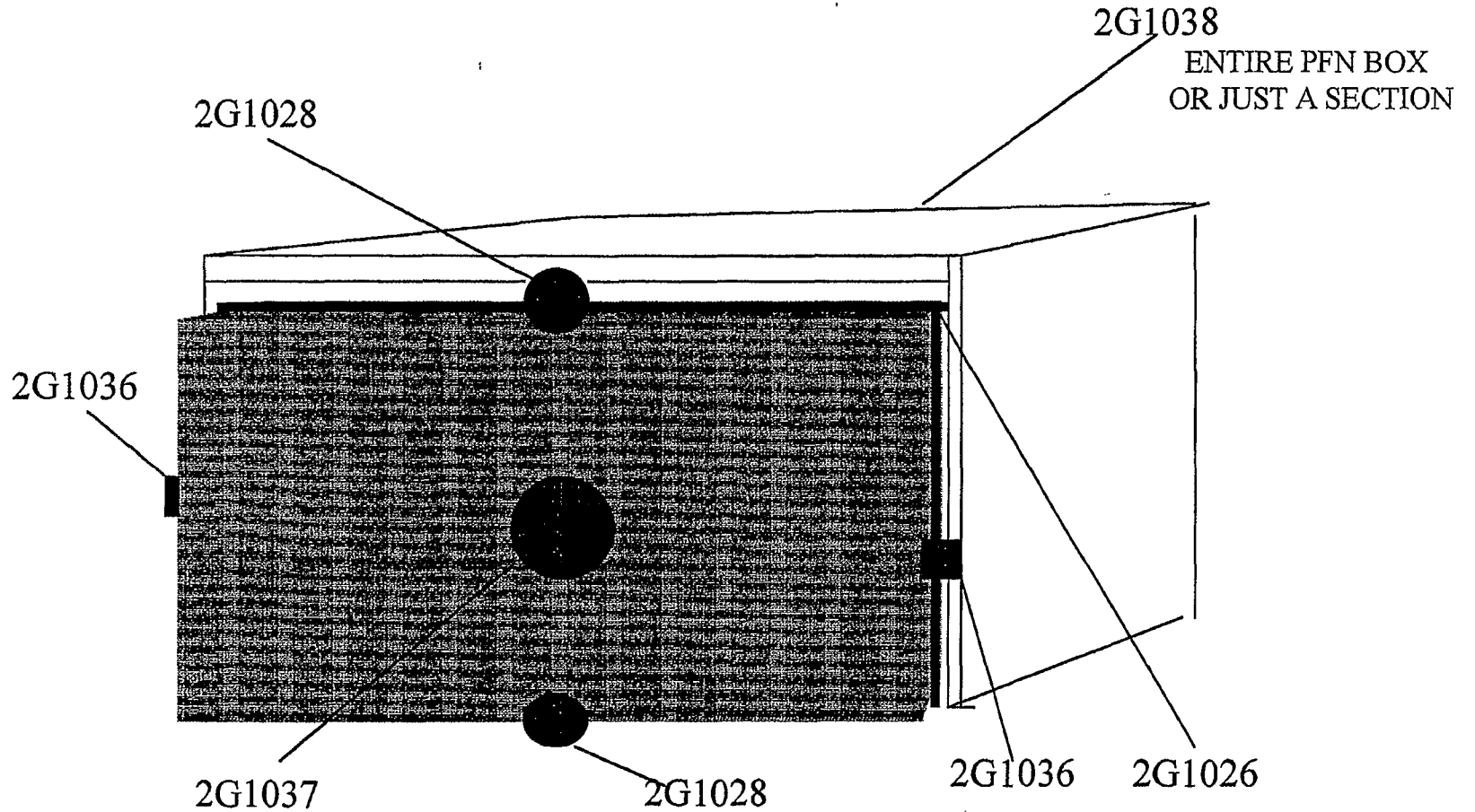


FIG 3

One and Two Way PFN's

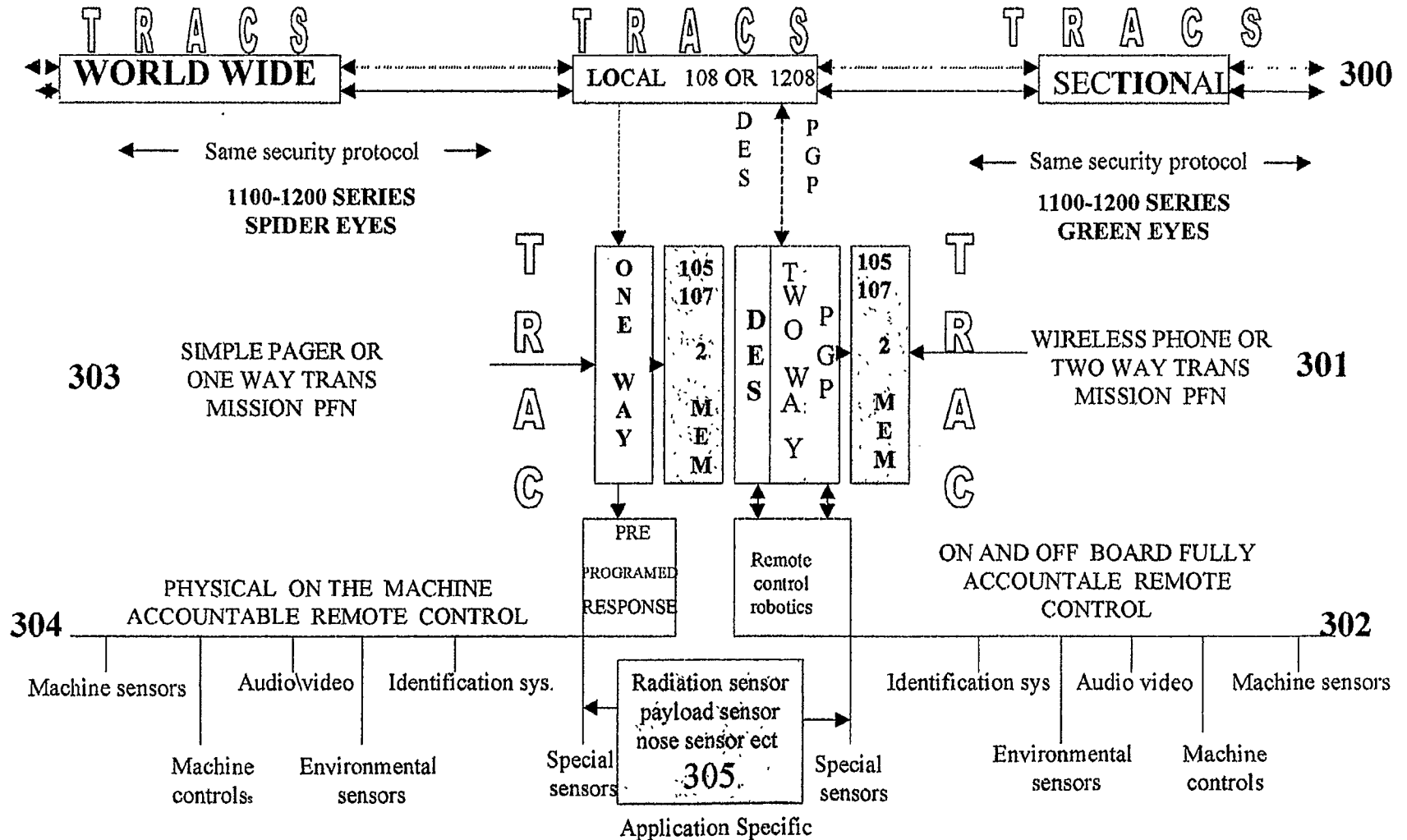


FIG 3A

PFN DATA STORAGE PROPERTIES

COMMUNICATION	AUDIO VIDEO	MACHINE CONTROL AND TELEMETRY	PERSONEL TELEMETRY	ENV. TELEMETRY
1 WAY PAGE	R-O	R-O	R-O	R-O
1 WAY RF SIGNAL	R-O	R-O	R-O	R-O
2 WAY PAGE	R-O-r-RR mc	R-O-r-RR-mc	R-O-r-RR-mc	R-O-r-RR-m
PHONE	R-O-r-RR	R-O-r-RR	R-O-r-RR	R-O-r-RR
2 WAY RF SIGNAL	R-O-r-RR	R-O-r-RR	R-O-r-RR	R-O-r-RR
CORDLESS PHONES	R-O-r-RR-LD	R-O-r-RR-LD	R-O-r-RR-LD	R-O-r-RR-LD
SHORT RANGE RF SIG.	R-O-r-RR-LD	R-O-r-RR-LD	R-O-r-RR-LD	

RECORD = R REPORT = r ONBOARD = O REMOTE RECORD = RR
 MINIMUM CAPACITY = mc
 LIMITED DISTANCE = LD

FIG 4

ACCOUNTABLE COST EFFECTIVE SECURE PFN
REMOTE CONTROL IN ONE WAY APPLICATIONS

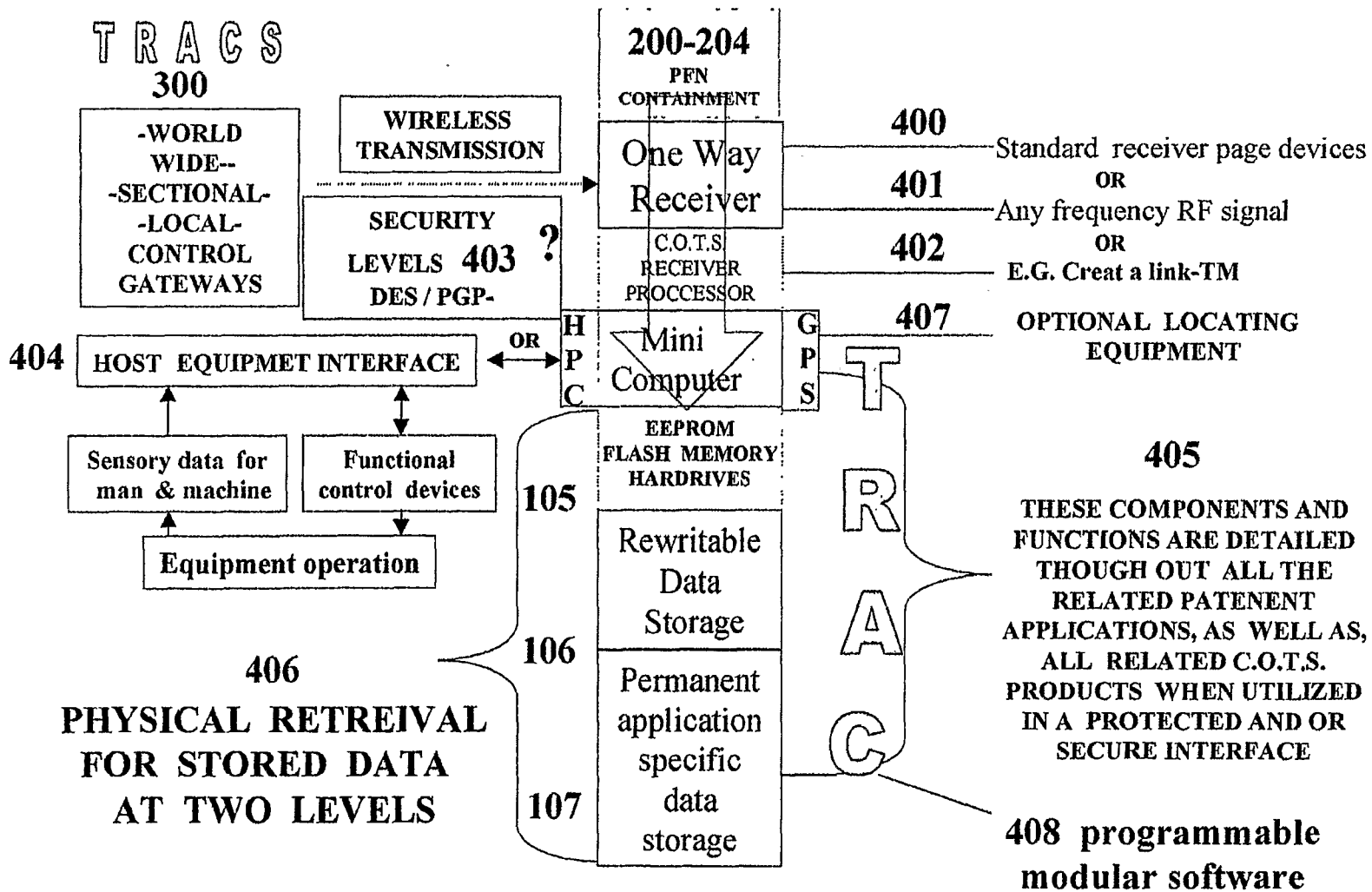


FIG 5

ACCOUNTABLE COST EFFECTIVE SECURE PFN
REMOTE CONTROL IN TWO WAY APPLICATIONS

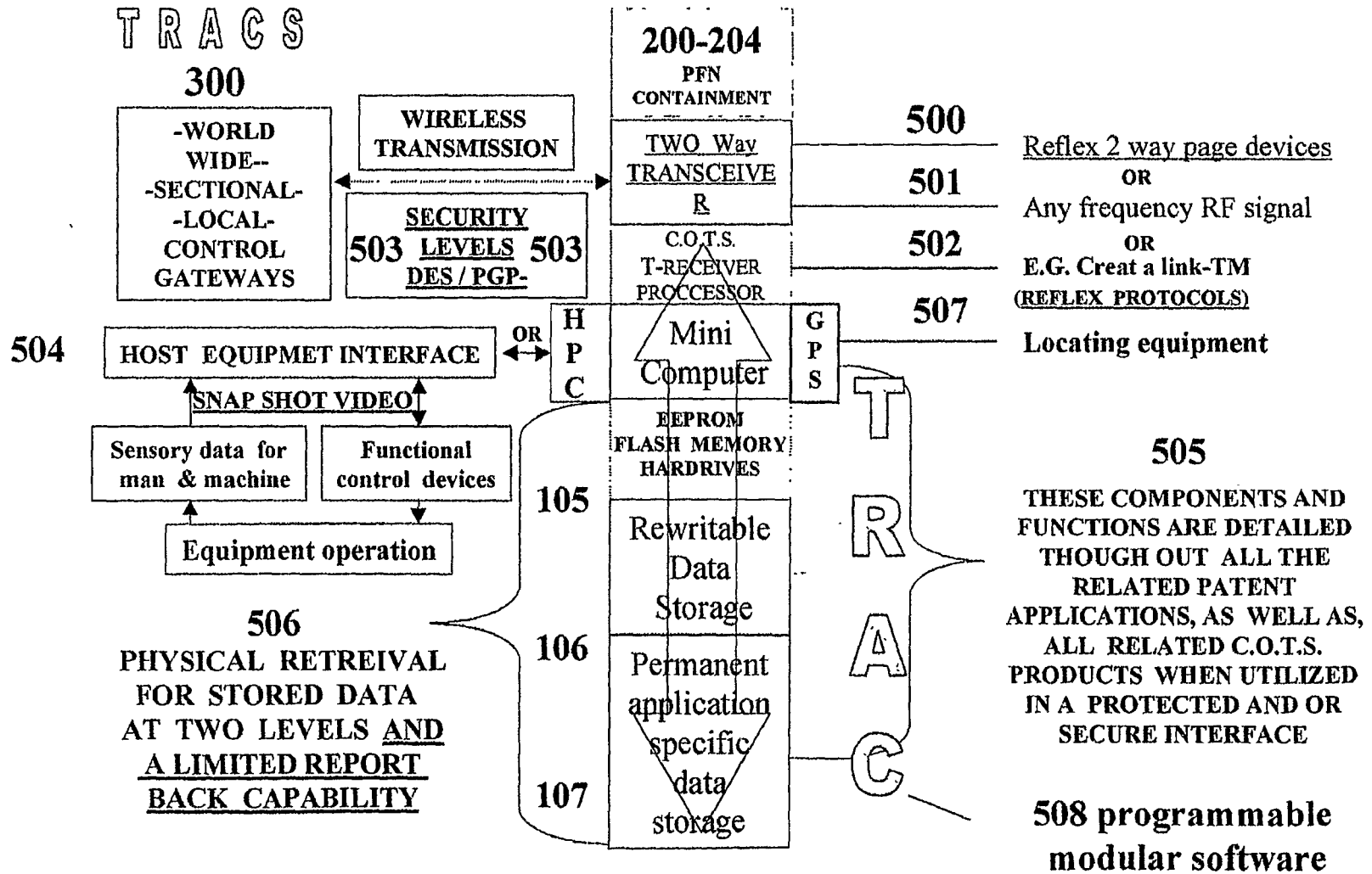


FIG 6

SOPHISTICATED SECURE PFN
REMOTE CONTROL WITH TWO WAY APPLICATIONS

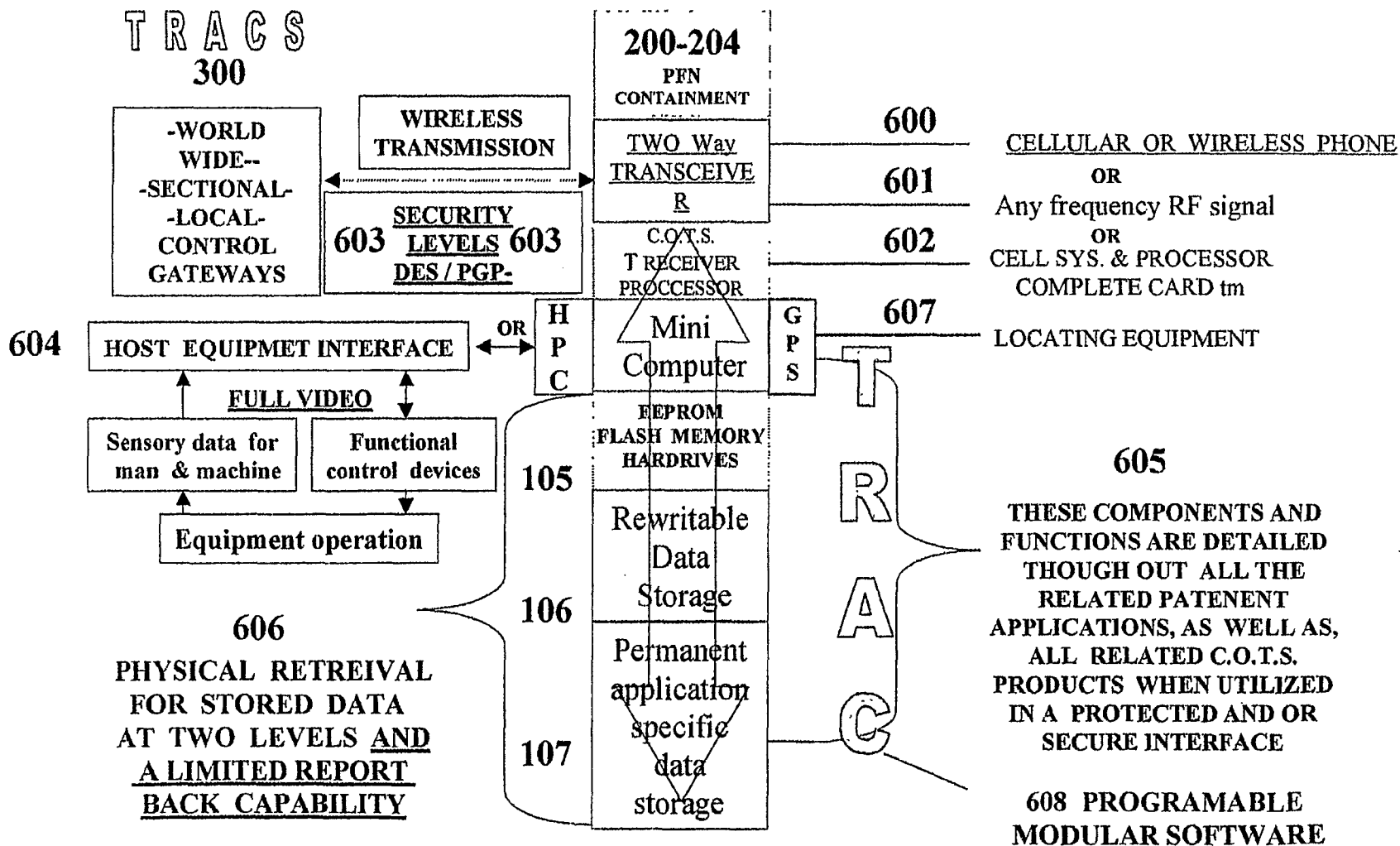


Fig 6 a

PRESENT TO FUTURE PROTECTED PRIMARY FOCAL NODE CONSOLIDATIONS

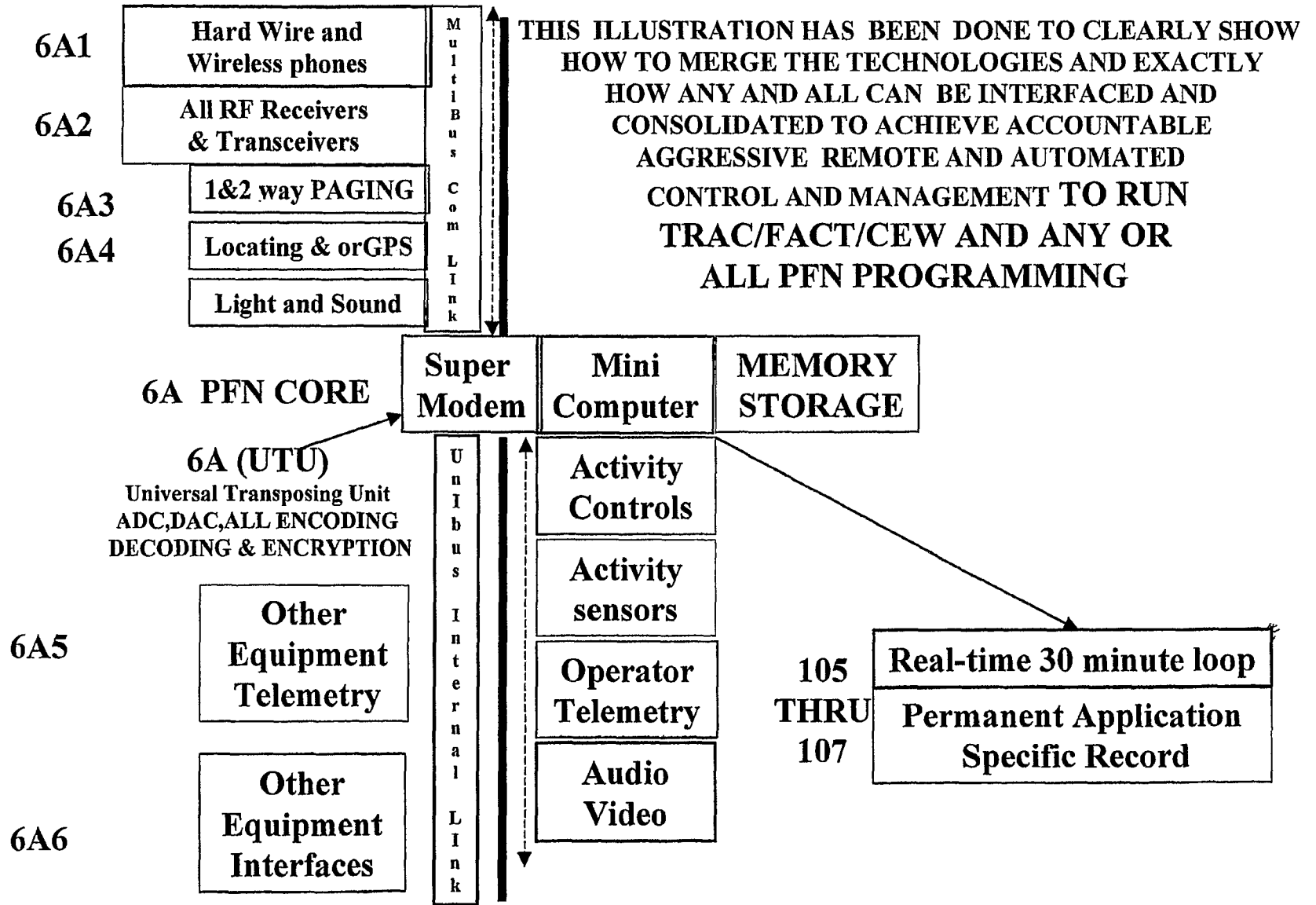


FIG 7

HAZARDOUS ENVIRONMENTAL USES OF PFN'S

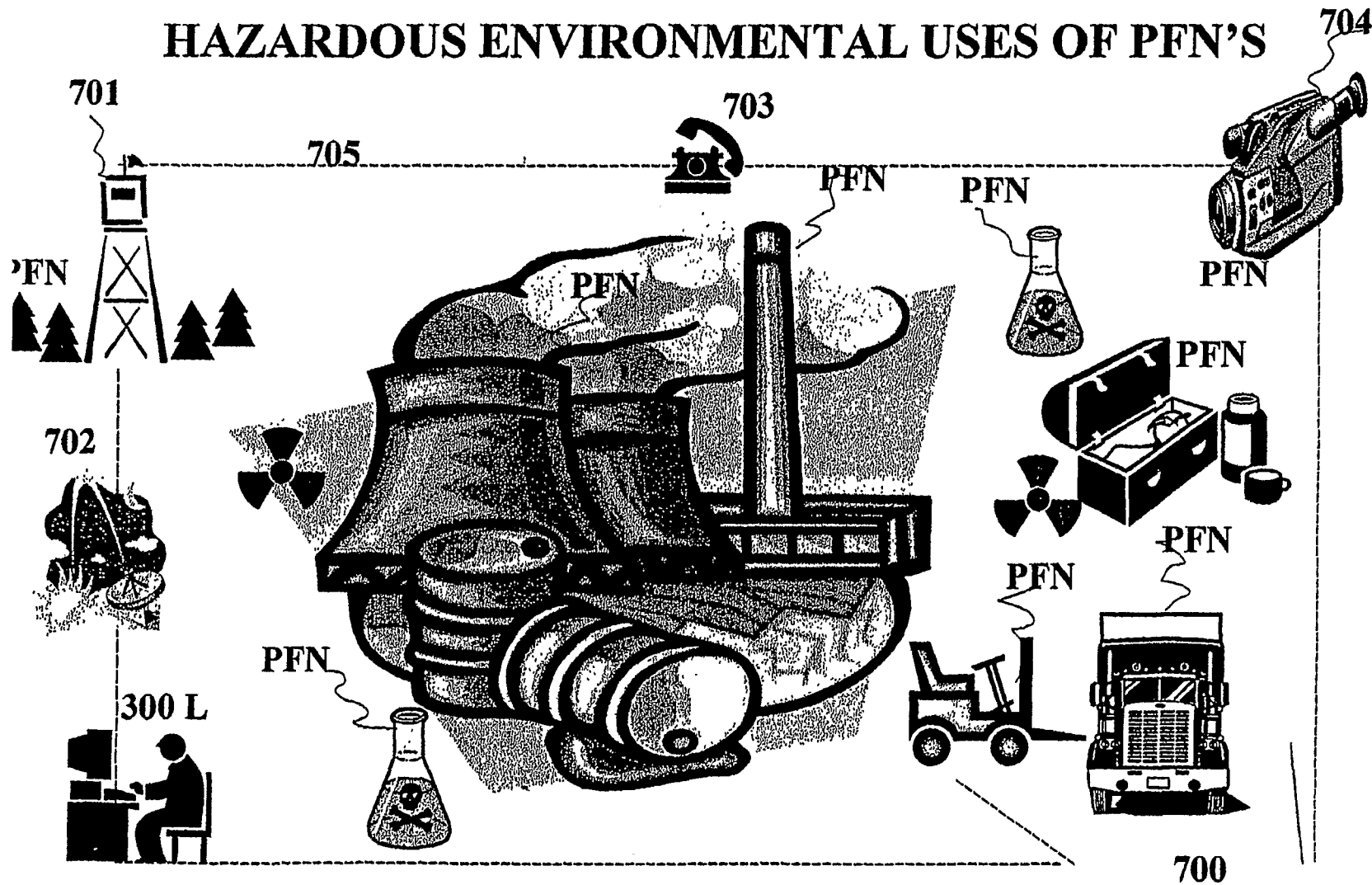
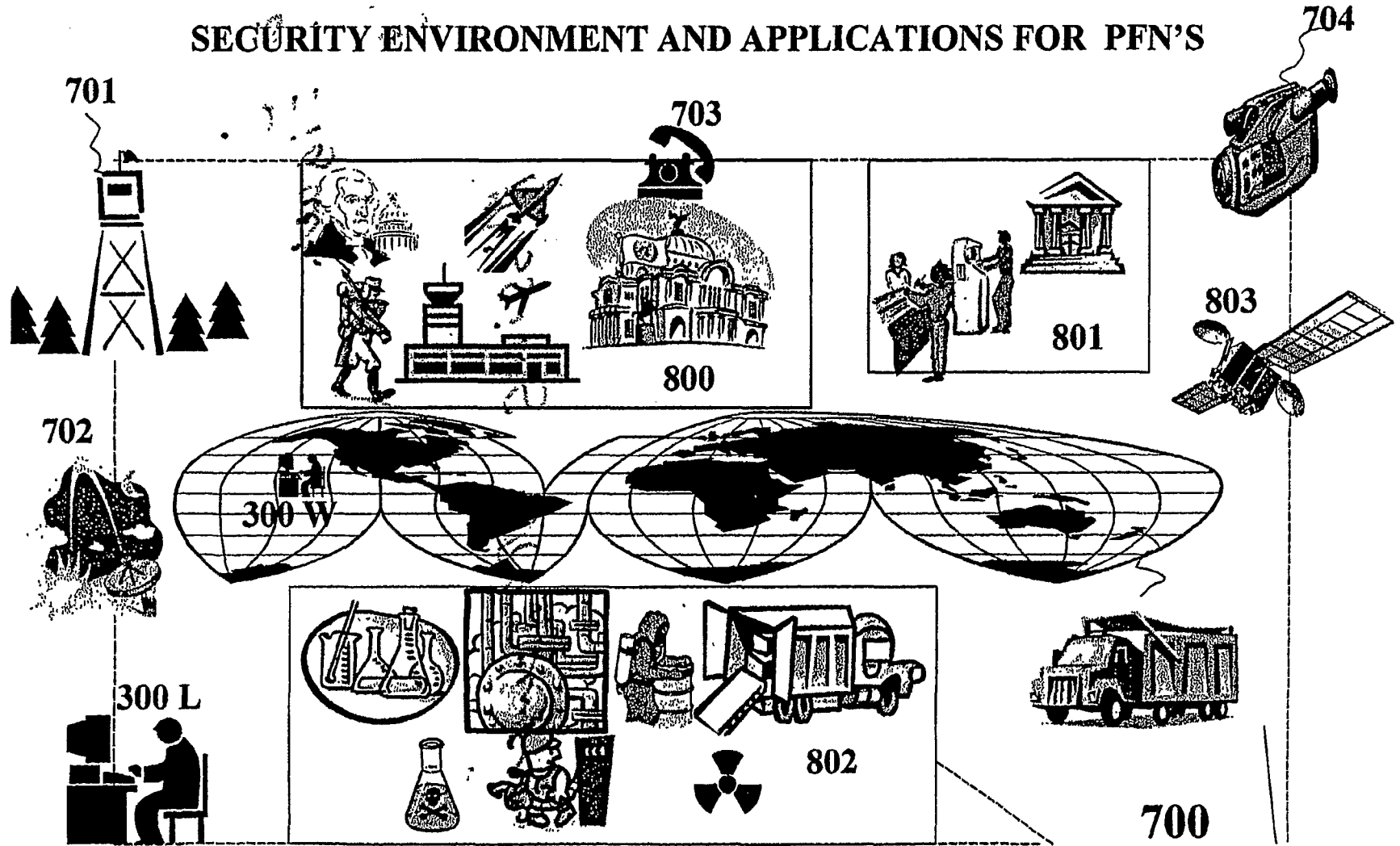


FIG 8

SECURITY ENVIRONMENT AND APPLICATIONS FOR PFN'S



Frequency Allocation Table

Freq. Range (MHz)	Radio Service	Freq. Range (MHz)	Radio Service
0.090 - 0.110	Radio Navigation - Maritime	13.360 - 13.410	Fixed - Radio Astronomy
0.110 - 0.130	Fixed - Maritime - Radiolocation	13.410 - 13.600	Fixed & Mobile
0.130 - 0.160	Fixed - Maritime	13.600 - 13.800	Broadcasting
0.160 - 0.190	Fixed	13.800 - 14.000	Fixed & Mobile
0.190 - 0.285	Aeronautical - Radionavigation	14.000 - 14.250	Amateur 20 Meter Band
0.285 - 0.325	Maritime & Aeronautical Radionavigation	14.350 - 14.990	Fixed & Mobile
0.325 - 0.335	Aeronautical & Maritime Radionavigation	15.000	WWV Time Standard
0.335 - 0.405	Aeronautical Radionavigation	15.010 - 15.100	Aeronautical Mobile
0.045 - 0.415	Radionavigation	15.100 - 15.600	Broadcasting
0.415 - 0.495	Maritime	15.600 - 16.360	Fixed
0.500	Distress & Calling	16.360 - 17.410	Maritime Mobile
0.505 - 0.510	Maritime	17.410 - 17.550	Fixed
0.510 - 0.525	Aeronautical, Radionavigation	17.550 - 17.900	Broadcasting
0.525 - 0.535	Broadcasting - Aero. Radionavigation	17.900 - 18.030	Aeronautical Mobile
0.530	Travelers Information	18.030 - 18.068	Fixed
0.535 - 1.625	Broadcasting	18.068 - 18.168	Amateur 17 Meter Band
1.610	Travelers Information	18.168 - 18.780	Fixed
1.625 - 1.705	Broadcasting - Fixed - Mobile	18.780 - 18.900	Maritime Mobile
1.705 - 1.800	Fixed - Aeronautical, Radionavigation	18.900 - 19.680	Fixed
1.800 - 1.850	Amateur 160 Meter Band	19.680 - 19.800	Maritime Mobile
1.850 - 2.000	Amateur - Radionavigation - Fixed & Mobile	19.800 - 19.990	Fixed
2.000 - 2.650	Fixed & Mobile	20.000	WWV Time Standard
2.065 - 2.107	Maritime Mobile	20.010 - 21.000	Fixed & Mobile
2.107 - 2.170	Fixed & Mobile	21.000 - 21.450	Amateur 15 Meter Band
2.170 - 2.1735	Maritime Mobile	21.450 - 21.850	Broadcasting
2.1735 - 2.2905	Mobile (Distress)	21.850 - 21.870	Fixed
2.182	Distress & Calling	21.870 - 21.924	Aeronautical Fixed
2.194 - 2.300	Fixed - Mobile	21.924 - 22.000	Aeronautical Mobile
2.300 - 2.495	Fixed - Mobile - Broadcasting	22.000 - 22.855	Maritime Mobile
2.500	WWV Time Signal	22.855 - 23.000	Fixed
2.505 - 2.850	Fixed & Mobile	22.000 - 23.200	Fixed & Mobile
2.855 - 3.025	Aeronautical Mobile	23.200 - 23.350	Aeronautical Fixed & Mobile
3.025 - 3.029	Search & Rescue	23.350 - 24.000	Fixed & Mobile
3.115 - 3.220	Fixed & Mobile	24.000 - 24.890	Fixed - Land Mobile
3.200 - 3.400	Fixed & Mobile - Broadcasting	24.890 - 24.990	Amateur 12 Meter Band
3.400 - 3.500	Aeronautical Mobile	25.000 - 25.000	WWV Time Standard
3.500 - 3.750	Amateur 80 Meter Band	25.010 - 25.320	Petroleum Radio Service
3.750 - 4.000	Amateur 75 M - Fixed & Mobile	25.330 - 25.600	U.S. Government
4.000 - 4.063	Fixed - Maritime Mobile	25.600 - 26.470	Broadcast/Broadcast Aux.
4.063 - 4.438	Maritime Mobile	26.480 - 26.960	U.S. Government
4.125	Distress & Safety	26.965 - 27.405	Citizens Radio Service
4.438 - 4.650	Fixed & Mobile	27.430 - 27.530	Business Radio Service
4.650 - 4.750	Aeronautical Mobile	27.540 - 28.000	U.S. Government
4.750 - 4.850	Fixed & Mobile - Broadcasting	28.000 - 29.700	Amateur 10 Meter Band
4.850 - 4.995	Fixed & Land Mobile - Broadcasting	29.700 - 29.600	Forest Products Radio Service
5.000	WWV Time Standard	29.800 - 29.690	Fixed Services
5.005 - 5.060	Fixed - Broadcasting	29.890 - 29.910	U.S. Government
5.060 - 5.450	Fixed - Mobile	29.910 - 30.000	Fixed Services
5.450 - 5.730	Aeronautical	30.000 - 30.580	U.S. Government
5.680	Search & Rescue	30.580 - 30.640	Special Industrial Radio Service
5.730 - 5.950	Fixed & Mobile	30.660 - 30.820	Petroleum - Forest Products - Motor Carrier
5.950 - 6.200	Broadcasting	30.840 - 31.260	Business - Motor Carrier - Forestry-Conserv.
6.200 - 6.525	Maritime Mobile	31.280 - 31.980	Forestry Conservation - Special Industrial
6.525 - 6.765	Aeronautical Mobile	32.000 - 33.000	U.S. Government
6.765 - 7.000	Fixed	33.020 - 33.160	Highway Maint. - Special Emerg. - Business
7.000 - 7.300	Amateur 40 Meter Band	33.180 - 33.380	Petroleum Radio Service
7.300 - 8.100	Fixed & Land Mobile	33.400	Business Radio Service
8.100 - 8.195	Fixed - Maritime Mobile	33.420 - 33.980	Fire Radio Service
8.195 - 8.815	Maritime Mobile	34.000 - 35.000	U.S. Government
8.364	Search & Rescue	35.020 - 35.180	Business Radio Service
8.815 - 9.040	Aeronautical Mobile	35.160 - 35.160	Telephone Maintenance Radio Service
9.040 - 9.500	Fixed	35.200 - 35.520	Paging - Special Industrial
9.500 - 9.900	Broadcasting	35.540 - 35.680	Paging
9.900 - 9.995	Fixed	35.700 - 35.720	Business Radio Service
10.000	WWV Time Standard	35.740 - 35.880	Special Industrial Radio Service
10.005 - 10.100	Aeronautical Mobile	35.880 - 35.980	Business Radio Service
10.100 - 10.150	Fixed - Amateur 30 Meter	36.000 - 37.000	U. S. Government
10.150 - 11.175	Fixed & Mobile	37.020 - 37.420	Police - Local Government
11.175 - 11.400	Aeronautical Mobile	37.440	Forest Products Radio Service
11.400 - 11.650	Fixed	37.460 - 37.860	Power Radio Service
11.650 - 12.050	Broadcasting	37.880	Forest Products Radio Service
12.050 - 12.230	Fixed	37.900 - 37.980	Highway Maintenance - Special Emergency
12.230 - 13.200	Maritime Mobile	38.000 - 39.000	U.S. Government (Fixed & mobile)
13.200 - 13.360	Aeronautical Mobile	39.020 - 39.980	Police - Local Government

Copyright © 1999

FIG 10

Freq. Range (MHz)	Radio Service	Freq. Range (MHz)	Radio Service
40.000 - 42.000	U.S. Government	159.495 - 160.200	Motor Carrier Radio Service
42.020 - 42.940	Police (State Police)	160.215 - 161.595	Railroad Radio Service
42.960 - 43.000	Business Radio Service	161.600	International Marine Band
43.020 - 43.180	Special Industrial Radio Service	161.640 - 161.760	Remote Broadcast Pickup
43.180 - 43.160	Telephone Maintenance (mobile units)	161.800 - 162.000	Marine Telephone
43.200 - 43.520	Paging - Special Industrial	162.000 - 174.000	U.S. Government (fixed & mobile)
43.540 - 43.680	Paging	163.250	Special Emergency (Paging)
43.700 - 44.600	Motor Carrier Radio Service	166.250	Remote Broadcast Pickup
44.620 - 45.040	Police - Forestry Conservation	170.150	Remote Broadcast Pickup
45.060 - 45.640	Police - Local Government	173.225 - 173.375	Relay Press - Forest Products - Petroleum
45.660 - 45.860	Police - Highway Maintenance	174.000 - 216.000	Broadcasting - T.V. Ch. 7 Through 13
45.880	Fire (intersystem)	216.000 - 220.000	U.S. Government (telemetry) - Marine
45.900 - 46.040	Police - Special Emergency	220.000 - 222.000	Private Land Mobile Services
46.060 - 46.500	Fire Radio Service	222.000 - 225.000	Amateur 1 1/4 Meter Band
46.520 - 46.580	Local Government Radio Service	225.000 - 400.000	U.S. Government (military aeronautical)
46.600 - 47.000	U.S. Government - Part 15 devices	400.000 - 406.100	Satellite - Meteorological
47.020 - 47.400	Highway Maintenance	406.100 - 420.000	U.S. Government (fixed & mobile)
47.420 - 47.680	Special Emergency - Special Industrial	420.000 - 450.000	Amateur 70 CM Band
47.700 - 48.540	Power Radio Service	450.000 - 451.000	Remote Broadcast Pickup
48.560 - 49.500	Forest Products - Petroleum Radio Service	451.025 - 451.150	Power Radio Service
49.520 - 49.580	Forest Products - Special Industrial	451.175 - 451.750	Power - Petroleum - Forest Products - Mfgs.
49.600 - 50.000	U.S. Government - Part 15 devices	451.775 - 452.025	Special Industrial Radio Service
50.000 - 54.000	Amateur 6 Meter Band	452.050 - 452.300	Taxi - Forest Products
54.000 - 72.000	Broadcasting (T.V. Ch. 2-3-4)	452.325 - 452.500	Taxi - Forest Prod. - Motor Carr. - R.R.
72.000 - 73.000	Fixed & Portable	452.525 - 452.800	Auto Emergency Radio Service
73.000 - 74.600	Radio Astronomy	452.625 - 452.950	Motor Carrier - Railroad
74.600 - 75.400	Aeronautical Navigation	452.975 - 453.000	Relay Press Radio Service
75.400 - 76.000	Fixed & Portable	453.025 - 453.975	Police - Local Govt. - Hwy. Maint. - Fire
76.000 - 108.000	Broadcasting (T.V. Ch. 5-6 & F.M.)	454.000	Petroleum (oilspill clean-up)
108.000 - 118.000	Aeronautical Navigation	454.025 - 454.350	Radio Common Carrier
118.000 - 137.000	Aeronautical	454.375 - 454.975	Mobile telephone
137.000 - 138.000	Meteorological Satellite	455.000 - 456.000	Remote Broadcast Pickup
138.000 - 144.000	U.S. Government	456.000 - 460.000	Mobile units 5 mhz above repeater output
144.000 - 146.000	Amateur 2 Meter Band	460.025 - 460.550	Police Radio Service
146.000 - 149.900	U.S. Government	460.575 - 460.825	Fire Radio Service
149.900 - 150.050	Radio Navigation - Satellite	460.650 - 462.175	Business Radio Service
150.050 - 150.800	U.S. Government	462.200 - 462.450	Manufacturers Radio Service
150.815 - 150.965	Auto Emergency Radio Service	462.475 - 462.525	Mfg. - Power - Tel. Maint. - Forest Prod.
150.980	Petroleum (oilspill clean-up)	462.550 - 462.725	General Mobile Radio Service (GMRS)
150.995 - 151.130	Highway Maintenance Radio Service	462.750 - 462.925	Business Radio Service (Paging)
151.145 - 151.490	Forestry Conservation Radio Service	462.950 - 463.175	Special Emergency Radio Service
151.490 - 151.595	Special Industrial Radio Service	463.200 - 465.000	Business Radio Service
151.625 - 151.955	Business Radio Service	465.000 - 470.000	Mobile units 5 mhz above repeater output
151.985	Telephone Maintenance Radio Service	470.000 - 608.000	Broadcasting - (T.V. chs. 14-36)
152.0075	Special Emergency (Paging)	608.000 - 614.000	Radio Astronomy
152.030 - 152.240	Mobile Telephone - Paging	614.000 - 806.000	Broadcasting (T.V. chs 38-69)
152.270 - 152.480	Taxi - Business Radio Service	806.000 - 824.000	Private Land Mobile (Mobile Units)
152.510 - 152.810	Mobile Telephone - Paging	824.000 - 849.000	Cellular Telecommunications Serv. (Mobiles)
152.840	Paging	849.000 - 851.000	Aeronautical, Mobile Telephone
152.870 - 153.035	Sp. Indust.-Remote Broadcast-Motion Pict.	851.000 - 869.000	Private Land Mobile Service
153.035 - 153.395	Remote Pickup-Mfg-Forest Prods-Petroleum	869.000 - 894.000	Cellular Telecommunications Service
153.410 - 153.725	Power Radio Service	894.000 - 896.000	Aeronautical, Mobile Telephone
153.740 - 154.115	Fire - Local Government	896.000 - 901.000	Private Land Mobile Service (Mobile Units)
154.130 - 154.445	Fire Radio Service	901.000 - 902.000	Reserved for Future Use
154.460 - 154.690	Local Govt. - Power - Spec. Industrial	902.000 - 928.000	Amateur 23 CM Band - ISM - U.S. Government
154.515 - 154.625	Business - Forest Products	928.000 - 929.000	Private Fixed Service
154.650 - 154.950	Petroleum (Oilspill Clean Up)	929.000 - 932.000	Paging
154.965 - 155.145	Police Radio Service	932.000 - 935.000	Government - Non-Government Fixed
155.160 - 155.400	Local Government - Police	935.000 - 940.000	Private Land Mobile Service
155.415 - 155.700	Special Emergency - Police	940.000 - 941.000	Reserved for Future Use
155.715 - 158.030	Police Radio Service	941.000 - 944.000	Government - Non-Government Fixed
156.045 - 156.240	Local Government - Police	944.000 - 952.000	Broadcast Auxiliary - STL links
156.250 - 157.425	Highway Maintenance - Police	952.000 - 960.000	Private Fixed Service
157.450	International Marine band	960.000 - 1215.000	Aeronautical Navigation
157.470 - 157.515	Special Emergency (Paging)	1215.000 - 1240.000	Radiolocation
157.530 - 157.710	Auto Emergency Radio Service	1240.000 - 1300.000	Amateur 23 CM Band
157.740	Taxi (mobile units) - Business Radio Service		
157.770 - 158.070	Paging		
158.100	Mobile telephone (mobile units)		
158.130 - 158.265	Paging		
158.280 - 158.460	Power - Petroleum - Forest Products		
158.490 - 158.670	Petroleum - Forest Prod. - Manufacturers		
158.700	Mobile Telephone (mobile units)		
158.730 - 158.970	Paging		
158.985 - 159.210	Local Government - Police		
159.225 - 159.465	Highway Maintenance - Police		
159.480	Forestry Conservation Radio Service		
	Petroleum (oilspill clean-up)		

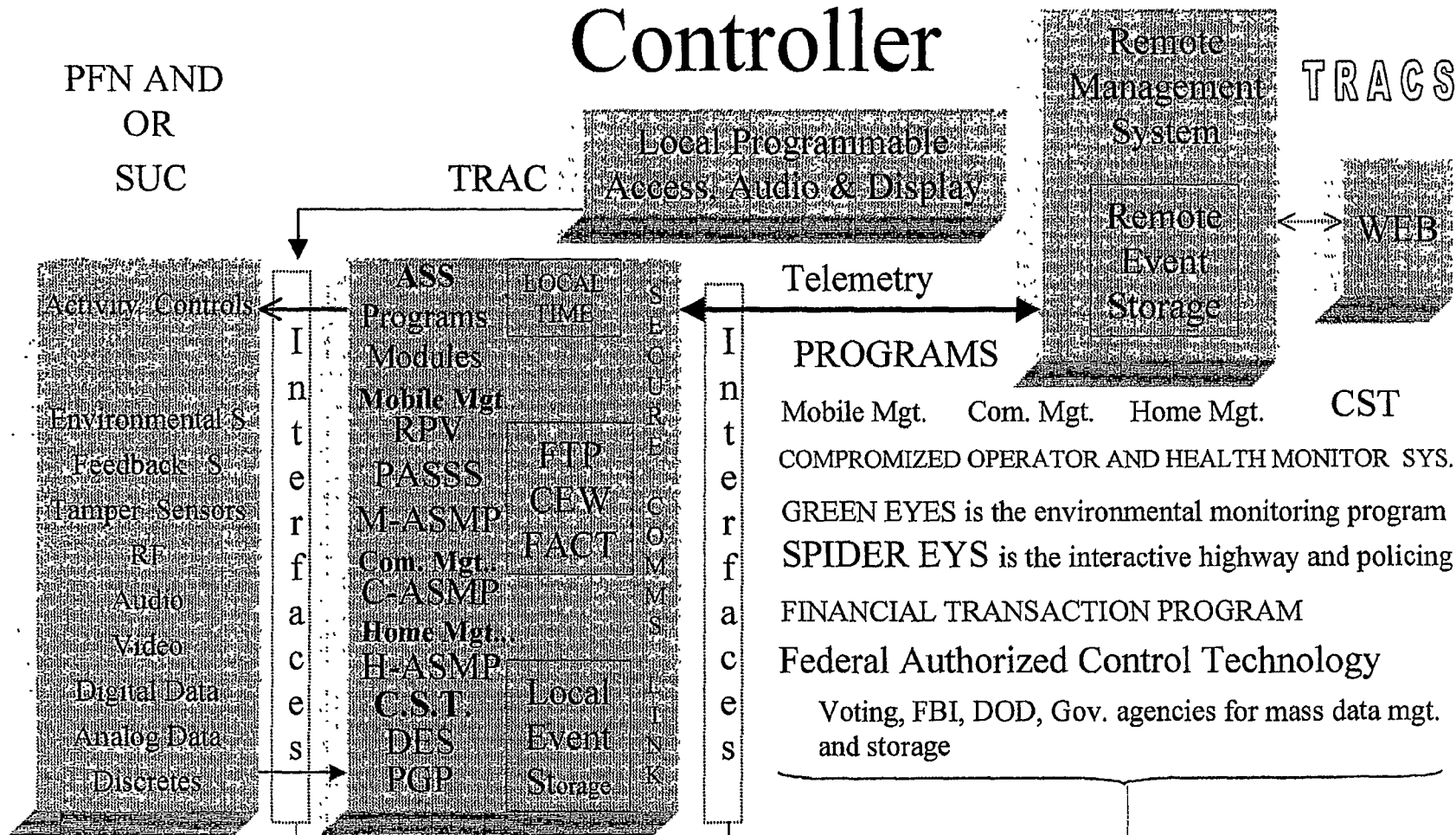
(Selected 5 MHz bands in the 470 - 512 MHz band are allocated for Land Mobile use in the ten largest urban areas of the country. Portions of the band from 420 to 430 MHz are allocated for land mobile use in Buffalo, Cleveland and Detroit. TV ch 17 (488 - 494 MHz) is available for Common Carrier Fixed use in Hawaii and channels 15 - 17 (478 - 494 MHz) for Common Carrier and Private Fixed service in the Gulf of Mexico.)

Copyright © 1990

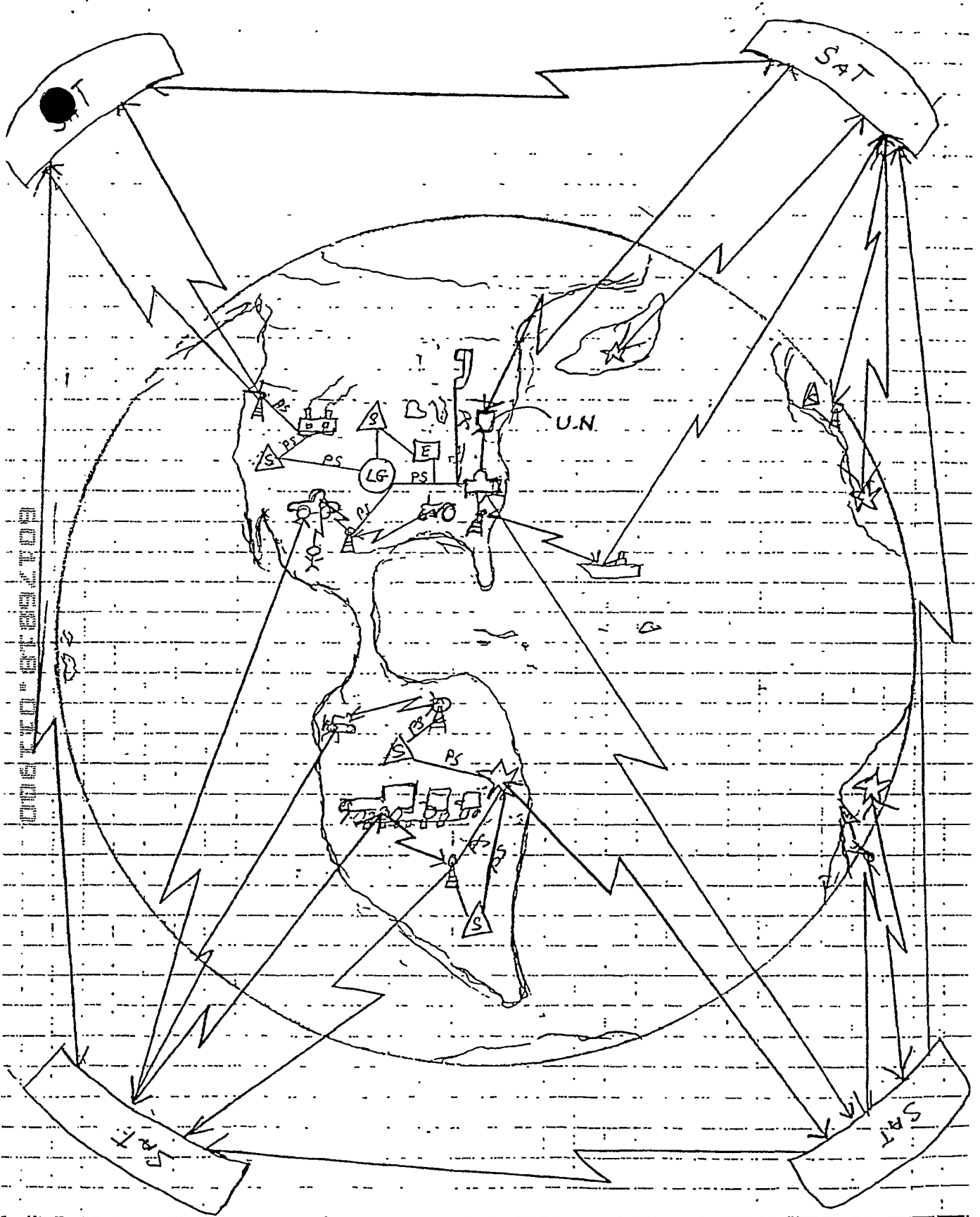
FIG 11

Trusted Remote Activity

Controller



Industry and Governmental Standardization and Legislation Effort



1613



LSU Libraries

U.S. Federal Government Agencies Directory

A List of Federal Agencies on the Internet

Read a [scope note](#) and see yesterday's [access stats](#).

View the [awards, honors, and recommendations](#) we have received.

Last updated Friday, 06-Nov-98 08:49:24 Send updates and corrections to Smittie Bolner (sbolner@lsu.edu).

[Keyword search](#) of Federal Agencies
(or use your browser's **Find** command)

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official
---------------------------	--------------------------	-----------------------------	-----------------------------	---	--------------------------------

Executive Branch

Executive Office of the President

- White House Office
- Office of the Vice President of the United States
- Office of the First Lady
- Council of Economic Advisers
- Council on Environmental Quality
- National Economic Council
- National Security Council
- Office of Administration
- Office of Management and Budget
- Office of National Drug Control Policy
- Office of Science and Technology Policy
- President's Council on Sustainable Development
- President's Foreign Intelligence Advisory Board
- United States Trade Representative
- White House Office for Women's Initiatives and Outreach

Executive Agencies

Department of Agriculture

- Farm and Foreign Agriculture Services
 - Farm Service Agency
 - Foreign Agricultural Service
 - Commodity Credit Corporation
 - Risk Management
- Food, Nutrition, and Consumer Services
 - Food and Nutrition Service

00176313 011900

Food Safety

Food Safety and Inspection Service

Marketing and Regulatory Services

Agricultural Marketing Service

Animal and Plant Health Inspection Service

Grain Inspection, Packers and Stockyards Administration

Natural Resources and Environment

Forest Service

Natural Resources Conservation Service

Research, Education and Economics

Agricultural Research Service (ARS)

National Agricultural Library

Agricultural Genome Information System

Pasture Systems and Watershed Management Research Lab (PSWMRL)

Subtropical Agricultural Research Laboratory

Water Management Research Laboratory (WMRL)

Cooperative State Research, Education, and Extension Service

Economic Research Service

National Agricultural Statistics Service

Rural Development

National Rural Development Partnership (NRDP)

Rural Business-Cooperative Service

Rural Housing Service

Rural Utilities Service

Office of the Chief Economist

Agricultural Labor Affairs Coordinator

Office of Risk Assessment and Cost-Benefit Analysis (ORACBA)

World Agricultural Outlook Board

Alternative Agricultural Research and Commercialization Center (AARC)

Department of Commerce

Office of the Secretary

Staff Offices

Office of Consumer Affairs

Office of Business Liason

Office of General Counsel

Office of Public Affairs

Administrative Offices

Herbert C. Hoover Building Library

Human Resources Management

Office of Small and Disadvantaged Business Utilization

Office of the Inspector General

Bureau of Export Administration

Economics and Statistics Administration

Bureau of Economic Analysis (BEA)

Bureau of the Census

CenStats

RELEASE 04/09

- STAT-USA (formerly Office of Business Analysis)
- Economic Development Administration
- International Trade Administration
 - U.S. and Foreign Commercial Service
 - Export Assistance Centers
 - Import Administration (IA)
 - Market Access Compliance (MAC)
 - Trade Compliance Center
 - Trade Information Center
- Minority Business Development Agency
- National Oceanic and Atmospheric Administration (NOAA)
 - Coastal Ocean Program (COP)
 - High Performance Computing and Communications (HPCC)
 - National Environmental Satellite, Data, and Information Service (NESDIS)
 - Environmental Information Services (EIS)
 - National Climatic Data Center (NCDC)
 - National Geophysical Data Center (NGDC)
 - National Oceanographic Data Center (NODC)
 - Office of Satellite Data Processing and Distribution
 - National Marine Fisheries Service (NMFS)
 - National Ocean Service (NOS)
 - National Weather Service (NWS)
 - Office of Global Programs
 - Office of Oceanic and Atmospheric Research
 - Environmental Research Laboratories
 - Aeronomy Laboratory
 - Atlantic Oceanographic and Meteorological Laboratory
 - Air Resources Laboratory
 - Climate Diagnostics Center
 - Climate Monitoring and Diagnostics Laboratory
 - Environmental Technology Laboratory
 - Forecast Systems Laboratory
 - Geophysical Fluid Dynamics Laboratory
 - Great Lakes Environmental Research Laboratory
 - National Severe Storms Laboratory
 - Pacific Marine Environmental Laboratory
 - Space Environment Center
 - Office of Research and Technology Applications (ORTA)
- National Telecommunications and Information Administration
 - Institute for Telecommunications Sciences
- Patent and Trademark Office
 - U.S. Patents Database at CNIDR
- Technology Administration
 - National Institute of Standards and Technology
 - National Technical Information Service (NTIS)
 - FedWorld Information Network
 - Office of Technology Policy

5010818-01900

Department of Defense (DefenseLINK)

Office of the Secretary of Defense

Office of the Executive Secretariat

Office of General Counsel

Office of Inspector General

Under Secretaries of Defense

Office of the Under Secretary of Defense for Acquisition and Technology (ACQWeb)

Office of the Under Secretary of Defense (Comptroller)

Department of Defense National Performance Review Activities

Office of the Under Secretary of Defense for Personnel and Readiness

Office of the Under Secretary of Defense for Policy

Joint Chiefs of Staff (JCSLink)

Joint Staff

Directorate for Manpower and Personnel (J-1)

Directorate for Intelligence (J-2)

Directorate for Operations

Logistics Directorate (J-4)

Strategic Plans and Policy Directorate (J-5)

Directorate for Command, Control, Communications, and Computer System (J-6)

Operational Plans and Interoperability Directorate (J-7)

Force Structure, Resources and Assessment Directorate (J-8)

Directorate of Management

Defense Agencies

Advanced Information Technology Services--Joint Program Office (AITS-JPO)

Armed Forces Radiobiology Research Institute (AFRRI)

Ballistic Missile Defense Organization (BMDOLINK)

Defense Advanced Research Projects Agency (DARPA)

Defense Commissary Agency (DeCA)

Defense Contract Audit Agency (DCAA)

Defense Finance and Accounting Service (DFAS)

Defense Information Systems Agency (DISA)

Defense Intelligence Agency (DIA)

Defense Legal Services Agency

Defense Logistics Agency (DLA)

Corporate Administration

DLA Environmental and Safety Policy Office (CAAE)

Defense Automatic Addressing System Center (DAASC)

DLA Office of Operations Research and Resource Analysis (DORRA)

Chief Information Officer

Defense Systems Design Center (DSDC)

Defense Automated Printing Service Center

Defense Automated Printing Service

Index of Specifications and Standards (DoDISS)

Single Stock Point for Specifications and Standards (DoDSSP)

Defense Administrative Support Center

Defense Contract Management Command (DCMC)

Defense Contract Management District East (DCMDE)

Defense Contract Management District International (DCMDI)

50176849-01400

- Defense Contract Management District West (DCMDW)
- Defense Logistics Support Command (DLSC)
- Automatic Identification Technology Office
- Inventory Control Points
- Defense Energy Support Center (DESC)
- Defense Industrial Supply Center (DISC)
- Defense Supply Center Columbus (DSCC)
- Defense Supply Center Richmond (DSCR)
- Defense Supply Center Philadelphia (DSCP)
- Defense Distribution Center (DDC)

Service Centers

- Defense Reutilization and Marketing Service (DRMS)
- Defense Logistics Information Service (DLIS)
- Defense National Stockpile Center (DNSC)
- Defense Distribution Systems Center (DDSC)

- Defense Security Assistance Agency
- Defense Security Service (DSS) (formerly Defense Investigative Service)
- Defense Special Weapons Agency
- Defense Technical Information Center (DTIC)
- National Imagery and Mapping Agency (NIMA)
- National Security Agency/Central Security Service
- On-Site Inspection Agency (OSIALink)

Department of Defense Field Activities

- American Forces Information Service
- Defense Medical Programs Activity
- Defense Prisoner of War/Missing Personnel Office
- Defense Technology Security Administration
- Department of Defense Human Resources Field Activity
- Defense Civilian Personnel Management Service (CPMS)
- Defense Manpower Data Center (DMDC)

Department of Defense Education Activity

- Office of Civilian Health and Medical Program of the Uniformed Services
- Office of Economic Adjustment
- TRICARE Management Activity
- Washington Headquarters Services

Unified Commands

- U.S. European Command, Stuttgart-Vaihingen, Germany
- U.S. Pacific Command, Honolulu, HI
- U.S. Atlantic Command, Norfolk, VA
- U.S. Southern Command, Miami, FL
- U.S. Central Command, MacDill Air Force Base, FL
- U.S. Space Command, Peterson Air Force Base, CO
- U.S. Special Operations Command, MacDill Air Force Base, FL
- U.S. Transportation Command, Scott Air Force Base, IL
- U.S. Strategic Command, Offutt Air Force Base, NE

Coast Guard (in time of war)

- Commandant (G-C)
- Master Chief Petty Officer of the Coast Guard

50106BB-0190

Chief Administrative Law Judge for the U.S. Coast Guard
Civil Rights Directorate (G-H)
Partnerships in Education
Chief of Staff (G-CCS)
National Pollution Funds Center
Acquisitions Directorate (G-A)
Chief Counsel (G-L)
Human Resources Directorate (G-W)
Reserve and Training (G-WT)
Personnel Management Staff (G-WP)
Resource Management Staff (G-WR)
Health and Safety Directorate (G-WH)
Marine Safety and Environmental Protection (G-M)
Operations Directorate (G-O)
U.S. Coast Guard Auxillary
Office of Boating Safety
Office of Law Enforcement
National Response Center
Navigation Center
Systems Directorate (G-S)
Operations Systems Center
Research and Development Center
United States Coast Guard Academy
Department of the Air Force
Headquarters United States Air Force
Air Combat Command
Air Education and Training Command
Air Force Materiel Command
Air Force Reserve Command
Air Force Reserve Officer Training Corps (AFROTC)
Air Force Special Operations Command (AFSOC)
Air Force Space Command
Air Force Mobility Command
Air National Guard
Pacific Air Forces
U.S. Air Forces in Europe
Field Operating Agencies
Air Force Agency for Modeling and Simulation
Air Force Audit Agency
Air Force Base Conversion Agency
Air Force Center for Environmental Excellence
Air Force Center for Quality and Management Innovation
Air Force Civil Engineer Support Agency
Air Force Colonel Matters Office
Air Force Communications Agency
Air Force Contingency Supply Squadron
Air Force Flight Standards Agency
Air Force Historical Research Agency

00178818 01900

- Air Force History Support Office
- Air Force Information Warfare Center
- Air Force Inspection Agency
- Air Force Logistics Management Agency
- Air Force Medical Logistics Office
- Air Force Medical Support Agency
- Air Force National Security Emergency Preparedness Agency
- Air Force Office of Scientific Research
- Air Force Office of Special Investigations
- Air Force Personnel Center
- Air Force Safety Center
- Air Force Services Agency
- Air Force Studies and Analyses Agency
- Air Force Technical Applications Center
- Air Force Weather Agency
- Air Force Intelligence Agency
- Air Force Reserve Personnel Center
- United States Air Force Academy
- Department of the Army
- U.S. Army Corps of Engineers
- Regional Headquarters
- Great Lakes Regional Headquarters (CELRD-GL)
- Ohio River Regional Headquarters (CELRD-OR)
- Missouri River Regional Headquarters (CENWD)
- North Pacific Regional Headquarters (CENWD-NP)
- Divisions
- Great Lakes and Ohio River Division (CELRD)
- Mississippi Valley Division (CEMVD)
- North Atlantic Division (CENAD)
- Northwestern Division (CENWD)
- Pacific Ocean Division (CEPOD)
- South Atlantic Division (CESAD)
- South Pacific Division (CESPD)
- Southwestern Division (CESWD)
- Laboratories
- Cold Regions Research and Engineering Laboratory (CECRL)
- Construction Engineering Research Laboratories(CECER)
- Waterways Experiment Station (CEWES)
- Topographic Engineering Center (CETEC)
- Army Digitization Office (ADO)
- Army Research Laboratory (ARL)
- U.S. Army Financial Management
- U.S. Military Academy
- White Sands Missile Range (WSMR)
- Department of the Navy
- Department of the Navy Environmental Program
- Office of the Assistant Secretary of the Navy (Financial Management and Comptroller)
- Office of Budget

5017ESTB-011900

Office of Information
Office of the Naval Inspector General
Office of Naval Research (ONR)
United States Marine Corps
Commandant of the Marine Corps
Headquarters, United States Marine Corps
HQMC Staff Agencies
Marine Corps Uniform Board
Administration and Resources
Historical Division
Inspector General
Staff Judge Advocate to the Commandant
Morale, Welfare and Recreation
Division of Public Affairs
Programs and Resources
Marine Corps Combat Development Command
Total Quality Leadership
Director, Marine Corps Staff
Command, Control, Communications, computer and Intelligence (C4I)
Department
Health Services
Installations and Logistics Department
Manpower and Reserve Affairs
Office of Legislative Affairs
Plans, Policies and Operations
Marine Corps Systems Command
Marine Corps Recruiting Command
Safety Division
Marine Expeditionary Units
United States Naval Academy
Joint Service Schools
Defense Acquisition University
Defense Systems Management College
Joint Military Intelligence College
National Defense University
National War College
Air War College
Army War College
Marine War College
Naval War College
Industrial College of the Armed Forces
Armed Forces Staff College
Information Resources Management College
Uniformed Services University of the Health Sciences
National Guard

Department of Education

External Relations

Office of Intergovernmental and Interagency Affairs
Information Resource Center
Office of Non-Public Education
Partnership for Family Involvement in Education
Office of Legislation and Congressional Affairs

Operations

Office of Management
Family Policy Compliance Office
Office of Hearings and Appeals
Office of the Chief Information Officer
Office of the Chief Financial Officer

Programs

Office of Bilingual Education and Minority Languages Affairs (OBEMLA)
Office for Civil Rights
Office of Educational Research and Improvement (OERI)
National Center for Education Statistics (NCES)
National Educational Research Policy and Priorities Board
National Institute on Early Childhood Development and Education
National Institute on the Education of At-Risk Students
National Institute on Educational Governance, Finance, Policy-Making, and Management
National Institute on Postsecondary Education, Libraries, and Lifelong Learning (PLL)
National Institute on Student Achievement, Curriculum, and Assessment
National Library of Education
National Research and Development Centers
Office of Reform Assistance and Dissemination
Office of Elementary and Secondary Education (OESE)
Office of Indian Education
Office of Migrant Education
Office of Postsecondary Education (OPE)
Office of Special Education and Rehabilitative Service
National Institute on Disability and Rehabilitation Research
Rehabilitation Services Administration
Office of Special Education Programs
Office of Vocational and Adult Education (OVAE)
Regional Offices

Department of Energy

Programs and Offices

Columbus Environmental Management Project
Energy Efficiency and Renewable Energy Network
Energy Information Administration
Energy Sciences Network (ESnet)
Environment, Safety and Health
Environmental Management
Federal Energy Regulatory Commission
Fusion Energy Sciences Program

60176919-011900

Human Resources and Administration
Oakland Operations Office
Office of the Chief Financial Officer
Office of Civilian Radioactive Waste Management
Office of Defense Programs
Office of the Departmental Representative to the Defense Nuclear Facilities Safety Board (DNFSB)
Office of Economic Impact and Diversity
Office of Energy Research
Office of Field Management
Office of Fissile Materials Disposition
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Inspector General
Office of Nonproliferation and National Security
Office of Policy and International Affairs
Office of Nuclear Energy, Science, and Technology
Office of Procurement and Assistance Management
Office of Scientific and Technical Information
Office of the Secretary of Energy Advisory Board
Office of Worker and Community Transition

Laboratories and Facilities

Argonne National Laboratory (ANL)
Brookhaven National Laboratory
Thomas Jefferson National Accelerator Facility (formerly Continuous Electron Beam Accelerator Facility (CEBAF))
Energy Efficiency and Renewable Energy Network (EREN)
Fermi National Accelerator Laboratory (Fermilab)
Hanford Site (Richland Operations Office)
Idaho National Engineering and Environmental Laboratory (INEEL)
Kansas City Plant
Lawrence Berkeley Laboratory (LBL)
Lawrence Livermore National Laboratory
National Energy Research Supercomputer Center
Los Alamos National Laboratory (LANL)
Advanced Computing Laboratory
National Renewable Energy Laboratory
Nevada Operations Office
Oak Ridge National Laboratories
Center for Computational Sciences
Pacific Northwest National Laboratory (PNL)
William R. Wiley Environmental Molecular Sciences Laboratory
Princeton Plasma Physics Laboratory
Sandia National Laboratories
Savannah River Operations Office
Stanford Linear Accelerator Center (SLAC)

EO 1.25513 - 011900

Department of Health and Human ServicesAdministration on AgingAdministration for Children and FamiliesHealth Care Financing AdministrationPublic Health Service (PHS)Agency for Toxic Substances and Disease RegistryCase Studies in Environmental MedicineCenters for Disease Control and Prevention (CDC)National Center for Chronic Disease Prevention and Health PromotionNational Center for Environmental HealthNational Center for Health StatisticsNational Center for Infectious DiseasesNational Center for Injury Prevention and ControlNational Institute for Occupational Safety and HealthMining Health & Safety Research ProgramEpidemiology Program OfficeInternational Health Program OfficePublic Health Practice Program OfficeNational Immunization Program Childhood Immunization InitiativeFood and Drug Administration (FDA)National Center for Food Safety and Applied Nutrition (CFSAN)National Center for Toxicological Research (NCTR)Indian Health Service (IHS)National Institutes of Health (NIH)Advanced Laboratory Workstation ProjectDivision of Computer Research and Technology (DCRT)BioInformatics Molecular Analysis Section (BIMAS)BioMagResBank Database GatewayGenoBase Database GatewayCenter for Scientific Review (CSR) (formerly Division of Research Grants)National Cancer Institute (NCI)CancerNetNational Human Genome Research Institute (NHGRI)National Center for Research Resources (NCRR)National Eye InstituteNational Heart, Lung and Blood Institute (NHLBI)National Institute for Allergy and Infectious Diseases (NIAID)National Institute of Child Health and Human DevelopmentNational Institute of Diabetes and Digestive and Kidney Disease (NIDDK)National Institute of Drug AbuseNational Institute of Environmental Health Sciences (NIEHS)National Institute of General Medical Sciences (NIGMS)National Institute of Mental Health (NIMH)National Institute of Neurological Disorders and Stroke (NINDS)National Institute of Nursing ResearchNational Institute on AgingNational Library of Medicine (NLM)National Center for Biotechnology Information (NCBI) at NLM

S O C I E T Y O F S E R V I C E S

Substance Abuse and Mental Health Services Administration

Department of Housing and Urban Development (HUD)

Office of the Secretary

- Administrative Law Judges
- Board of Contract Appeals
- Chief Information Officer
- Departmental Equal Employment Opportunity
- Office of Departmental Operations and Coordination
- Office of Federal Housing Enterprise Oversight
- Office of Labor Relations
- Office of Lead Hazard Control
- Office of Small and Disadvantaged Business Utilization
- Office of Special Actions

Secretary's Representatives

Headquarters Program Offices

- Government National Mortgage Association (Ginnie Mae)
- Office of Community Planning and Development
- Office of Fair Housing and Equal Opportunity
- Office of Housing/Federal Housing Authority (FHA)
- Office of Public and Indian Housing

Headquarters Support Offices

- Office of Administration
- Office of the Chief Financial Officer
- Office of Congressional and Intergovernmental Relations
- Office of General Counsel
- Office of Policy Development and Research
- Office of Public Affairs

Office of Inspector General

Local Offices

Department of the Interior

Secretary of the Interior

Office of the Secretary

- Deputy Secretary
- Executive Secretariat
- Office of Legislative and Congressional Affairs
- Office of Communications
- Office of the Solicitor
- Office of Inspector General
- Office of the Special Trustee for American Indians
- Office of Policy, Management and Budget
- Human Resources
 - Office of Personnel
 - Office of Ethics
 - Office of National Service and Educational Partnerships
- Office of Aircraft Services

2025 RELEASE UNDER E.O. 14176

Office of Acquisition and Property Management
Office of the Budget
Office of Environmental Policy and Compliance
Office of Financial Management
Office of Hearings and Appeals
Office of Insular Affairs
Office of International Affairs
Office of Managing Risk and Public Safety
Office of Small and Disadvantaged Business Utilization
Office of Information Resources Management
Assistant Secretary--Fish and Wildlife and Parks
National Park Service (ParkNet)
National Park Service NatureNet
Air Resources Division
American Indian Liason Office
Geological Resources Division
Water Resources Division
U.S. Fish and Wildlife Service
Air Quality Branch
Division of Contracting and General Services
Division of Endangered Species
Division of Environmental Contaminants
Division of Federal Aid
Fish and Wildlife Reference Service
Management Assistance Team
Division of Finance
Division of Habitat Conservation
Coastal Habitat Conservation Programs
National Wetlands Inventory
Division of Information Resources Management
FWS Data Administration
Geographic Information Systems and Spatial Data
Division of Law Enforcement
US Fish and Wildlife Forensics Lab, Ashland, Oregon
Division of Policy and Directives Management
Division of Realty
Federal Duck Stamp Office
Federal Junior Duck Stamp Conservation and Design Program
Fire Management
National Conservation Training Center
National Wildlife Refuge System
North American Waterfowl and Wetlands Office
Office for Human Resources
Office of International Affairs
Office of Miratory Bird Management
Washington Office Fisheries
Regions
Region 1 (Pacific Region)

50175818 011900

- Region 2 (Southwest Region)
- Region 3 (Great Lakes-Big Rivers Region)
- Region 4 (Southeast Region)
- Region 5 (Northeast Region)
- Region 6 (Mountain-Prairies Region)
- Region 7 (Alaska Region)

Assistant Secretary--Indian Affairs

- Bureau of Indian Affairs (BIA)
 - Branch of Acknowledgement and Research
 - Office of Congressional and Legislative Affairs
 - Office of Indian Education Programs
 - Office of Tribal Services
 - Office of Trust Responsibilities
 - Division of Energy and Mineral Resources
 - Division of Forestry
 - Geographic Data Service Center
- Office of American Indian Trust (OAIT)
 - Office of Self-Governance

Assistant Secretary--Land and Minerals Management

- Bureau of Land Management (BLM)
 - National Applied Resource Sciences Center
 - National Business Center
 - National Human Resource Management Center (NHRMC)
 - National Information Resource Management Center
 - National Interagency Fire Center
 - National Training Center
 - National Wild Horse and Burro Program
 - State Offices
 - Minerals Management Service
 - Environmental Studies Program Information System
 - Offshore Minerals Management Program (OMM)
 - Royalty Management Program
 - Office of Surface Mining Reclamation and Enforcement

Assistant Secretary--Water and Science

- Bureau of Reclamation
 - Acquisition and Assistance Management Services
 - Denver Administrative Service Center
 - Human Resources Center
 - Management Service Office
 - Program Analysis Office
 - Reclamation Services Center
 - Technical Service Center
 - Regional Offices
 - Great Plains Region
 - Lower Colorado Region
 - Mid-Pacific Region
 - Pacific Northwest Region
 - Upper Colorado Region

60476348-91490

U.S. Geological Survey (USGS)

Department of Justice (DOJ)

Office of the Attorney General

Office of the Deputy Attorney General

Office of the Solicitor General

Office of the Associate Attorney General

Community Relations Service

Executive Office for United States Trustees

Foreign Claims Settlement Commission

Office of Community Oriented Policing Services (COPS)

Office of Dispute Resolution

Office of Information and Privacy

Office of Justice Programs

Program Offices

American Indian and Alaska Native Affairs Desk

Corrections Program Office

Drug Courts Program Office

Executive Office for Weed and Seed

Violence Against Women Grants Office

Violence Against Women Office

Bureaus

Bureau of Justice Assistance

Bureau of Justice Statistics

National Institute of Justice

Crime Mapping Research Center

National Criminal Justice Reference Service

Justice Information Center

Office of Science and Technology

National Law Enforcement and Corrections Technology Center

(JustNet)

Office of Juvenile Justice and Delinquency Prevention

Office for Victims of Crime

Federal Crimes Victims Division

State Compensation and Assistance Division

Special Projects Division

Support Offices

Equal Employment Opportunity Office

Office of Administration

Office of Budget and Management Services

Office for Civil Rights

Office of the Comptroller

Office of Congressional and Public Affairs

Office of General Counsel

Antitrust Division

Civil Division

Civil Rights Division

00670"03020202

Environment and National Resources Division

Tax Division

Office of Intergovernmental Affairs

Office of Legal Counsel

Office of Legislative Affairs

Office of Policy Development

Office of Public Affairs

Bureau of Prisons

National Institute of Corrections

Criminal Division

Drug Enforcement Administration (DEA)

Executive Office for United States Attorneys

United States Attorneys

Federal Bureau of Investigation (FBI)

FBI Academy

FBI Laboratory

Field Offices

National Computer Crime Squad

National Infrastructure Protection Center (NIPC)

Immigration and Naturalization Service (INS)

United States Marshals Service

United States National Central Bureau (USNCB)--INTERPOL

Executive Office for Immigration Review

Justice Management Division

National Drug Intelligence Center

Office of the Inspector General

Office of Intelligence Policy and Review

Office of the Pardon Attorney

Office of Professional Responsibility

United States Parole Commission

Department of Labor (DOL)

Office of the Secretary

Office of the Assistant Secretary for Administration and Management

Office of the Assistant Secretary for Policy

Office of the Chief Financial Officer

Office of the Chief Information Officer

Office of the Inspector General

Office of the Solicitor

Administrative Review Board

Benefits Review Board

Bureau of International Labor Affairs

Bureau of Labor Statistics

Employees' Compensation Appeals Board (ECAB)

Employment and Training Administration

Employment Standards Administration

Office of Federal Contract Compliance Programs

SECRET 01990

- Office of Labor-Management Standards
- Office of Workers' Compensation Programs
 - Division of Federal Employees' Compensation
 - Division of Coal Mine Workers' Compensation
 - Division of Longshore and Harbor Workers' Compensation
- Wage and Hour Division
- Mine Safety and Health Administration
 - Directorate of Educational Policy and Development
 - National Mine Health and Safety Academy
- District Offices
- Occupational Safety and Health Administration (OSHA)
- Office of Administrative Law Judges
- Office of Small Business Programs
- Pension and Welfare Benefits Administration
- Veterans' Employment and Training Service
- Women's Bureau

Department of State

Secretary of State

- Operations Center
- Policy Planning Staff
- Office of Resources, Plans and Policy
- Office of the Chief of Protocol
- Office of the Permanent Representative to the United Nations
- Bureau of Public Affairs
 - Office of the Historian
- Bureau of Legislative Affairs
- Bureau of Intelligence and Research
- Office of Inspector General
- Office of the Legal Adviser

Office of Under Secretary for Political Affairs

Geographic Bureaus

- Bureau of African Affairs
- Bureau of East Asian and Pacific Affairs
- Bureau of European and Canadian Affairs
- Bureau of Inter-American Affairs
- Bureau of Near Eastern Affairs
- Bureau of South Asian Affairs

Office of the Special Adviser to the Secretary for the New Independent States

Bureau of International Organization Affairs

Office of Under Secretary for Economic, Business, and Agricultural Affairs

- Office of the Coordinator for Business Affairs
- Bureau of Economic and Business Affairs

Office of Under Secretary for Arms Control and International Security Affairs

- Bureau of Political Military Affairs
 - Office of Defense Trade Controls
 - Nonproliferation and Disarmament Fund

SECRET - 01490

19/46

- Office of Under Secretary for Management
 - Office of Foreign Missions
 - Foreign Service Institute
 - Director General of Foreign Service and Director of Personnel
 - Family Liason Office
 - Bureau of Administration
 - Office of Allowances
 - Office of Overseas Schools
 - Office of the Procurement Executive
 - Office of Small and Disadvantaged Business Utilization
 - Ralph J. Bunche Library
 - Bureau of Consular Affairs
 - Bureau of Diplomatic Security
 - Overseas Security Advisory Council (OSAC)
 - Bureau of Finance and Management Policy
 - Office of Under Secretary for Global Affairs
 - Bureau of Democracy, Human Rights, and Labor
 - Bureau for International Narcotics and Law Enforcement Affairs
 - Bureau of Oceans and International Environmental and Scientific Affairs
 - Bureau of Population, Refugees, and Migration
 - Office of the Coordinator for Counterterrorism
 - Office of the Senior Coordinator for International Women's Issues
 - U.S. Missions Online
 - Office of Authentication

- Department of Transportation
 - Office of the Secretary
 - Bureau of Transportation Statistics
 - Coast Guard (in time of peace)
 - Federal Aviation Administration (FAA)
 - Associate Administrator for Administration
 - Associate Administrator for Commercial Space Transportation
 - Civil Aviation Security
 - Office of the Associate Administrator for Airports
 - Office of System Safety
 - Flight Standards Service
 - Mike Monroney Aeronautical Center
 - William J. Hughes Technical Center
 - Federal Highway Administration
 - Associate Administrator for Policy
 - Office of International Programs
 - Office of Policy Development
 - Office of Highway Information Management
 - Associate Administrator for Research and Development
 - Turner-Fairbank Highway Research Center
 - Office of Research and Development Operations and Support
 - Office of Engineering Research and Development

004904090807

- Office of Safety and Traffic Operations Research and Development
- Traffic and Driver Information Systems Division
- Associate Administrator for Motor Carriers
- Office of Administration
- Office of Program Development
- Federal Railroad Administration
- Federal Transit Administration
- National Highway Traffic Safety Administration (NHTSA)
- Maritime Administration
- National Transportation Library
- Research and Special Programs Administration
- Saint Lawrence Seaway Development Corporation
- Surface Transportation Board
- Transportation Administrative Service Center (TASC)

Department of the Treasury

Treasury Bureaus

- Internal Revenue Service (IRS)
- United States Customs Service
- Bureau of Alcohol, Tobacco, and Firearms
- Financial Management Service
- United States Secret Service
- Office of Thrift Supervision
- United States Mint
- Office of the Comptroller of the Currency
- Federal Law Enforcement Training Center
- Bureau of the Public Debt
- Bureau of Engraving and Printing
- Financial Crimes Enforcement Network
- Community Development Financial Institutions Fund

Treasury Offices

- Office of Domestic Finance
- Office of Economic Policy
- Foreign Investment Survey
- Office of Enforcement
- Office of International Affairs
- Office of Legislative Affairs
- Office of Management
- Chief Information Officer
- Chief Financial Officer
- Office of Equal Opportunity Program
- Government Information Technology Services (GITS)
- GITS Security
- Office of Small and Disadvantaged Business Utilization
- Office of Treasury Reinvention
- Office of Budget

2006 FEB 28 04:59 PM EST

Department of Veterans Affairs

Board of Contract Appeals

Board of Veterans' Appeals

Chief Information Officers Council

Inter-Agency Benchmarking and Best Practices Council

National Cemetery System (NCS)

Office of Acquisition and Materiel Management

Office of Congressional Affairs

Office of Financial Management

Office of Information Resources Management

Office of Inspector General

Office of Occupational Safety and Health

Office of Small and Disadvantaged Business Utilization

Veterans Health Administration (VHA)

Diabetes Program

National Center for Health Promotion and Disease Prevention

National Chaplain Center

Nursing Service

Office of Research and Development

Physical Medicine and Rehabilitation Service

Veterans Integrated Service Networks

Veterans Benefits Association (VBA)

Debt Management Center

Compensation and Pension Service

Education Service

Insurance Service

Loan Guaranty Service

Vocational Rehabilitation and Counseling Service

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official
-----------	----------	-------------	-------------	-------------------------------------	----------------

Judicial Branch

Administrative Office of the U.S. Courts (Federal Judiciary Homepage)

Federal Judicial Center

United States Sentencing Commission

United States Supreme Court

Supreme Court via LII at Cornell Law School (opinions since 1990 and selected historical decisions)

Supreme Court via FindLaw (opinions since 1893)

Supreme Court via Oyez Oyez Oyez (Real Audio recordings of oral arguments)

Courts of Appeal (see also U.S. Federal Courts Finder)

First Circuit

First Circuit via Emory University School of Law (opinions since November 1995)

First Circuit via FindLaw (opinions since November 1995)

Second Circuit

Second Circuit via Touro Law Center (opinions since January 1995)

SC178818-011900

Second Circuit via Pace University School of Law (opinions since September 1995)

Second Circuit via FindLaw (opinions since January 1995)

Third Circuit

Third Circuit via Villanova Center for Information Law and Policy (opinions since May 1994)

Third Circuit via FindLaw (opinions since May 1994)

Fourth Circuit

Fourth Circuit via Emory University School of Law (opinions since January 1995)

Fourth Circuit via FindLaw (opinions since January 1995)

Fifth Circuit

Official Fifth Circuit Web Site (opinions since 1991, other documents, general information)

Fifth Circuit via FindLaw (recent opinions only)

Sixth Circuit

Sixth Circuit via Emory University School of Law (opinions since January 1995)

Sixth Circuit via FindLaw (opinions since January 1995)

Seventh Circuit

Seventh Circuit via Chicago-Kent College of Law (opinions since January 1993)

Seventh Circuit via FindLaw (opinions since June 1995)

Eighth Circuit

Eighth Circuit via Washington University School of Law (opinions since November 1995)

Eighth Circuit via FindLaw (opinions since November 1995)

Ninth Circuit

Office of the Circuit Executive--Official Ninth Circuit Web Site (general information; no opinions available)

Ninth Circuit via Villanova Center for Information Law and Policy (opinions since June 1995)

Ninth Circuit via FindLaw (opinions since 1990)

Tenth Circuit

Tenth Circuit Clerk--Official Tenth Circuit Web Site (general information; no opinions available)

Tenth Circuit via Emory University School of Law (opinions from August 1995 to October 1997)

Tenth Circuit via Washburn University School of Law (opinions since October 1997)

Tenth Circuit via FindLaw (recent opinions only)

Eleventh Circuit

Eleventh Circuit Library Reference Desk (links and general information; no opinions available)

Eleventh Circuit Internet Pilot Project (opinions from the last three months)

Eleventh Circuit via Emory University School of Law (opinions since November 1994)

Eleventh Circuit via FindLaw (opinions since December 1994)

District of Columbia Circuit

Official D.C. Circuit Web Site (opinions since September 1997; general information)

D.C. Circuit via Georgetown University Law Center (opinions since March 1995)

D.C. Circuit via FindLaw (opinions since February 1995)

Federal Circuit

Official Federal Circuit Web Site (recent opinions only)

Federal Circuit via Emory University School of Law (opinions since August 1995)

Federal Circuit via Georgetown University Law Center (opinions since August 1995)

Federal Circuit via FindLaw (recent opinions only)
U.S. Court of Appeals for the Armed Forces (administratively located in the Department of Defense)

Official U.S. Court of Appeals for the Armed Forces Web Site (opinions since October 1996; general information)

<u>Executive</u>	<u>Judicial</u>	<u>Legislative</u>	<u>Independent</u>	<u>Boards, Commissions, and Committees</u>	<u>Quasi-Official</u>
------------------	-----------------	--------------------	--------------------	--	-----------------------

Legislative Branch

U.S. House of Representatives

Representatives on the Web

U.S. House of Representatives Internet Law Library

U.S. Senate

Senators on the Web

Congressional Budget Office (CBO)

General Accounting Office (GAO)

Government Printing Office (GPO)

Institute for Federal Printing and Publishing (IFPP)

LSU Libraries GPO Access Gateway

Library of Congress

LOCIS: Library of Congress Online Public Access Catalog

LC Marvel

THOMAS: Legislative Information on the Internet

103rd Congress Bills

104th Congress Bills

105th Congress Bills

Office of Compliance

Office of Technology Assessment

Stennis Center for Public Service

<u>Executive</u>	<u>Judicial</u>	<u>Legislative</u>	<u>Independent</u>	<u>Boards, Commissions, and Committees</u>	<u>Quasi-Official</u>
------------------	-----------------	--------------------	--------------------	--	-----------------------

Independent Establishments and Government Corporations

African Development Foundation

Central Intelligence Agency (CIA)

Intelligence Community

Commission on Civil Rights

Commodity Futures Trading Commission (CFTC)

Consumer Product Safety Commission (CPSC)

Corporation for National Service

Defense Nuclear Facilities Safety Board (DNFSB)

Environmental Protection Agency (EPA)

Equal Employment Opportunity Commission (EEOC)

24 | 46

SECRET

- Export-Import Bank of the United States
- Farm Credit Administration
- Federal Communications Commission (FCC)
- Federal Deposit Insurance Corporation (FDIC)
- Federal Election Commission (FEC)
- Federal Emergency Management Agency (FEMA)
- Federal Housing Finance Board
- Federal Labor Relations Authority
- Federal Maritime Commission
- Federal Mediation and Conciliation Service
- Federal Mine Safety and Health Review Commission
- Federal Reserve System Board of Governors
 - Federal Reserve Bank of Atlanta
 - Federal Reserve Bank of Boston
 - Federal Reserve Bank of Chicago
 - Federal Reserve Bank of Cleveland
 - Federal Reserve Bank of Dallas
 - Federal Reserve Bank of Kansas City
 - Federal Reserve Bank of Minneapolis
 - Federal Reserve Bank of New York
 - Federal Reserve Bank of Philadelphia
 - Federal Reserve Bank of San Francisco
 - Federal Reserve Bank of St. Louis
- Federal Retirement Thrift Investment Board
- Federal Trade Commission (FTC)
- General Services Administration (GSA)
 - Consumer Information Center
 - Federal Supply Service
 - Federal Technology Service (formerly Federal Telecommunications Service)
 - Office of Information Technology Integration
 - Office of Information Security
 - Federal Information Center
 - Federal Information Relay Service
 - Catalog of Federal Domestic Assistance Programs
 - Office of Governmentwide Policy
 - Public Buildings Service
- Inter-American Foundation
- Merit Systems Protection Board
- National Aeronautics and Space Administration (NASA)
 - Ames Research Center
 - Dryden Flight Research Center
 - Goddard Institute for Space Studies
 - Goddard Space Flight Center
 - Independent Validation and Verification Facility
 - Jet Propulsion Laboratory
 - Johnson Space Center
 - Kennedy Space Center
 - Langley Research Center

CONFIDENTIAL

Lewis Research Center

Marshall Space Flight Center

Moffett Federal Airfield

Stennis Space Center

Wallops Flight Facility

White Sands Test Facility

National Archives and Records Administration (NARA)

The Center for Electronic Records

National Capital Planning Commission

National Credit Union Administration (NCUA)

National Foundation on the Arts and the Humanities

The Institute of Museum and Library Services

National Endowment for the Arts

ArtsEdge

National Endowment for the Humanities (NEH)

National Labor Relations Board (NLRB)

National Mediation Board

National Railroad Passenger Corporation (Amtrak)

National Performance Review (NPR)

FinanceNet

National Science Foundation (NSF)

National Transportation Safety Board

Nuclear Regulatory Commission (NRC)

Occupational Safety and Health Review Commission

Office of Government Ethics

Office of Personnel Management

Overseas Private Investment Corporation

Panama Canal Commission

Peace Corps

Pennsylvania Avenue Development Corporation

Pension Benefit Guaranty Corporation

Postal Rate Commission

Railroad Retirement Board

Resolution Trust Corporation

Securities and Exchange Commission (SEC)

EDGAR Database

Selective Service System

Small Business Administration (SBA)

Social Security Administration (SSA)

Regional Offices:

Atlanta Region

Boston Region

Chicago Region

Denver Region

Kansas City Region

New York Region

San Francisco Region

Seattle Region

5010848-01500

26/46

Tennessee Valley Authority
Thrift Depositor Protection Oversight Board
Trade and Development Agency
United States Arms Control and Disarmament Agency
United States Information Agency (USIA)
International Broadcasting Bureau
Voice of America (VOA)
United States International Development Cooperation Agency
Agency for International Development (USAID)
The Environmental and Natural Resource Information Center
United States International Trade Commission (USITC)
United States Postal Service (USPS)

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official
-----------	----------	-------------	-------------	-------------------------------------	----------------

Boards, Commissions, and Committees

Administrative Committee of the Federal Register
Advisory Commission on Intergovernmental Relations
Advisory Council on Historic Preservation
American Battle Monuments Commission
Appalachian Regional Commission
Architectural and Transportation Barriers Compliance Board (Access Board)
Arctic Research Commission
Arthritis and Musculoskeletal Interagency Coordinating Committee
Barry M. Goldwater Scholarship and Excellence in Education Foundation
Citizens' Stamp Advisory Committee
Commission of Fine Arts
Committee on Foreign Investment in the United States
Committee for the Implementation of Textile Agreements
Committee for Purchase from People Who Are Blind or Severely Disabled
Coordinating Council on Juvenile Justice and Delinquency Prevention
Critical Infrastructure Assurance Office (CIAO)
Delaware River Basin Commission
Endangered Species Committee
Export Administration Review Board
Federal Financial Institutions Examination Council
Federal Financing Bank
Federal Interagency Committee on Education
Federal Interagency Council on Statistical Policy
FedStats
Federal Laboratory Consortium for Technology Transfer
Federal Library and Information Center Committee
Franklin Delano Roosevelt Memorial Commission
Harry S. Truman Scholarship Foundation
Illinois and Michigan Canal National Heritage Corridor Commission
Indian Arts and Crafts Board
Information Security Oversight Office

50175318-011900

27/46

- Interagency Committee on Employment of People with Disabilities
- Interagency Savings Bonds Committee
- J. William Fulbright Foreign Scholarship Board
- James Madison Memorial Fellowship Foundation
- Japan-United States Friendship Commission
- Joint Board for the Enrollment of Actuaries
- Marine Mammal Commission
- Medicare Payment Advisory Commission (MedPAC) (formerly the Physician Payment Review Commission and the Prospective Payment Assessment Commission)
- Migratory Bird Conservation Commission
- Mississippi River Commission
- National Commission on Libraries and Information Science
- National Communications System
- National Council on Disability
- National Gambling Impact Study Commission
- National Occupational Information Coordinating Committee
- National Park Foundation
 - The National Park Foundation's Complete Guide to America's Parks
- Northwest Power Planning Council
- Office of Navajo and Hopi Indian Relocation
- Office of Women's Business Ownership
- Permanent Committee for the Oliver Wendell Holmes Devise
- Physician Payment Review Commission
- President's Committee on Employment of People with Disabilities
- President's Council on Integrity and Efficiency
- President's Foreign Intelligence Advisory Board
- Regulatory Information Service Center
- Susquehanna River Basin Commission
- Textile Trade Policy Group
- Trade Policy Committee
- United States Holocaust Memorial Museum
- United States Nuclear Waste Technical Review Board
- Veterans Day National Committee
- White House Commission on Presidential Scholars

SECRET 011900

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official
-----------	----------	-------------	-------------	-------------------------------------	----------------

Quasi-Official Agencies

- Legal Services Corporation
- Smithsonian Institution
 - Anacostia Museum
 - Arthur M. Sackler Gallery
 - Arts and Industries Building
 - Center for Earth and Planetary Studies (CEPS)
 - Cooper-Hewitt, National Design Museum
 - Freer Gallery of Art
 - Harvard-Smithsonian Center for Astrophysics

- Hirshhorn Museum and Sculpture Garden
- National Air and Space Museum
- National Museum of African Art
- National Museum of American Art
- National Museum of American History
- National Museum of Natural History
- National Museum of the American Indian
- National Portrait Gallery
- National Postal Museum
- National Zoo
- State Justice Institute
- United States Institute of Peace

Executive	Judicial	Legislative	Independent	Boards, Commissions, and Committees	Quasi-Official
-----------	----------	-------------	-------------	-------------------------------------	----------------

Awards, Honors, and Recommendations Received:



[LSU Libraries](#) | [LSU and Louisiana](#) | [Internet Webliography](#) | [LSU Home Page](#)

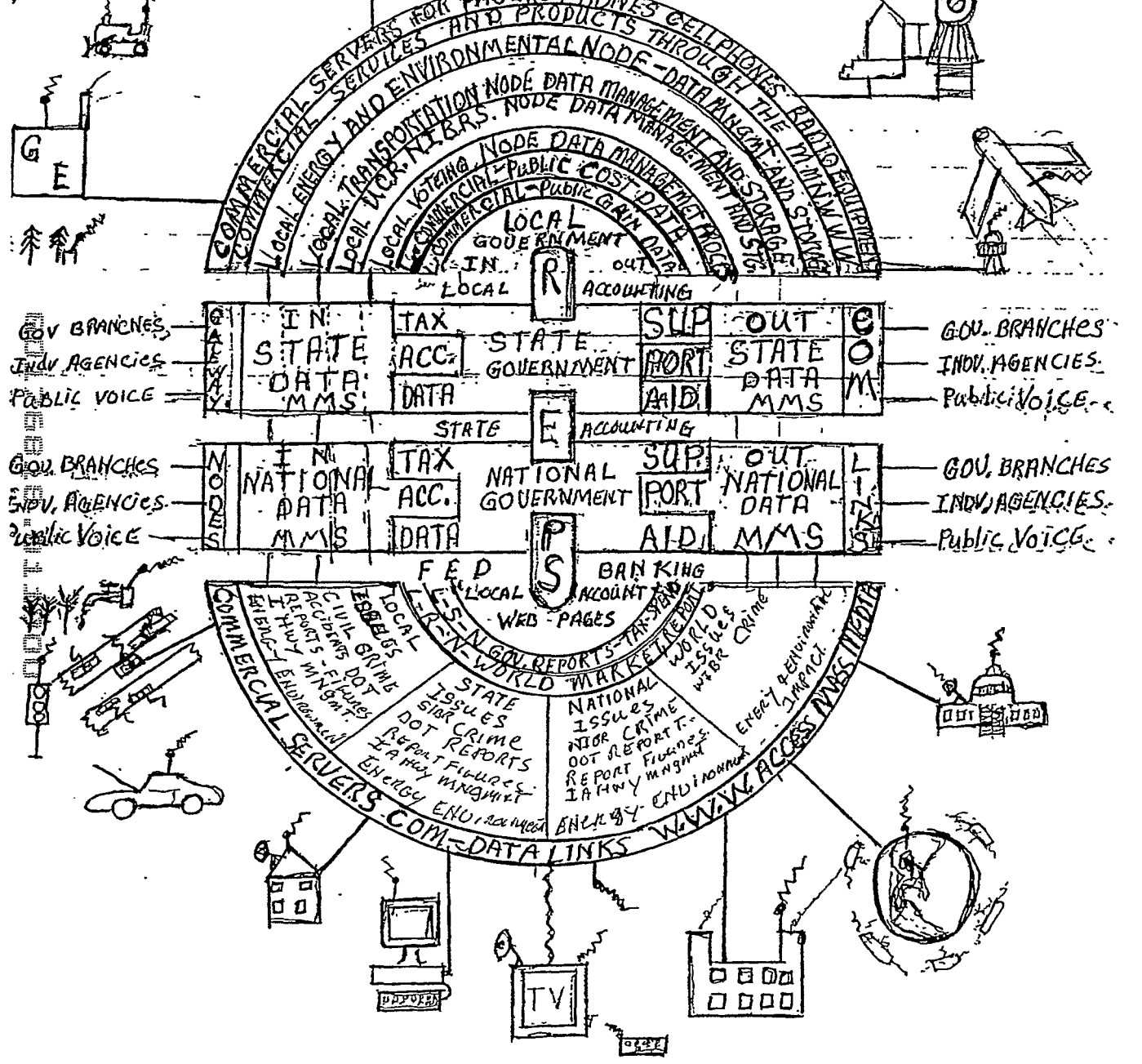
Send updates and corrections to Smittie Bolner (sbolner@lsu.edu).

Copyright © 1995 LSU Libraries
Louisiana State University, Baton Rouge, LA 70803-3300

URL: <http://www.lib.lsu.edu/gov/fedgov.html>
Last updated: Friday, 06-Nov-98 08:49:24

LSU LIBRARIES ONLINE

PHN WWW
ECONOMIC AND ENVIRONMENTAL TECHNOLOGY ACCOUNTING SYSTEM FOR DEMOCRATIC GOVERNMENT



Layer Name	Description
Application	The layer we all know and love as end users trying to do something.
Presentation	Deals with syntax and semantics of transmitted data. Usually represented as a conversion of data to some specified form
Session	Creates enhanced network connections, usually connection-based service. Also deals with different synchronization issues
Transport	Creates distinct network connections. Makes sure that connections are reliable. Deals with transmission types of service. Also deals with flow control.
Network	Sends packets. Concerned with packet routing, controls network congestion. Works with different network protocols.
Data Link	Sends frames of data. Works out transmission errors of the physical medium.
Physical	Transmits the data over the channel.

Layer 7	Application/User How information is to be exchanged between the user and the station.
Layer 6	Presentation How information is to be translated from the station's format in to that understandable by the user.
Layer 5	Session Organises, synchronizes and manages the dialogue between users.
Layer 4	Transport How data is to be transmitted and recieved.
Layer 3	Network How communication is estabtrshed, mantained and terminated between stations.
Layer 2	Data Trnk How the data is packaged for transmission.
Layer 1	Physical Trnk Describes the function of the electrical and machanical characteristics of the network.

OSI MODEL - 011900

OSI Layer	Apple Computer	Banyan Systems	DEC DECnet	IBM SNA	Microsoft Networking	Novell NetWare	TCP/IP Internet	Xerox XNS	OSI Protocols
Application Layer 7	Application Programs and Protocols for file transfer, electronic mail, etc								
Presentation Layer 6	AppleTalk Filing Protocol (AFP)	Remote Procedural Calls (Net RPC)	Network Management Network Application	Transaction Services Presentation Services	Server Message Block (SMB)	NetWare Core Protocols (NCP)	Application Specific Protocols	Control and Process Interaction	ISO 8823
Session Layer 5	AppleTalk Sesson Protocol (ASP)		Session	Data Flow Control	Network Basic Input/Output System (NetBIOS)	Network Basic Input/Output System (NetBIOS)	(Telnet, FTP, SNMP, SMTP, ICMP, etc.)		ISO 8327
Transport Layer 4	AppleTalk Transaction Protocol (ATP)	VINES InterProcess Communications (VIPC)	End Communications	Transmission Control	Network Basic Extended User Interface (NetBEUI)	Sequenced Packet Exchange (SPX)	Transmission Control Protocol (TCP)	Sequenced Packet Protocol (SPP)	ISO 8073 TP0-4
Network Layer 3	Datagram Delivery Protocol (DDP)	VINES Internet Protocol (VIP)	Routing	Path Control		Internet Packet Exchange (IPX)	Internet Protocol (IP)	Internet Datagram Protocol (IDP)	ISO 8473 (CLNP)
Data Link Layer 2	Network Interface Cards Ethernet, Token-Ring, ARCNET, StarLAN, LocalTalk, FDDI, ATM, etc NIC Drivers Open Datalink Interface (ODI), Network Independent Interface Specification (NDIS)								
Physical Layer 1	Transmission Media Twisted Pair, Coax Fiber Optic, Wireless Media etc								

ISO REFERENCE MODEL

The International Standards Organization (ISO) offers a seven-layer model defining network communication. This model allows communication software to be broken into modules. Each layer provides services needed by the next layer in a way that frees the upper layer from concern about how these services are provided. This simplifies the design of each layer.

Lower-Layer Protocols

- **Physical Layer (layer 1)**
This layer provides mechanical, electrical, functional, and procedural means to activate and deactivate physical transmission connections between datalinks.
- **Datalink Layer (layer 2)**
This layer provides functional and procedural means for connectionless-mode transmission among networks. SUPER-UX supports CSMA/CD for Ethernet.
- **Network Layer (layer 3)**
This layer provides a means of connectionless-mode transmission among transport entities. It makes transport entities independent of routing and relay considerations associated with connectionless-mode transmission. SUPER-UX supports Internet Protocol (IP) for Ethernet and HYPERchannel-DX.
- **Transport Layer (layer 4)**
This layer provides transparent data transfer between sessions and relieves them of concern about achieving reliable and cost effective data transfer. SUPER-UX supports Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). SUPER-UX also supports UltraNet (TP-4).

Upper-Layer Protocols

- **Session Layer (layer 5)**
This layer provides the services needed by protocols in the presentation layer to organize and synchronize their dialogue and manage data exchange.
- **Presentation Layer (layer 6)**
This layer manages the representation of the information that application layer protocols either communicate or reference during communication.
- **Application Layer (layer 7)**
This layer serves as the window between corresponding application processes that are exchanging information.

FIG 15

**FACT COMPONENT IDENTITY CHIPS
AND FIRMWARE MAIN SWITCH**

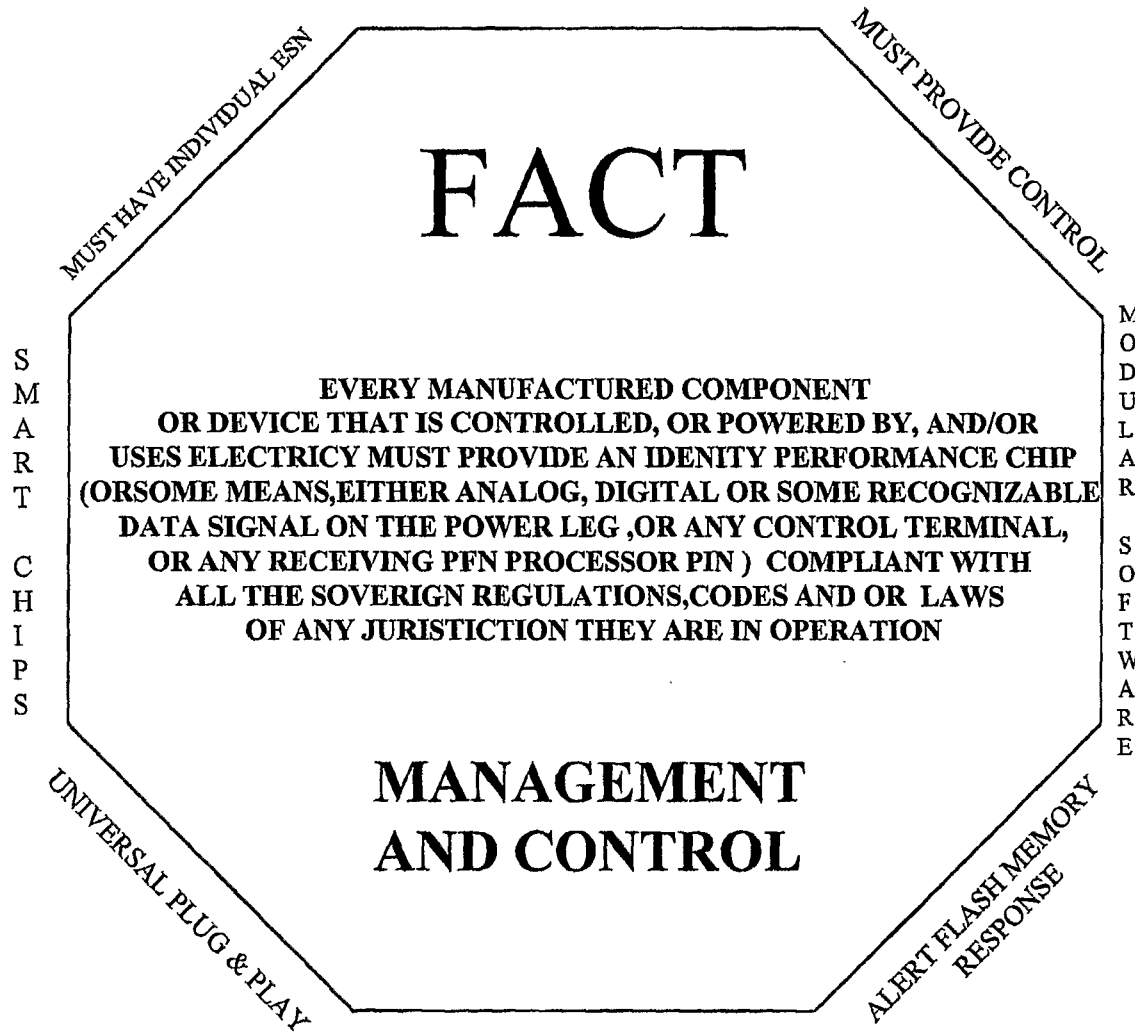


FIG.16

PFN TRAC FACT MNGT. SYS.

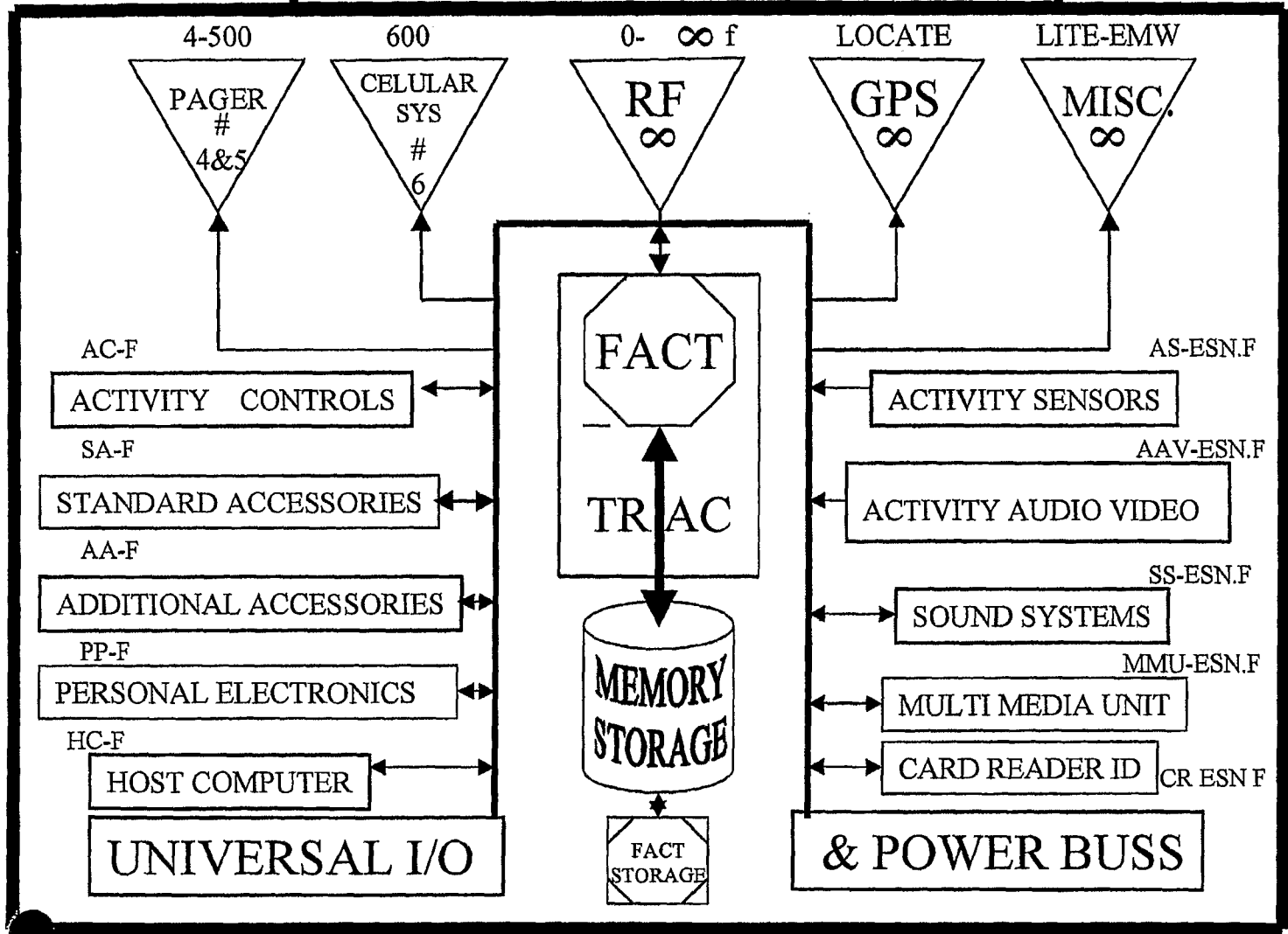


FIG 17

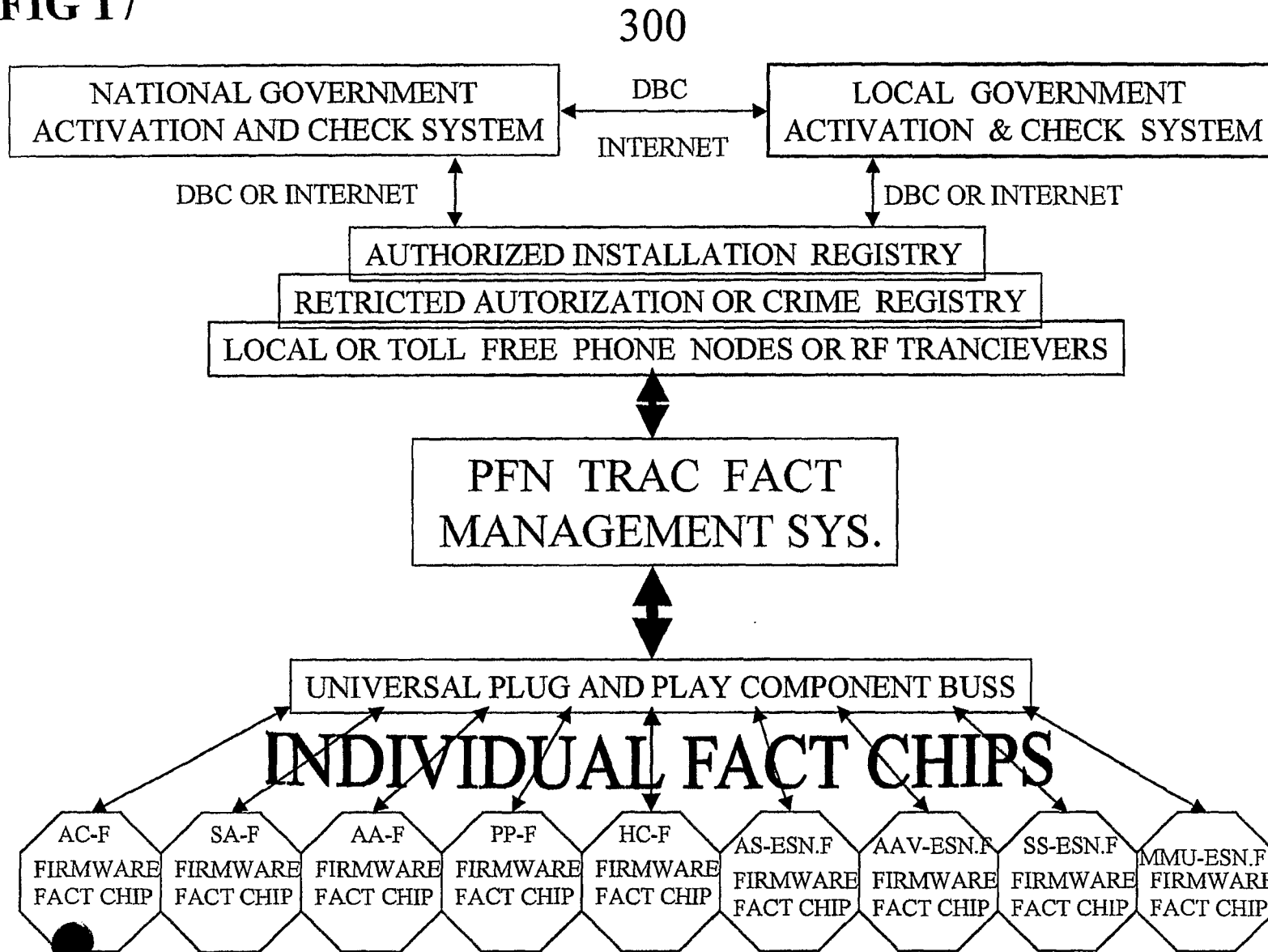
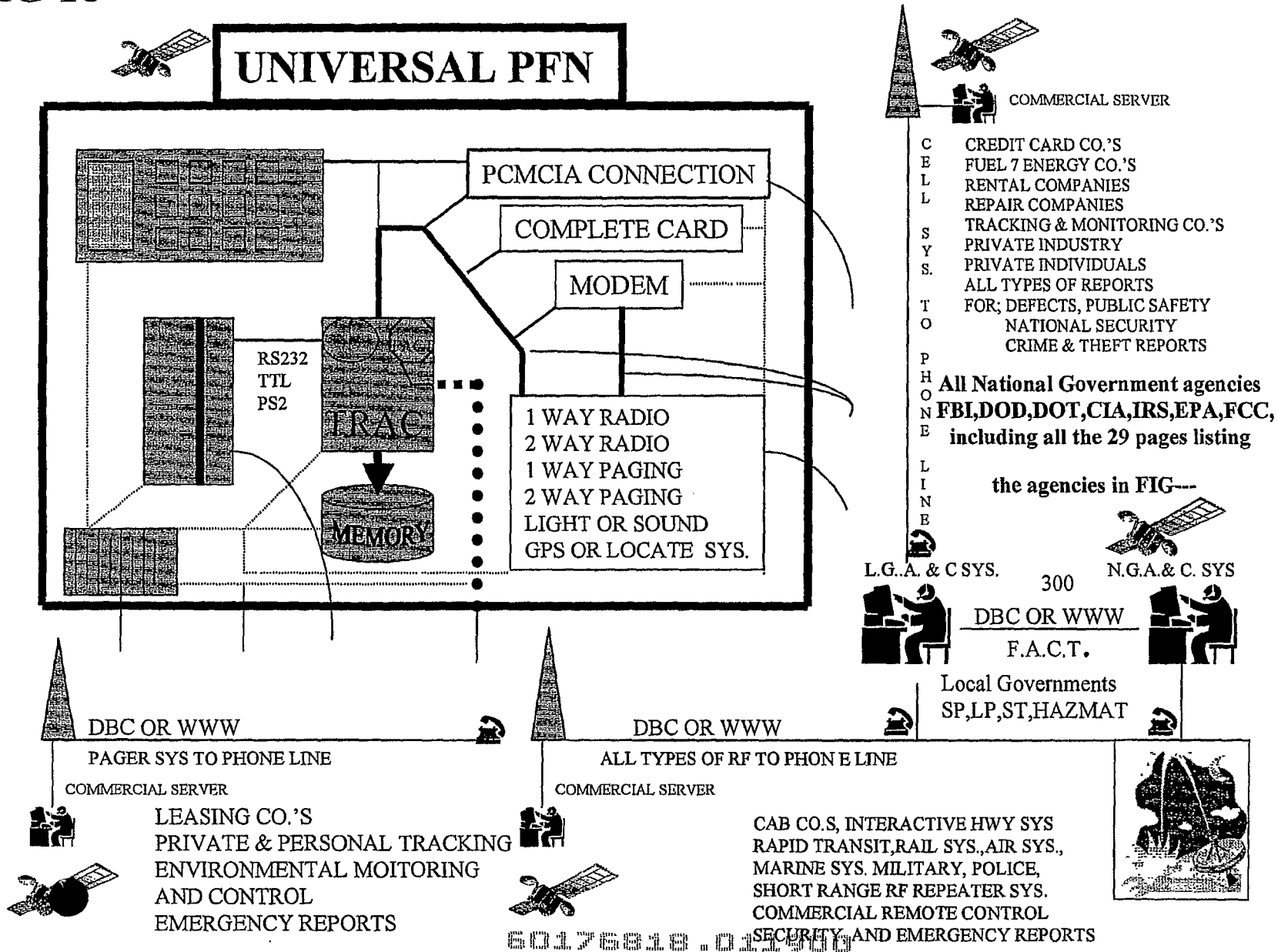


FIG 18



UNIVERSAL PFN

PCMCIA CONNECTION

COMPLETE CARD

MODEM

RS232
TTL
PS2

TRAC

MEMORY

- 1 WAY RADIO
- 2 WAY RADIO
- 1 WAY PAGING
- 2 WAY PAGING
- LIGHT OR SOUND
- GPS OR LOCATE SYS.

COMMERCIAL SERVER

- C
E
L
L
S
Y
S.
T
O
P
H
O
N
E
L
I
N
E
- CREDIT CARD CO.'S
 - FUEL 7 ENERGY CO.'S
 - RENTAL COMPANIES
 - REPAIR COMPANIES
 - TRACKING & MONITORING CO.'S
 - PRIVATE INDUSTRY
 - PRIVATE INDIVIDUALS
 - ALL TYPES OF REPORTS FOR: DEFECTS, PUBLIC SAFETY
 - NATIONAL SECURITY
 - CRIME & THEFT REPORTS

All National Government agencies
FBI,DOD,DOT,CIA,IRS,EPA,FCC,
 including all the 29 pages listing

the agencies in FIG---

L.G.A. & C SYS.

300

N.G.A. & C. SYS

DBC OR WWW

F.A.C.T.

Local Governments
 SP,LP,ST,HAZMAT

DBC OR WWW

PAGER SYS TO PHONE LINE

COMMERCIAL SERVER

- LEASING CO.'S
- PRIVATE & PERSONAL TRACKING
- ENVIRONMENTAL MOITORING AND CONTROL
- EMERGENCY REPORTS

DBC OR WWW

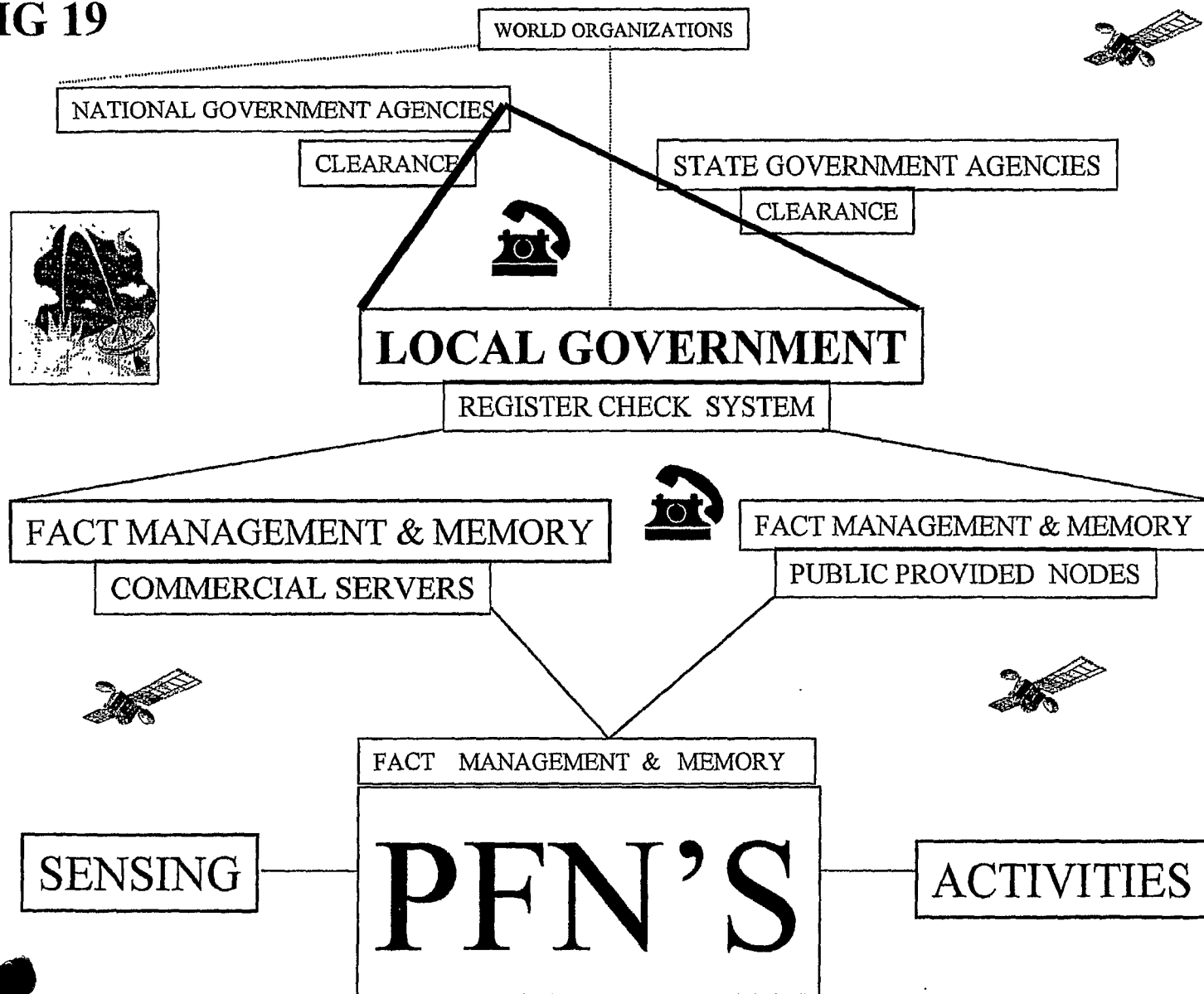
ALL TYPES OF RF TO PHONE LINE

COMMERCIAL SERVER

- CAB CO.S, INTERACTIVE HWY SYS
- RAPID TRANSIT,RAIL SYS.,AIR SYS.,
- MARINE SYS. MILITARY, POLICE,
- SHORT RANGE RF REPEATER SYS.
- COMMERCIAL REMOTE CONTROL
- SECURITY AND EMERGENCY REPORTS

60176818 . 01.11.11

FIG 19



60176818 . 01.1900

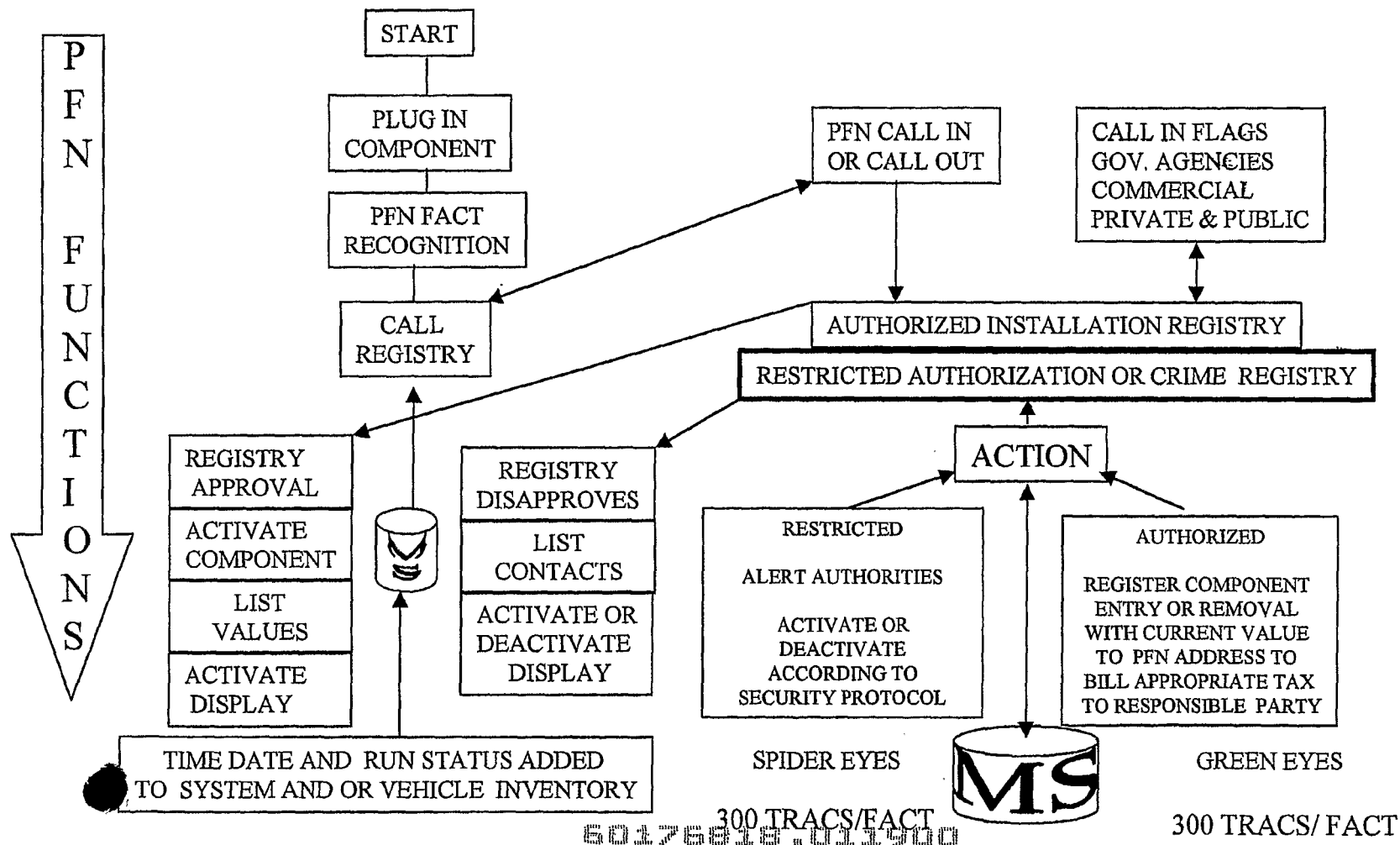
FIG 20

**SOFTWARE FLOW CHART
FOR FACT IN THE PFN**

NEW INSTALL

**SOFTWARE FLOW CHART
FOR FACT IN MAIN REGISTRY**

NEW INSTALL



300 TRACS/FACT
60176818 01.1.1990

300 TRACS/FACT

FIG 21

**SOFTWARE FLOW CHART
FOR FACT IN THE PFN**

AUTHORIZED UNIT INTERROGATION

**SOFTWARE FLOW CHART
FOR FACT IN MAIN REGISTRY**

AUTHORIZED UNIT INTERROGATION

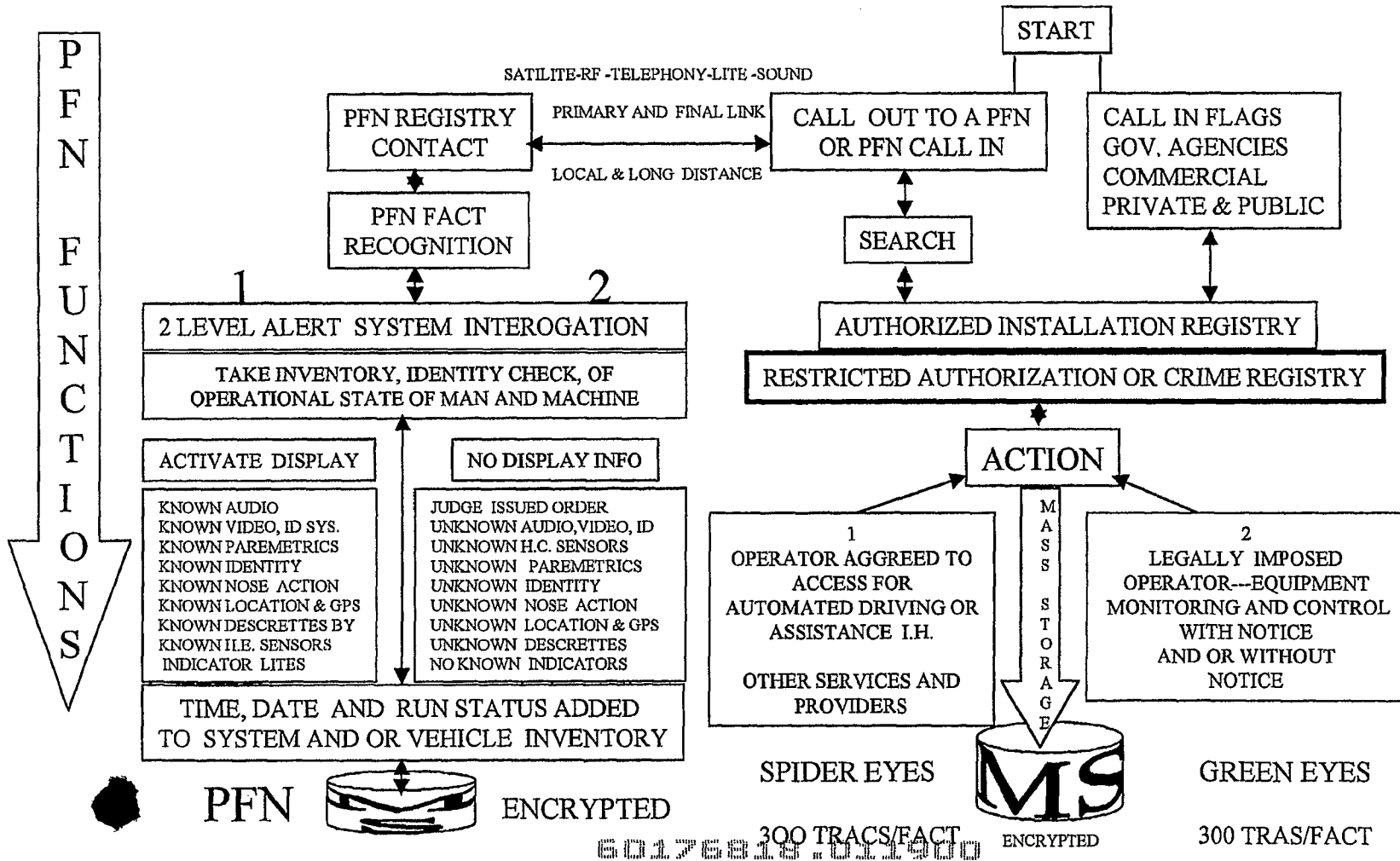


FIG 22

