

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

LENOVO (UNITED STATES) INC.,
Petitioner,

v.

INTELLECTUAL VENTURES, II LLC,
Patent Owner,

IPR2024-00124
U.S. Pat. No. 7,325,140 B2

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 7,325,140 B2**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. STATEMENT OF PRECISE RELIEF REQUESTED	1
III. THE 140 PATENT	2
A. Overview of the 140 Patent	2
B. Overview of the 140 Patent’s File History	3
C. Priority Date of the 140 Patent	5
D. Person of Ordinary Skill in the Art	7
E. Claim Construction Under 37 C.F.R. § 42.104(b)(3)	8
1. “said managed network element” (claim 1)	9
2. Means-Plus-Function Terms (claims 1, 11, 13, 14 and 16)	9
3. Limitation [1.b]: “an out of band access connection means”	10
a. Function:	10
b. Structure:	10
4. Limitation [1.c]: “virtual management interface connection means”	10
a. Function:	10
b. Structure:	11
5. Claim 11: “protection means”	11
a. Function	11
b. Structure	11
6. Claim 13: “monitoring means for monitoring the status of at least one computer network component”	11
a. Function	11
b. Structure	12
7. Limitation [14.b]: “a monitoring means for monitoring the status of the network power supply”	12
a. Function:	12

b.	Structure:.....	12
8.	Limitation [14.c] “reporting means for reporting the status of the network power supply”.....	12
a.	Function:	12
b.	Structure:.....	13
9.	Claim 16: “means for monitoring connection attempts made through the management access controller.”	13
a.	Function:	13
b.	Structure:.....	13
IV.	OVERVIEW OF THE PRIOR ART REFERENCES	13
A.	EX1005 - Neufeld	13
B.	EX1020 - IPMI.....	17
C.	PRIOR ART STATUS	19
1.	Patents	19
2.	Patent Publications.....	19
3.	Non-Patent Publications.....	20
V.	GROUND 1: NEUFELD RENDERS OBVIOUS CLAIMS 1-4, 6, 7, 10, 11, 13, AND 16.....	21
A.	Claim 1	21
1.	[1.pre].....	21
2.	[1.a]	25
3.	[1.b]	28
4.	[1.c]	32
B.	Claim 2	34
C.	Claim 3	36
D.	Claim 4	37
E.	Claim 6	38
F.	Claim 7	39
G.	Claim 10	40
H.	Claim 11	40

I.	Claim 13	41
J.	Claim 16	42
VI.	GROUND 2: NEUFELD IN VIEW OF SYVANNE RENDERS OBVIOUS CLAIMS 11 AND 12.....	43
VII.	GROUND 3: NEUFELD IN VIEW OF FOWLER RENDERS OBVIOUS CLAIM 14.....	46
A.	Limitation [14.a].....	47
B.	Limitation [14.b]	48
C.	Limitation [14.c].....	49
VIII.	GROUND 4: NEUFELD IN VIEW OF FOWLER RENDER OBVIOUS CLAIM 13.....	51
IX.	GROUND 5: IPMI IN COMBINATION WITH LAWRENCE RENDERS OBVIOUS CLAIMS 1-3, 6, 7, 10 AND 11.....	52
A.	Introduction	52
B.	Claim 1	55
1.	Limitation [1.pre]	55
2.	Limitation [1.a]	59
3.	Limitation [1.b]	61
4.	Limitation [1.c]	64
C.	Claim 2	66
D.	Claim 3	68
E.	Claim 6	69
F.	Claim 7	71
G.	Claim 10	71
H.	Claim 11	72
X.	GROUND 6: IPMI AND LAWRENCE IN COMBINATION WITH LEEDY RENDER OBVIOUS CLAIM 4	73
XI.	GROUND 7: IPMI AND LAWRENCE IN COMBINATION WITH SYVANNE RENDER OBVIOUS CLAIMS 11 AND 12	75
XII.	GROUND 8: IPMI AND LAWRENCE IN COMBINATION WITH FOWLER RENDER OBVIOUS CLAIMS 13 AND 14.....	76

A.	Claim 14	77
1.	Limitation [14.a]	77
2.	Limitation [14.b]	78
3.	Limitation [14.c]	79
B.	Claim 13	80
XIII.	GROUND 9: IPMI IN COMBINATION WITH LAWRENCE AND RFC1492 RENDERS OBVIOUS CLAIM 16.....	80
A.	Claim 16	80
XIV.	DISCRETIONARY DENIAL IS NOT WARRANTED.....	81
A.	35 U.S.C. § 314(a) Analysis.....	81
B.	35 U.S.C. § 325(d) Analysis	82
XV.	COMPLIANCE WITH FORMAL REQUIREMENTS	82
A.	Mandatory Notices Under 37 C.F.R. §§ 42.8(b)(1)-(4)	82
1.	Real Party-In-Interest.....	82
2.	Related Matters	83
3.	Lead and Backup Counsel	83
4.	Service Information.....	83
B.	Proof of Service on the Patent Owner.....	83
C.	Power of Attorney	84
D.	Standing.....	84
E.	Fees.....	84
XVI.	PRESERVATION OF RIGHTS.....	84
XVII.	CONCLUSION.....	84

INDEX OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 8,474,016
1002	U.S. Patent No. 7,325,140
1003	Declaration of Dr. Sigurd Meldal for IPR2024-00109
1004	File History for U.S. Pat. App. No. 10/969,561
1005	U.S. Pat. Pub. No. 2003/0226015 (“Neufeld”)
1006	U.S. Pat. No. 7,085,385 (“Frantz”)
1007	U.S. Patent Publication No. 2003/0097503 (“Huckins”)
1008	“PCI-to-PCI Bridge Architecture Specification”, Rev. 1.1 (“PCI Bridge Spec”)
1009	“Datasheet PCF8584 I2C-bus controller” (“PCF8584”)
1010	U.S. Pat. App. No. 09/438,253 downloaded from USPTO website (“Emerson”)
1011	U.S. Patent No. 6,219,708 (“Martenson”)
1012	U.S. Patent No. 5,651,137 (“MacWilliams”)
1013	“RFC1492: An Access Control Protocol, Sometimes called TACACS” (“RFC1492”)
1014	“RFC2865: Remote Authentication Dial In User Service (RADIUS)” (“RFC2865”)
1015	U.S. Patent No. 7,260,555 (“Rossman”)
1016	U.S. Patent Publication No. 2003/0097590 (“Syvanne”)
1017	U.S. Patent No. 7,383,577 (“Hrstar”)
1018	“RFC1157: A Simple Management Network Management Protocol (SNMP)” (“RFC1157”)
1019	Microsoft Computer Dictionary (5th ed. 2002)
1020	“IPMI – Intelligent Platform Management Interface Specification V1.5” (Rev. 1.1 dated 2/20/2002) (“IPMI”)
1021	“RFC3414: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)” (“RFC3414”)
1022	“IP Filter Based Firewalls HOWTO” (“IPFILTER”)
1023	“IPMI – Intelligent Platform Management Interface Specification V2.0” (Draft dated 9/15/2003) (“IPMIv2.0”)
1024	Reserved
1025	U.S. Patent No. 7,055,148 (“Marsh”)
1026	Reserved
1027	U.S. Patent No. 6,286,074

Exhibit No.	Description
1028	U.S. Patent No. 6,973,517
1029	U.S. Patent No. 6,189,096
1030	U.S. Patent No. 7,469,298
1031	U.S. Patent No. 6,272,537
1032	IETF Bibtex listing for RFC 3414
1033	IETF Bibtex listing for RFC 1157
1034	IETF Bibtex listing for RFC 2865
1035	IETF Bibtex listing for RFC 1492
1036	U.S. Patent No. 7,496,950
1037	“DSP0114 Alert Standard Format (ASF) Specification (“DSP0114”)
1038	U.S. Patent No. 7,263,716
1039	Declaration of Nathaniel E. Frank-White
1040	WO 01/31849 A1 (“Fowler”)
1041	Reserved
1042	District Court Claim Construction Order dated 5/28/24
1043	U.S. Patent No. 7,269,639 (“Lawrence”)
1044	U.S. Patent No. 8,605,624 (“Desai”)
1045	WO 2004/015764 (“Leedy”)
1046	Declaration of Dr. Sigurd Meldal for IPR2024-00124
1047	U.S. Patent Application No. 10/461,827

CLAIMS
[1.pre] A remote device management communication system for securely controlling access to management applications and communications to and from said management applications on network devices in a distributed computer network that includes one or more network services, one or more secure management access controllers, and one or more managed network devices, the remote device management system comprising:
[1.a] at least one secure management access controller connected to one or more data bus of said managed network device for the communication of device management data;
[1.b] an out-of-band access connection means for connecting said one or more network services or remote users with said secure management access controller for management of said network device; and
[1.c] at least one virtual management interface connection means for connecting said one or more network services or remote users with said secure management access controller; wherein said virtual management interface connection means provides logical separation of management data from user data and utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.
[2] The system of claim 1 wherein the at least one secure management access controller includes a flash chip, non-volatile random access memory and random access memory.
[3] The system of claim 1 wherein the at least one secure management access controller is embedded in the network device to be managed.
[4] The system of claim 1 wherein the at least one secure management access controller accesses a flash chip, non-volatile random access memory and random access memory embedded in a main processor on the network device.
[5] The system of claim 1 wherein the network device includes a card reader and the at least one secure management access controller is embedded in a card capable of being read by the card reader.
[6] The system of claim 1 wherein the out-of-band access connection means comprises: a communication system; and a secure management access controller interface device.
[7] The system of claim 6 wherein the communication system is selected from the group consisting of a Public Switched Telephone Network, a broadband connection and a Virtual Private Network and the interface device is selected

CLAIMS
from the group consisting of an analog modem, a broadband modem, an Ethernet interface, a cellular interface and a card slot for accepting interface cards.
[8] The system of claim 1 wherein the at least one network communication means is selected from the group consisting of a local area network, a serial interface and a network connection.
[9] The system of claim 1 wherein the at least one network communication means supports at least one protocol selected from the group consisting of Transmission Control Protocol/Internet Protocol, Simple Network Management Protocol, Telnet, Trivial File Transfer Protocol, File Transfer Protocol, Hypertext Transfer Protocol, Hypertext Transfer Protocol over Secure Socket Layer and Secure Shell.
[10] The system of claim 1 wherein user and management communications are transmitted to the at least one secure management access controller and the at least one controller further comprises a virtual management interface for separating the user communications from the management communications.
[11] The system of claim 10 wherein the virtual management interface includes a protection means for protecting the management data.
[12] The system of claim 10 wherein the virtual management interface includes a secure transmission tunnel to protect management communications and a firewall to protect the at least one management access controller from unauthorized access.
[13] The system of claim 1 wherein the at least one the management access controller includes a monitoring means for monitoring the status of at least one computer network component and a network interface for reporting a status of the at least one computer network component to a network management station.
[14.a] The system of claim 1 further comprising: a network power supply;
[14.b] a monitoring means for monitoring the status of the network power supply; and
[14.c] a reporting means for reporting the status of the network power supply.
]15] The system of claim 1 further comprising an independent power supply for supplying power to the management access controller.
[16] The system of claim 1 further comprising a means for monitoring connection attempts made through the management access controller.

I. INTRODUCTION

U.S. Patent No. 7,325,140 (“the 140 patent,” EX1002) should never have been allowed by the examiner. The independent claim of the 140 patent is directed to the concept of providing in-band and out-of-band connections to a secure management access controller on a network device in order to allow an administrator to manage the network device remotely. These concepts were all well-known in the art as the 140 patent acknowledges. EX1002, 2:1-3:67. Allowance of the 140 patent was obtained by amending the independent claim to include low-level implementation details including a requirement for bus-based communication of management data, and a virtual management interface connection that logically separates management data from user data for the in-band connection. These implementation details were also well-known; the prior art patents and documents discussed herein disclose all of these concepts. The challenged claims of the 140 Patent should be found unpatentable in view of this prior art, which was not considered by the examiner.

II. STATEMENT OF PRECISE RELIEF REQUESTED

In accordance with 35 U.S.C. § 311, Petitioner requests cancelation of claims 1-4, 6, 7, 10-14 and 16 of the 140 patent in view of the following grounds:

Ground	Claims	Basis	Prior Art
1	1-4, 6, 7, 10, 11, 13 and 16	§103	Neufeld

Ground	Claims	Basis	Prior Art
2	11, 12	§103	Neufeld and Syvanne
3	14	§103	Neufeld and Fowler
4	13	§103	Neufeld and Fowler
5	1-3, 6, 7, 10, 11	§103	IPMI and Lawrence
6	4	§103	IPMI, Lawrence and Leedy
7	11, 12	§103	IPMI, Lawrence, and Syvanne
8	13, 14	§103	IPMI, Lawrence and Fowler
9	16	§103	IPMI, Lawrence and RFC1492

III. THE 140 PATENT

A. Overview of the 140 Patent

The 140 patent was filed on October 20, 2004, and issued on January 29, 2008. The 140 patent relates to remote management of network devices, *e.g.*, routers, in a secure manner. EX1002, 1:19-45 and 2:1-7. The 140 patent discloses including in a managed network device a “remote management access controller,” which is referred to as a “SMACC” (“Secure Management Access Control for Computer Chipset”) in some embodiments, that can be accessed by a remote administrator at a remote management center for the exchange of management communications to manage the network device. EX1002, 5:47-6:2. The 140 patent also discloses separating user traffic from device management traffic, logically and/or physically, both in the managed network device and while the management communications are in transit to the remote management access controller. EX1002, 4:12-14; 6:5-8. The remote management access controller has two types

of connections over which management communications can be exchanged with the remote management center: an in-band connection and an out-of-band connection. EX1002, 6:12-24; 11:60-12:4. On the in-band connection, management traffic is commingled with user traffic and a Virtual Management Interface (VMI) employs virtual private network (VPN) technology to provide logical separation of the management traffic from user data traffic. 6:24-33; 12:4-21. The out-of-band connection includes a SMACC Network Enabled Management Interface, which provides a dedicated, physically separate interface for the management network connection. EX1002, 12:22-36.

B. Overview of the 140 Patent's File History

The examiner rejected independent claims over prior art referred to as Nessett. EX1004, 88 (11/2/06 Rejection at 2). In response, the applicant amended the claims substantially by introducing new limitations requiring a (1) “controller connected to **one or more data bus** for the communication of device management data” (**emphasis added**) (2) “an out-of-band access . . . for management of said network,” and (3) “virtual management interface connection means” that connects to the secure management access controller and provides logical separation of management data from user data. EX1004, 104 (4/3/07 Response at 2). The applicant asserted that the data bus-based connection between a secure management access controller and a network device was supported by ¶¶ 0019 and

0056 and Figure 28 in the specification of the 140 patent application. EX1004, 108 (4/3/07 Response at 6). Although not explicitly stated, the “data bus-based connection between the secure management access controller is presumably the “SMACCI Bus” in Figure 28 below, which connects the SMACC Processor to the network device via the Bus Controller and the System PCI Bus.

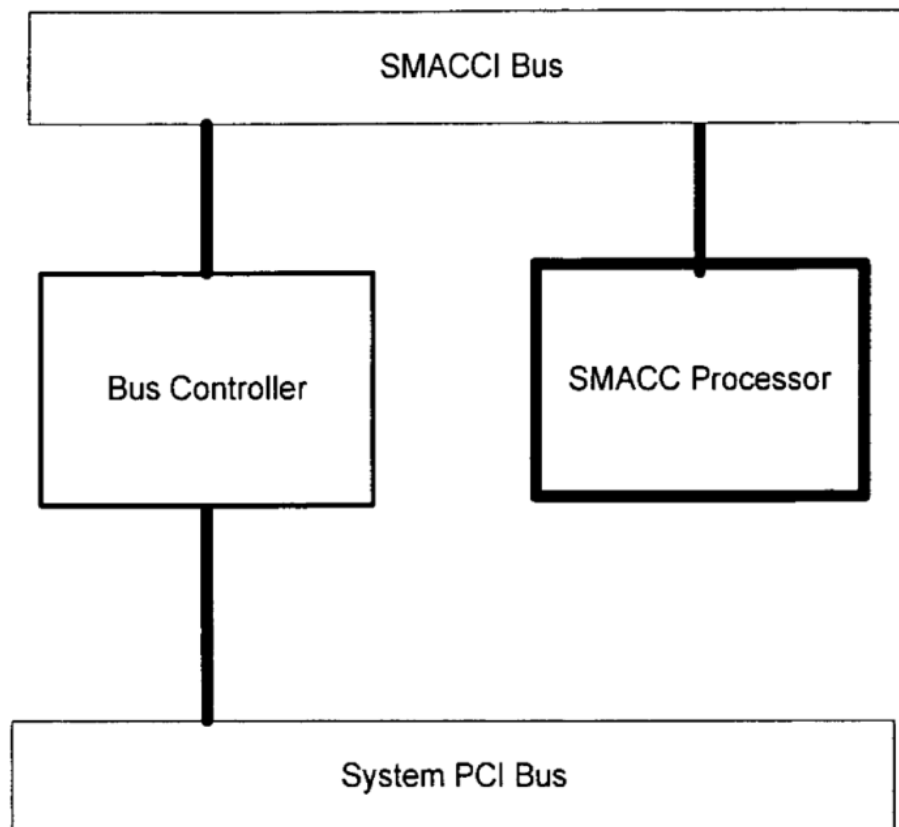


Fig. 28

The applicant argued that Nessett does not teach or suggest a data bus connection between a secure management access controller and the managed device, or the communication of device management data over such a connection,

as recited by the amended independent claims. EX1004, 108 (4/3/07 Response at 6). Independent claim 1 and all dependent claims 2-16 were allowed in response to these amendments and arguments. EX1004, 141 (9/6/07 NOA at 2).

C. Priority Date of the 140 Patent

The 140 patent is not entitled to any priority date earlier than 10/21/2003, which is the filing date of Provisional App. No. 60/512,777 to which the 140 patent claims priority. EX1002, 1.

The 140 patent also claims priority as a continuation-in-part of U.S. Pat. App. No. 10/461,827 (the “827 application”) filed 6/13/2003 (EX1047). However, no claim of the 140 patent is entitled to that priority. The claims of the 140 patent all require “at least one secure management access controller connected to one or more data bus of said managed network device for the communication of device management data.” EX1002, 22:40-44 (the “Bus Limitation”). The 140 patent illustrates a direct connection between a SMACC and both a system bus and a CPU bus of a network device as shown in, for example, Fig. 1 below.

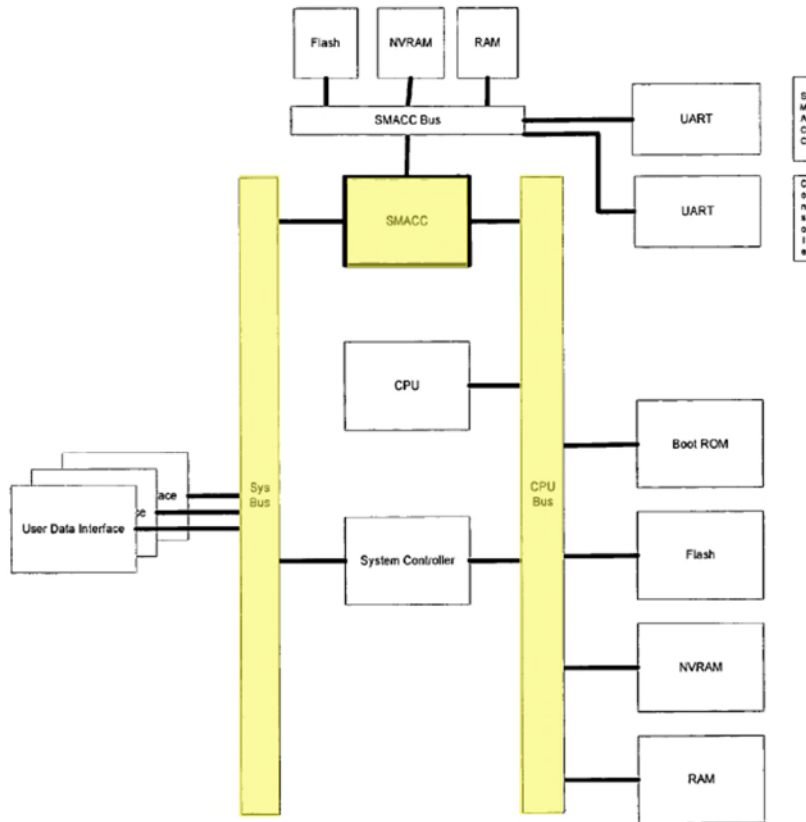


Fig. 1

In view of this disclosure in Fig. 1, the scope of the Bus Limitation of claim 1 is broad enough to include direct connections of the SMACC to at least two busses of the managed network device regardless of whether the Bus Limitation is limited to direct connections to the busses.

The 827 application, however, fails to disclose any direct connection of a “secure management access controller” to any bus of a managed network device, let alone a direct connection to two data busses of a managed network device as would be required to support the full scope of the Bus Limitation. In fact, the 827 application does not even mention the word “bus.” EX1047, *passim*. This is not

surprising because the 827 application is primarily directed toward a *stand-alone* “secure remote management appliance” without any direct connection to a bus of a network device. EX1047, ¶[36]. This is in direct contrast to the 140 patent, which is primarily directed toward the embedded SMACC concept illustrated above in Fig. 1 of the 140 patent. While the 827 application indicates in ¶[36] that the disclosure is not limited to the “preferred exemplary embodiment” of a stand-alone device, the 827 application does not provide any detail about how other embodiments would be implemented other than to state that the features of the “preferred exemplary device . . . also can be combined with other hardware and software features such as being integrated with a modem or with the console of a device.” EX1047, ¶[36]. That disclosure does not provide written description support or enablement for the full scope of the Bus Limitation which includes an embedded SMACC directly connected to two busses of a managed network device as discussed above. Accordingly, no claim of the 140 patent – all of which include the Bus Limitation – is entitled to priority to the 827 application.

D. Person of Ordinary Skill in the Art

A person of ordinary skill in the art (“POSITA”) at the time of the alleged invention of the 140 patent would have had a Bachelors’ degree in electrical or computer engineering or a comparable field of study, plus approximately two to three years of professional experience in the field of computer and/or network

design and security or other relevant industry experience. Additional graduate education could substitute for professional experience, and significant experience in the field could substitute for formal education. EX1046, ¶54.

E. Claim Construction Under 37 C.F.R. § 42.104(b)(3)

The Challenged Claims are interpreted using the same claim construction standard that is used to construe the claim in a civil action in federal district court. 37 C.F.R. § 42.100(b). Certain claim terms below have been construed in accordance with the district court's claim construction (EX1042) in the Related Litigation (defined below in Section XIV.A). All terms of 140 patent not specifically addressed below should be construed according to their plain and ordinary meanings.

Petitioner does not contend that its proposed constructions are complete constructions of these limitations or the claims for any other purpose, including for issues that have been raised in the related litigation. Because the prior art asserted herein discloses the preferred embodiment within the indisputable scope of the claims, the Board need not construe the outer bounds of the claims as part of these proceedings. The district court may have to address outer bounds of the claims in addressing infringement. *See, e.g., Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) (providing that only those

terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy).

1. “said managed network element” (claim 1)

For the purposes of this IPR, this term should be construed to mean “said managed network device.” EX1046, ¶58.¹

2. Means-Plus-Function Terms (claims 1, 11, 13, 14 and 16)

For the purposes of this IPR, Petitioner adopts the district court’s construction of the following means-plus-function terms in the Related Litigation. The scope of a means-plus-function claim term is limited to the structures, materials and acts that perform the identical claimed function or functions and that are identical or equivalent to those disclosed in the specification.

¹ Petitioner may take the position in the parallel district court case that the lack of antecedent basis renders this term indefinite. The construction provided in this Petition satisfies Petitioner’s obligation under 47 C.F.R. § 42.100(b)(3). IPR2022-00980, Paper 14, 11-12 (PTAB, 12/5/22) (“[N]or are we persuaded that Petitioner’s position that this term is indefinite . . . in a parallel district court proceeding, is fatal to its Petition.”).

3. Limitation [1.b]: “an out of band access connection means”

a. Function:

As recited in claim 1, the function performed by this claim element is “connecting said one or more network services or remote users with said secure management access controller for management of said network device”. EX1042,

2.

b. Structure:

As determined by the district court in the Related Litigation, the corresponding structure is one or more of the following networks: a Public Switched Telephone Network (PSTN) (2:45-57, 3:2-4, 12:37-61), an Integrated Services Digital Network (ISDN) (2:45-57), a cellular network (6:14-21, 7:60-62, 12:37-61), an Ethernet network (12:37-61), a wireless network, and/or a Digital Subscriber Line (DSL) (12:37-61, 15:55-60), where the one or more networks use one or more of the following protocols: SNMP, TFTP, FTP, DNS, SysLog, Telnet, SSH, HTTP, HTTPs, point to point IP, and/or XML (8:30-38). EX1042, 2-3.

4. Limitation [1.c]: “virtual management interface connection means”

a. Function:

As recited in claim 1, the functions performed by this claim element are (i) “connecting said one or more network services or remote users with said secure management access controller”; (ii) “provides logical separation of management

data from user data,” and (iii) “utilizes user interfaces of said managed network element for connecting said one or more network services or remote users with said secure management access controller.” EX1042, 3.

b. Structure:

As determined by the district court in the Related Litigation, the corresponding structure is a virtual private network (VPN) (6:22-44, 6:63-7:5, 12:5-21). EX1042, 3.

5. Claim 11: “protection means”

a. Function

As recited in claim 11, the function performed by this claim element is “protecting the management data.” EX1042, 4.

b. Structure

The corresponding structures include a firewall (EX1002, 3:49-60), a virtual private network (VPN) (EX1002, 3:49-60), or a combination of a firewall, VPN, and authentication and authorization applications (EX1002, 6:22-7:6). EX1042, 4.

6. Claim 13: “monitoring means for monitoring the status of at least one computer network component”

a. Function

As recited in claim 13, the function performed by this claim element is “monitoring the status of at least one computer network component.” EX1042, 5.

b. Structure

The corresponding structure a processor performing an algorithm to monitor network components for loss of connectivity by testing the network connection (7:25-44, 17:50-18:4, 18:20-32, 21:13-65, FIGS. 15-16), or an uninterruptable power supply (UPS) that monitors network components for loss of external power (11:25-46, 18:33-51, 20:36-47, FIGS. 2 and 17). EX1042, 5.

7. Limitation [14.b]: “a monitoring means for monitoring the status of the network power supply”.

a. Function:

As recited in claim 14, the function performed by this claim element is “monitoring the status of the network power supply.” EX1042, 5.

b. Structure:

The corresponding structure for performing the above-stated function is an uninterruptable power supply (UPS) that monitors network components for loss of power (11:25-46, 18:33-51, 20:36-47, FIGS. 2 and 17). EX1042, 5.

8. Limitation [14.c] “reporting means for reporting the status of the network power supply”

a. Function:

As recited in claim 14, the function performed by this claim element is “reporting the status of the network power supply.” EX1042, 6.

b. Structure:

The corresponding structure for performing the above-stated function is a processor performing the algorithm disclosed at 20:24-29 or the algorithm disclosed at 21:3-12. EX1042, 6.

9. Claim 16: “means for monitoring connection attempts made through the management access controller.”

a. Function:

As recited in claim 16, the function performed by this claim element is “monitoring connection attempts made through the management access controller.” EX1042, 6.

b. Structure:

The corresponding structure for performing the above-stated function is an Access Control Server (ACS) using protocols to authenticate and authorize access (19:44-64), or a processor running one or more of RADIUS, TACACS+ and/or LDAP (6:22-57, 7:7-24, 15:26-39; *see also* 4:37-40, 8:13-19). EX1042, 6.

IV. OVERVIEW OF THE PRIOR ART REFERENCES

A. EX1005 - Neufeld

Neufeld is entitled “Method and Apparatus for Configuring Security Options in a Computer System.’ EX1005, 1. Neufeld’s background section discusses several known concepts associated with remote management of network devices, including in-band communication, which Neufeld describes as communicating

with a managed server over “a standard network connection such as the managed server’s normal Ethernet connection,” and out of-band communication over some other interface such as a modem, serial port or Ethernet interface. EX1005, ¶¶[0011]-[0012]. Neufeld also discusses on-line communications in which the managed server’s operating system is up-and-running and off-line communications in which it is not. EX1005, ¶[0014]. Neufeld explains that it is advantageous for remote server management to enable all of these communication modes. EX1005, ¶[0015]. Neufeld further discloses that security is important when communicating with a server for remote management, particularly when doing so over the Internet or a VPN. EX1005, ¶¶[0017]-[0023].

Neufeld discloses a remote management embodiment in which a managed server 2 (including a CPU 3 and a monitor 4) is remotely managed by a network administrator on a remote management PC 5 that communicates in-band with server 3 via the server’s standard network N as well as out-of-band via a Management Network M as shown below in Neufeld’s Fig. 1:

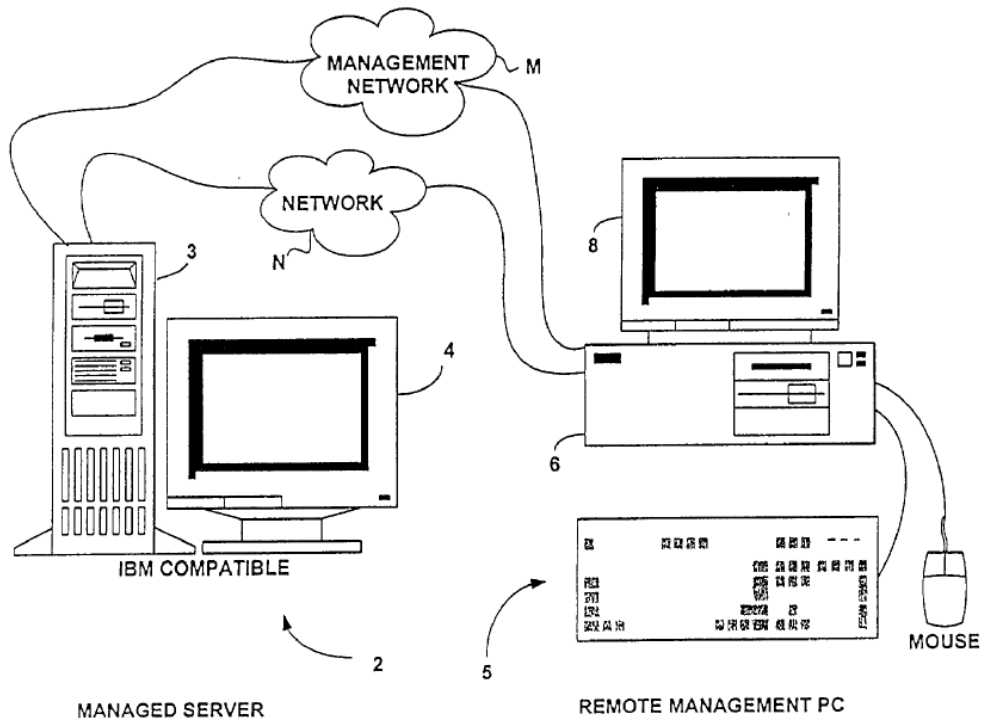
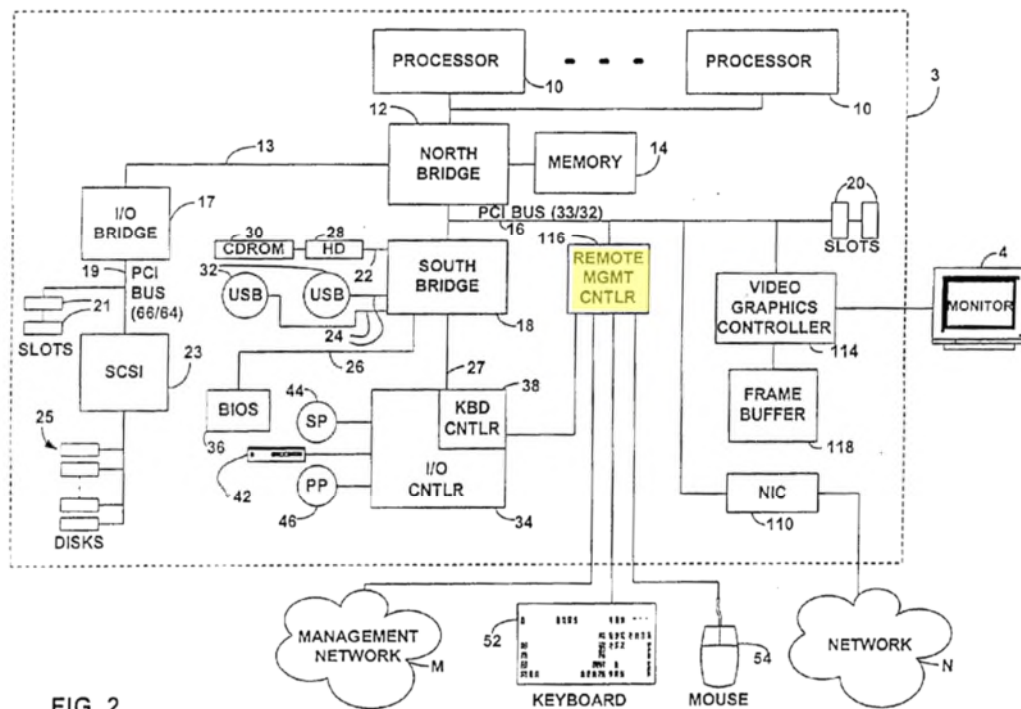


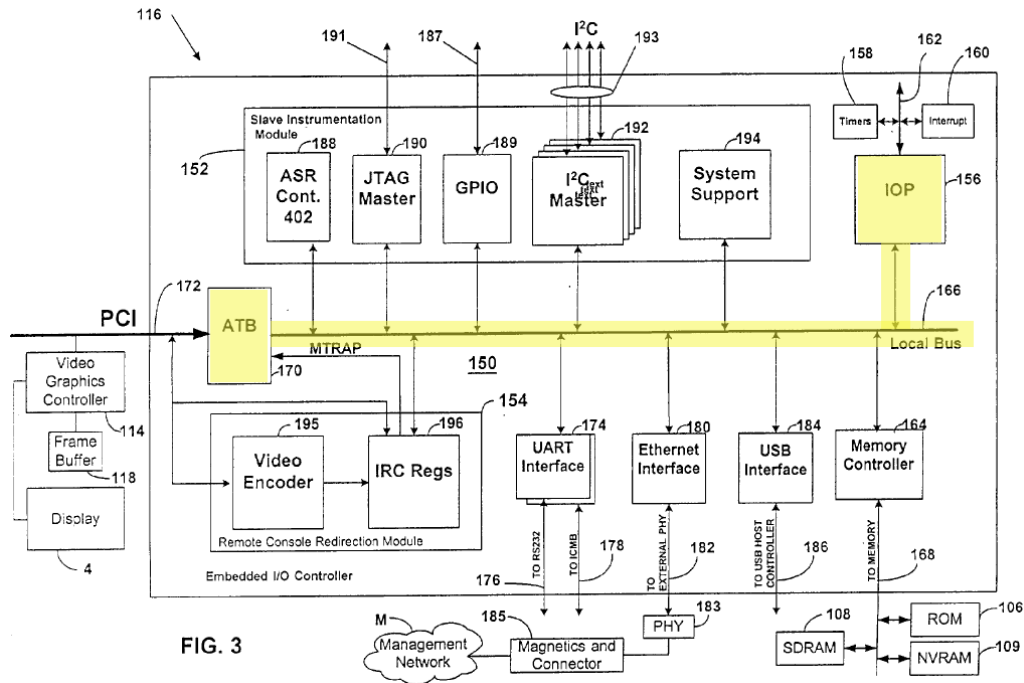
FIG. 1

The remote management PC 5 manages the server 2 by communicating with a remote server management controller 116 connected to the PCI bus 16 of the CPU 3 as shown in Fig. 2:²

² Annotations and highlighting added unless otherwise noted.



The remote server management controller 116 includes a processor, IOP (input/output processor) 156, which is connected to a local bridge 166 that in turn is connected to ATB (address translation and bridging unit) 170 that connects the remote management controller to the PCI bus 172 of the managed server's CPU 3 as shown in Fig. 3 below. The server's Network Interface Controller ("NIC") 110 is also connected to the PCI bus 172 as shown above.

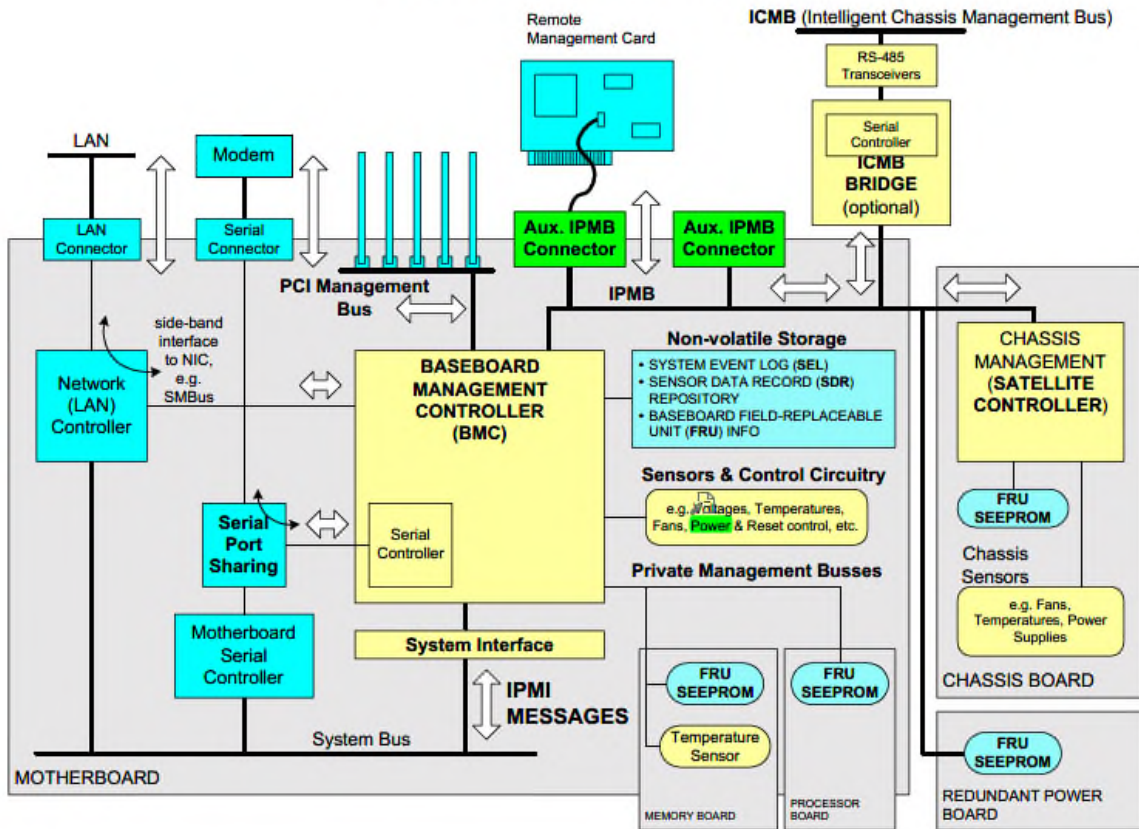


Also connected to the local bus 166 are a slave instrumentation panel 152 which allows the IOP 156 to control functions of the managed server 2 (e.g., rebooting it), and interfaces that provide for out-of-band communication such as the UART 174 and the Ethernet Interface 180.

B. EX1020 - IPMI

IPMI is a specification that “define[s] standardized, abstracted interfaces to the platform management subsystem.” EX1020, 1. “Platform management” refers to “the monitoring and control functions that are built into the platform hardware and primarily used for the purposes of monitoring of health of the system hardware.” *Id.* Fig. 1-2 below (green highlighting over power added, remainder in original) is a block diagram showing the main elements of an IPMI implementation:

Figure 1-2, IPMI Block Diagram



The heart of the system is the Baseboard Management Controller (BMC). The “BMC provides the intelligence behind the intelligent platform management” and (i) manages the interface between the system management software and the platform management hardware, (ii) provides autonomous monitoring, event logging, and recovery control, and (iii) serves as the gateway between system management software and the Intelligent Chassis Management Bus (“ICMB”) and Intelligent Peripheral Management Bus (“ICPB”). EX1020, 9. IPMI provides multiple different interfaces to the platform management system including, as shown above, a modem connected to a serial port which can be used for

communications over, e.g., the PSTN, a remote management card, the ICMB, ICPB (all corresponding to out-of-band connections), and via the system's "LAN connector" as shown in the upper left-hand corner of Figure 1-2 (an in-band connection). IPMI, 10.

Additional prior art relied on for the challenges herein will be discussed in connection with those challenges below.

C. PRIOR ART STATUS

Neufeld, IPMI and the additional prior art documents relied on in this Petition qualify as prior art on the following statutory bases:

1. Patents

Exhibit No.	Name	Filing Date	Issue Date	Statutory Basis
1006	Fowler	10/26/2000	5/3/2001	102(b), 102(e)
1043	Lawrence	12/13/2000	9/11/2007	102(e)

2. Patent Publications

Exhibit No.	Name	Filing Date	Publication Date	Statutory Basis
1005	Neufeld	5/31/2002	12/4/2003	102(e)
1016	Syvanne	11/19/2001	5/22/2003	102(a), 102(e)
1045	Leedy	8/8/2003	2/19/2004	102(e)

3. Non-Patent Publications

Each of the following documents bears an indicia of publication and/or is supported by additional evidence of publication.

EX1013 (RFC1492) is prior art under §102(b) because it was published in July 1993 as evidenced by EX1013 at 1 (“Distribution of this memo is unlimited”; FRE §803(16)), by its citation in EX1029, 9:36-38, and by its IETF “bibtex” listing (EX1035, 1).

EX1020 (IPMI) is prior art under §102(b) because it was published on 2/2/2002 as evidenced by EX1020, 1; and by its citation in IPMIv2.0. EX1023, 6.

EX1022 (IPFILTER) is prior art under §102(b) because it was published on 8/28/2000. EX1022, 2; EX1039, 1, 2 and 36-64 (copy of EX1022).

EX1023 (IPMIv2.0) is prior art under §102(a) because it was published on 9/15/03. EX1023, 1; EX1039, 1-2 (signed declaration from the Record Request Processor at the Internet Archive) and 110-182 (authenticated copy of the Internet Archive’s record of the archived file for the URL and date specified by https://web.archive.org/web/20031002054319/http://www.intel.com/design/servers/ipmi/RMCP+_and_SOL_Proposals.pdf).

V. GROUND 1: NEUFELD RENDERS OBVIOUS CLAIMS 1-4, 6, 7, 10, 11, 13, AND 16

A. Claim 1

1. [1.pre]

To the extent the preamble is limiting, Neufeld discloses it. In Neufeld, the claimed “remote device management communication system” includes one or more managed servers 2 connected to a remote console 5 by a network N and a management network M. EX1005, ¶[0034] and Fig. 1. The claimed “managed network devices” are the managed servers 2. EX1046, ¶90.

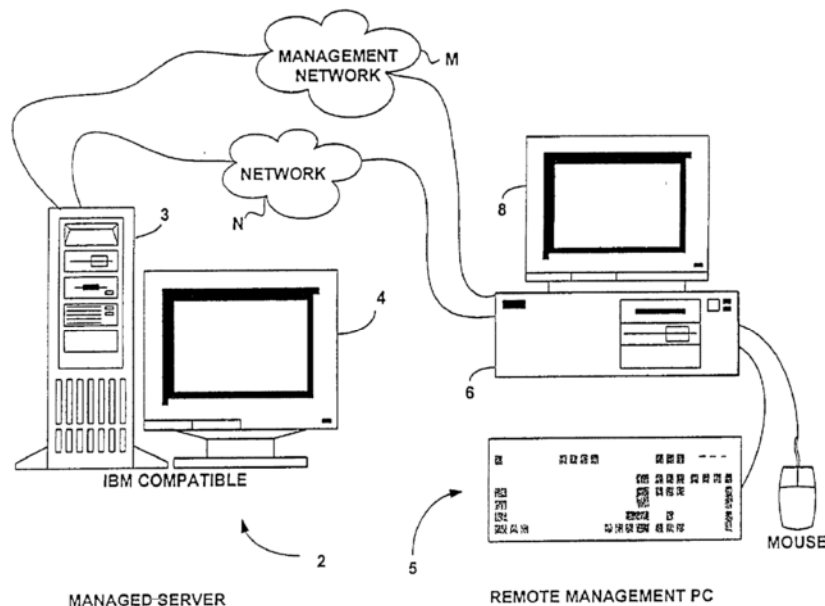
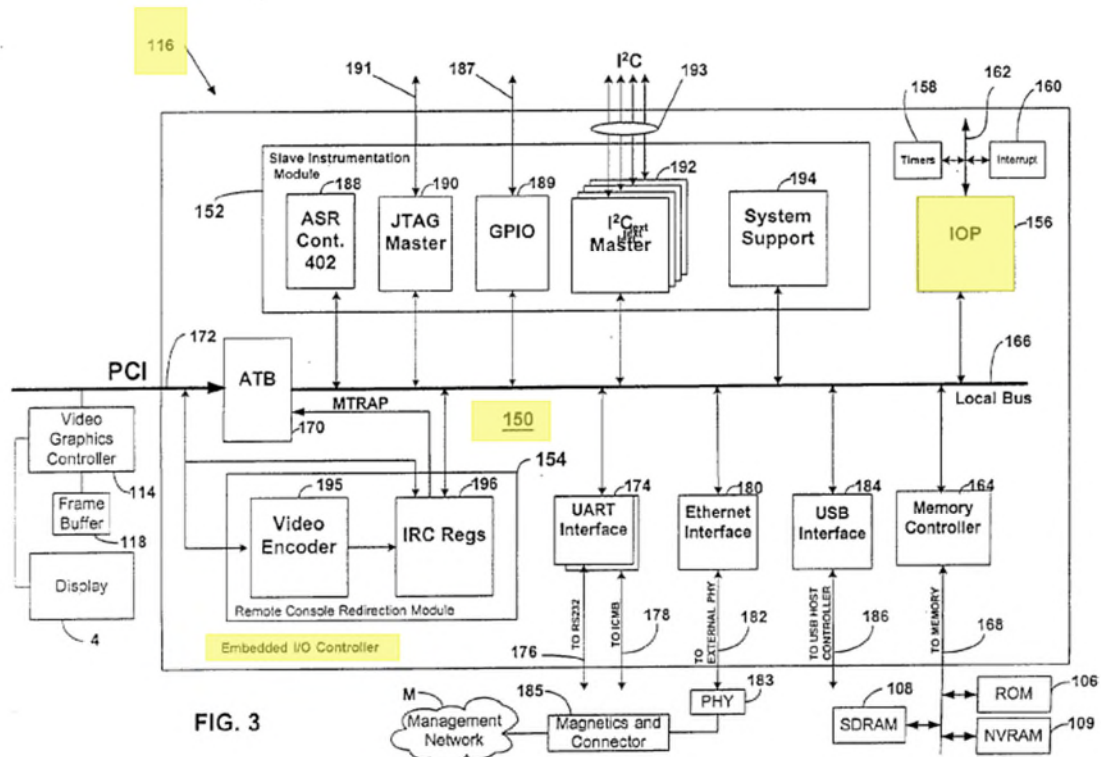


FIG. 1

The network N can be any sort of network capable of transmitting data between two devices. EX1005, ¶[0035]. The managed server 2 includes a CPU 3 that houses a remote server management controller 116, which in some embodiments is implemented using a single ASIC for the embedded I/O controller

150. EX1005, ¶¶[0034], [0051-[0053], Figs. 2-3. The remote server management controller 116 is the claimed “secure management access controller.” EX1046, ¶91.



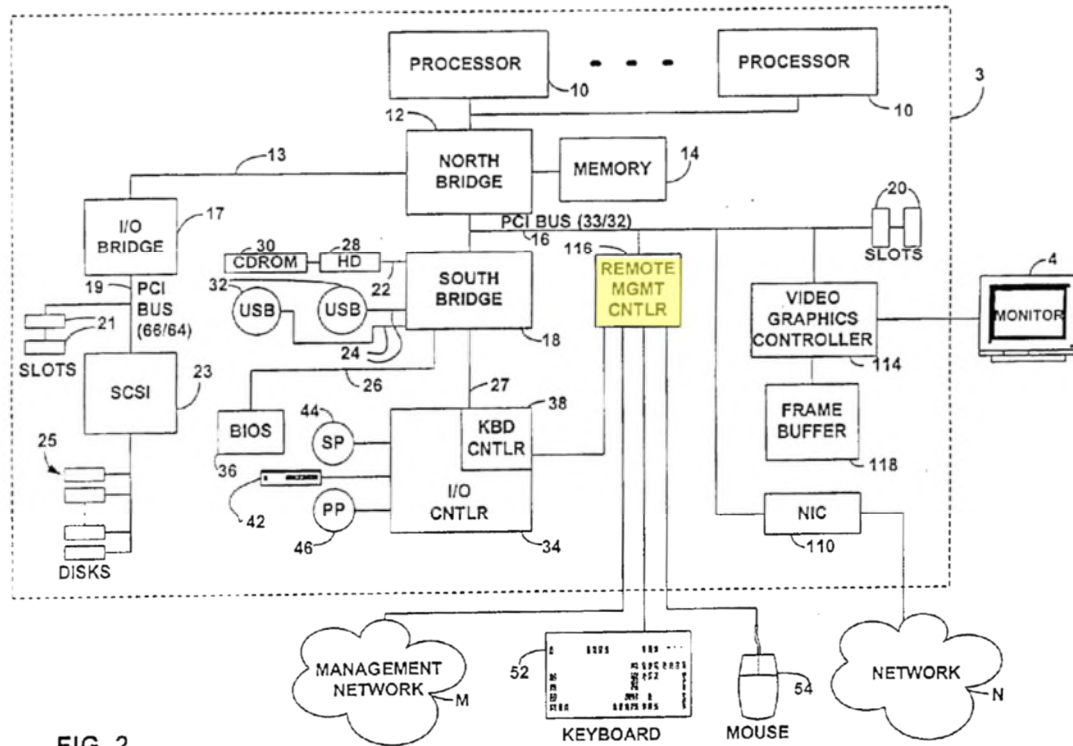


FIG. 2

The embedded I/O controller 150 includes an Input/Output processor (“IOP”) 156. The IOP 156 is coupled to functional modules of the remote server management controller 116. EX1005, ¶[0034]. The IOP 156 “provides general control and functions as a management processor for the remote server management controller 116”. EX1005, ¶[0054]; EX1046, ¶92.

The claimed “management applications” are access control and monitoring applications which are performed by the remote server management controller 116 to provide for ‘lights out’ management.” EX1005, ¶[0076]. These applications on the remote server management controller 116 implement critical functions (e.g., booting and powering down the managed server, modifying flash ROM/firmware),

moderately critical functions (e.g., altering user profiles, performing or suppressing backups) and non-critical functions (e.g., file/device sharing, altering directories). EX1005, ¶[0080], Table 1. These management functions described in Neufeld correspond to the types of management functions described in the 140 patent, including controlling the boot process and performing configuration commands and updates. EX1002, 11:41-44, 17:29-30; EX1046, ¶93. Moreover, the IOP 156 dictates control and monitoring functions in managed server 2. EX1005, ¶[0066]. The IOP 156 securely controls access to management applications by providing to the network device “functionality for accessing, interacting, and monitoring the managed server 2” EX1005, ¶[0034]; EX1046, ¶94.

Neufeld’s remote device management communication system controls communications to and from management applications by establishing an “out-of-band communication session with the remote server management controller 116.” EX1005, ¶[0034]. As disclosed by Neufeld, there are several methods for establishing communications to and from the managed server 2. “In out-of-band communication, a ‘back door’ communication channel is established by a remote server management tool (such as a remote console or terminal emulator) using some other interface with the server (such as (1) through the server's modem, (2) via a direct connection to a serial port, (3) through an infrared communication port,

or (4) through an Ethernet interface or the Internet).” EX1005, ¶[0012]; EX1046, ¶95.

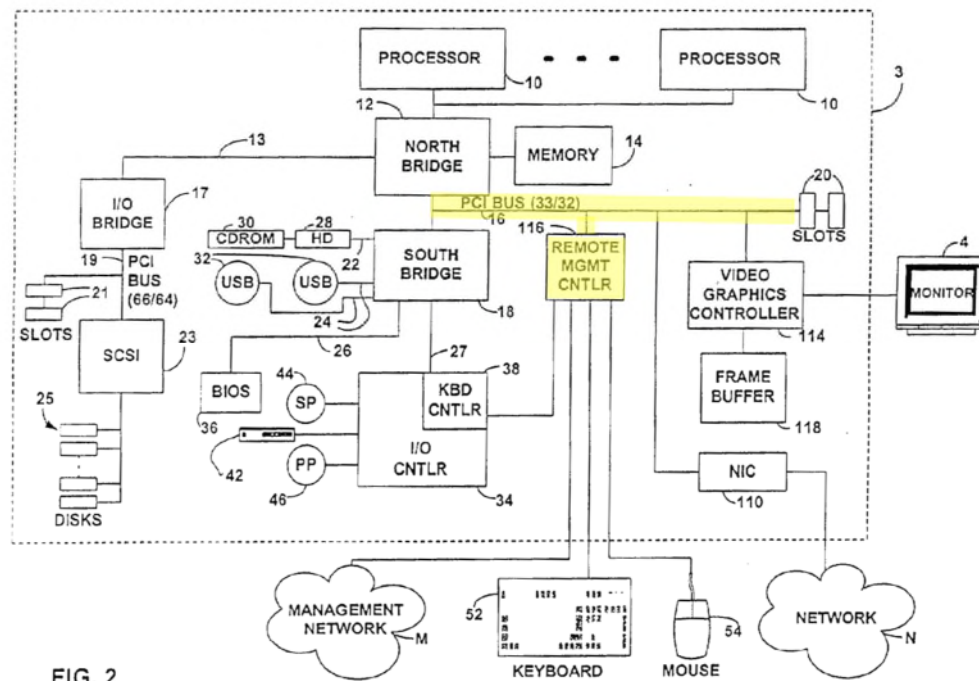
The claimed “distributed network” includes the devices in networks N and M including the client computers such as managed server(s) 2 and remote management PC(s) 5 as well as other client computers. EX1005, ¶[0083]; *see also id.* ¶[0008] (discussing distributed networks including a large number of servers connected to numerous client computers). Neufeld further discloses that the network N can include the public Internet, which inherently includes large numbers of servers, client computers, and devices such as routers. EX1005, ¶¶ [0035], [0088], EX1046, ¶96.

The claimed “network services” include sharing of files and printers (EX1005, ¶[0007]), Emergency Management services (“EMS”) (EX1005, ¶[0074]) directory service and authentication and encryption services (EX1005, ¶[0076]). Additionally, Neufeld discloses that the network N can include the public Internet, which inherently includes network services such as Domain Name Service (“DNS”). EX1005, ¶¶ [0035], [0088]; EX1046, ¶97 (explaining that the public Internet inherently includes DNS servers that provide DNS services).

2. [1.a]

Neufeld discloses this limitation. As discussed above for limitation [1.pre], Neufeld’s remote server management controller 116 including the Input/Output

Processor (IOP) 156 is the claimed “secure management access controller,” and managed server 2 is the claimed “managed network device.” Neufeld discloses that the remote server management controller 116 is connected to PCI bus 16/172 that is a data bus of the managed server 2. EX1005, ¶¶[0043], [0057], Figs. 2-3; EX1046, ¶99.

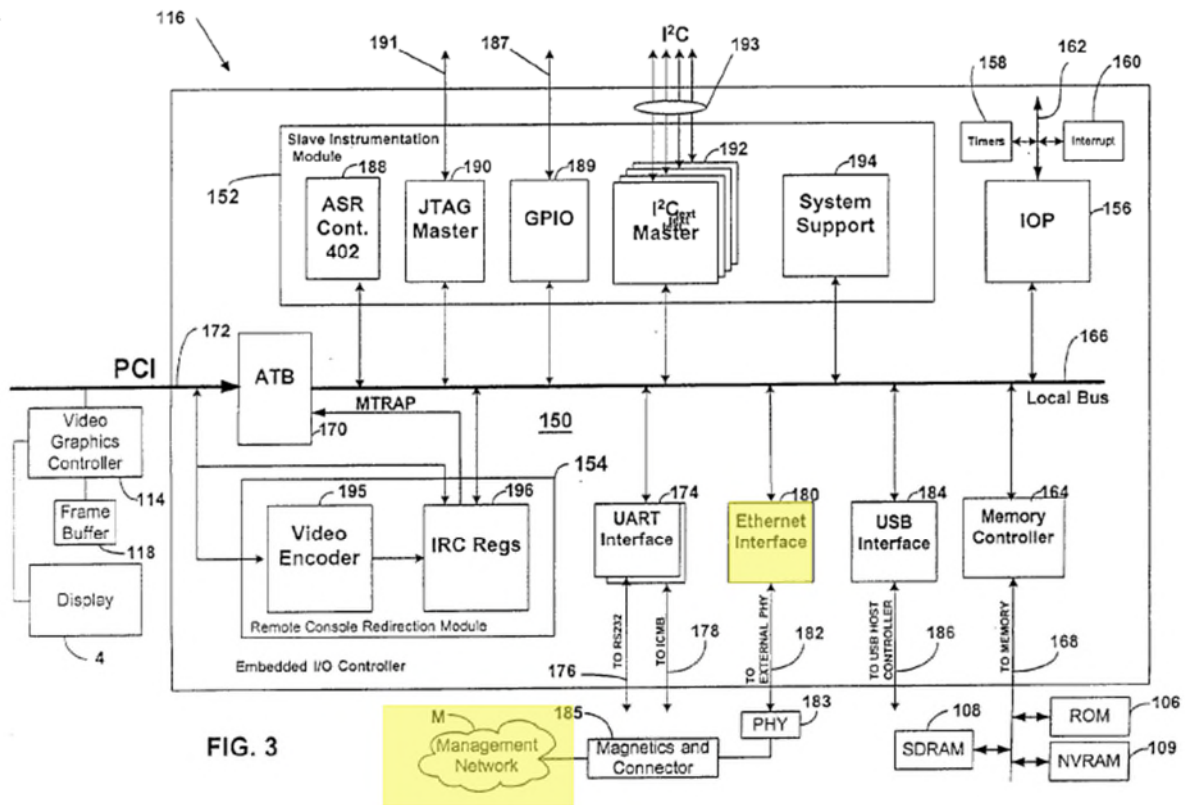


discloses that management messages are communicated to the remote server management controller 116 via the connection to the PCI bus 16/172. Such device management data travels across PCI bus 16/172 between the remote server management controller 116 and the components with which it communicates. EX1046, ¶100.

3. [1.b]

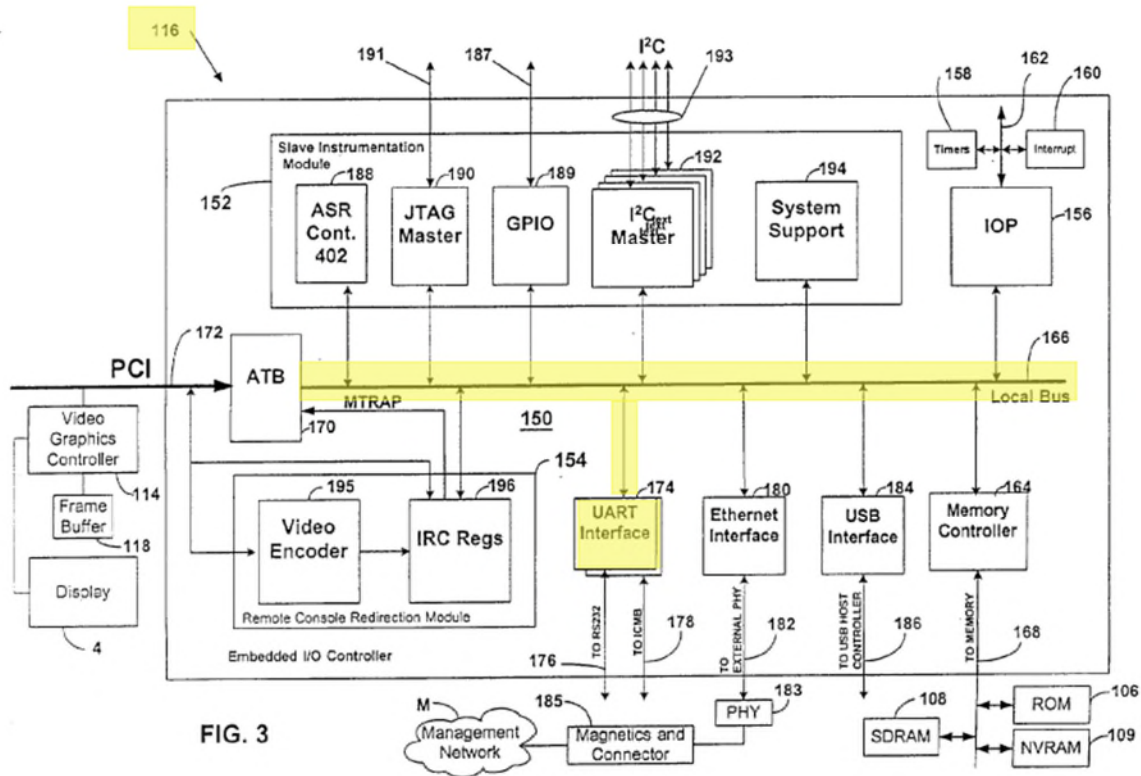
Neufeld discloses and renders obvious this limitation. As discussed in Section III.E.3, the function performed by the “out-of-band connection means” in this claim is “connecting said one or more network services or remote users with said secure management access controller,” and the corresponding structures for performing this function include at least an Ethernet network or the PSTN. EX1046, ¶102.

Neufeld’s remote server management controller 116, includes an Ethernet interface 180 connected to a Management Network M to provide the main external communication interface between the remote server management controller 116 and the outside world. EX1005, ¶[0061].



Neufeld's Management Network M connected to the Ethernet interface 180 is the same as, or is at least equivalent to, one of the corresponding structures disclosed by the 140 patent for this limitation, the Ethernet network. EX1002, 12:37-46; EX1046, ¶101. Neufeld's Management Network M performs the identical function as the 140 patent's Ethernet network, namely connecting a remote user (e.g., a remote administrator) at remote management PC 5 via network M with the remote server management controller 116 to engage in out-of-band communication of management data with the remote server management controller 116. EX1005, ¶¶[[0043], [0062]; EX1002, 12:37-46; EX1046, ¶104.

Neufeld further discloses a UART interface module 174 which is operatively coupled to internal bus 166 of the remote management controller 116.



The UART interface module 174 as disclosed by Neufeld “comprises two standard 16550 UARTs each of which may provide a separate serial communication interface.” EX1005, ¶[0059]. A “UART” is a universal asynchronous rceiver/transmitter that performs serial communication. EX1046, ¶105. Neufeld further discloses that one of these UARTs in interface module 174 may be connected to any of a wide variety of industry standard modems. EX1005, ¶[0059]. This structure is the same as, or is at least equivalent to, one of the corresponding structures for this limitation disclosed by the 140 patent, a POTS (plain old

telephone system) connection using the PSTN, which were typically implemented using modems. EX1003, 2:45-57, 3:2-4, 12:37-61; EX1046, ¶106. Neufeld's UART interface module 174 and modem performs the identical function of connecting a remote user at remote management PC 5 with the remote server management controller 116 for the communication of management data. EX1005, ¶[0059], EX1046, ¶106.

As discussed in Section III.E.3, the district court's claim construction further requires that "the one or more networks use one or more of the following protocols: SNMP, TFTP, FTP, DNS, SysLog, Telnet, SSH, HTTP, HTTPs, point to point IP, and/or XML." It would have been obvious to a POSITA to use one of these protocols for the out-of-band connection on either the Management Network M accessed via the Ethernet interface 180 or the PSTN accessed via the UART and modem because, as admitted in the 140 patent, these protocols "are typically utilized for management of a device." EX1002, 12:23-29; *see also* 3:4-7 (admitting that Telnet is the protocol most frequently used for remote login to network elements). The well-known use of such protocols is further evidenced by e.g., Emerson, which discloses that a that a "remote console," which a POSITA would understand to correspond to the remote management PC 5, may initiate a telnet session with the managed server and exchange "standard telnet formatted commands." EX1010 at 16; EX1046, ¶107. Similarly, it would have been obvious

to a POSITA to employ SNMP (simple network management protocol) as described in RFC1157 over the Ethernet connection to management network M as the SNMP protocol was very well-known in the art for remotely managing devices. EX1018, 2; EX1046, ¶107.

4. [1.c]

Neufeld discloses or renders obvious this limitation. As discussed in section III.E.4, the function performed by the “virtual management interface connection means” portion of this limitation is “connecting said one or more network services or remote users with said secure management access controller,” and the structure disclosed in the ’140 patent is “a virtual private network (VPN).” EX1042, 3.

Neufeld discloses a VPN:

Further, the arrangements of servers and clients in a larger network environment could be connected in any of a large number of topologies that may include local area networks (“LANs”), wide area networks (“WANs”), and municipal area networks (“MANs”). Clients may also have the ability to access these networks via a virtual private network (“VPN”) or via the Internet.

EX1005, ¶[0009]; EX1046, ¶109. Neufeld further discloses that in order for a network administrator to access the server from a remote terminal located outside of work, the administrator must typically use a VPN. EX1005, ¶[0022]; *see also id.*, ¶[0088, Table 4, User Id 7]; EX1046, ¶110. A POSITA would have understood

such access involves communications with Neufeld's remote server management controller 116 given that it is a network administrator that is accessing the server. EX1046, ¶110.

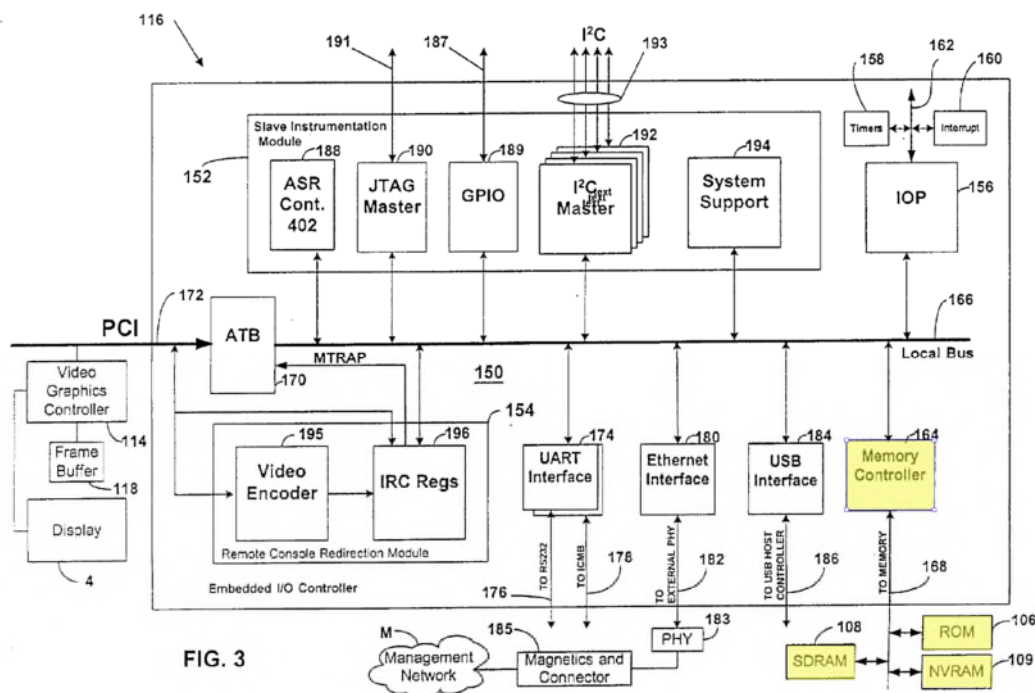
A POSITA would also have found obvious the requirement in limitation [1.c] for providing logical separation of management data from user data because a POSITA would have found it obvious to utilize a point-to-point VPN with tunneling functionality on Neufeld's managed server 2 via the in-band connection used for non-management user traffic (i.e., the NIC 110 and network N) in order to provide for a dedicated VPN for communications of management data with the remote management PC 5. A POSITA would have had knowledge of point-to-point VPNs using tunneling at the time of invention, would have understood that tunneling employs encryption to secure the VPN communications, and would have found it obvious to configure Neufeld's managed server to employ a point-to-point VPN with tunneling for communication of management data because VPN tunneling was a well-known, and indeed was the most common method, for implementing a point-to-point VPN. EX1046, ¶111 (discussing the use of L2TP/IPsec to create a secure L2TP tunnel protected by IPsec). Such VPN technology is the same as, or is at least equivalent, to the corresponding VPN structure for this limitation disclosed by the 140 patent. EX1046, ¶112.

A point-to-point VPN with tunneling used for the communication of management data between the remote server management controller 116 and the remote management PC 5 via the network N also performs the claimed function performed by the VPN technology of the 140 patent, namely providing logical separation of user data and management data. EX1046, ¶113. The use of a dedicated point-to-point VPN using tunneling technology provides for logical separation because the VPN tunneling necessarily differentiates traffic for the dedicated VPN from other user traffic. EX1046, ¶114. The VPN tunneling functionality dedicated to communications of management data from remote management PC 5 also performs the function of connecting a remote user on remote management PC 5 with Neufeld's remote server management controller 116 for communication of management data using the same user interface (Neufeld's NIC 110 connected to network N) over which non-management user data is communicated to the managed server 2. EX1046, ¶115.

B. Claim 2

Neufeld renders obvious claim 2. Neufeld discloses that the remote server management controller 116 includes a memory controller 164 that is coupled to dedicated memory via a memory interface 168. EX1005, ¶[0055]. Neufeld discloses that this dedicated memory may include "battery-backed SRAM, SDRAM, ROM, NVRAM or any other appropriate type of memory." In the

embodiment of Figure 3 show below, the memory interface 168 is coupled to SDRAM 108, ROM 106, and NVRAM 109. EX1005 ¶[0055], Fig. 3; EX1046, ¶116.



SDRAM is a form of random access memory. Fig. 3; EX1046, ¶117.

NVRAM and ROM are both types of non-volatile random access memory. *Id.*

Neufeld discloses NVRAM but does not specify any limitation on the type of NVRAM that may be used. In view of Neufeld’s disclosure of that “any other appropriate type of memory” could be used, a POSITA would have found it obvious to include a flash memory chip, either as a part of Neufeld’s NVRAM or in place of Neufeld’s ROM for, e.g., storing firmware to allow for updates to the firmware. The use of flash chips for non-volatile memory was well-known at the

time of the 140 patent, and flash chips were known to be a reliable and cost-effective mechanism for implementing non-volatile random access storage. A flash EEPROM (an electrically erasable programmable read only memory) device is a non-volatile memory commonly used for storing firmware and permits its entire memory to be erased in a single step. EX1025, 2:4-14, 10:60-11:1. Neufeld therefore renders obvious the use of the use a flash chip, non-volatile random access memory and random access memory as dedicated memory connected to the memory interface 168 which is coupled to the memory controller 164 in Neufeld's remote server management controller 116. EX1046, ¶118.

To the extent that claim 2 requires the flash chip, non-volatile random access memory and random access memory to be physically part of Neufeld's remote server management controller 116, it would have been obvious for a POSITA include those memory devices in the remote server management controller 116 as this a design choice and involves nothing more than choosing from a finite number of known alternatives (internal vs. external memory) and requires no more than ordinary skill in the art. EX1046, ¶119. *See also* the following discussion of claim 3.

C. Claim 3

Neufeld discloses this limitation to render obvious claim 3. Neufeld discloses that the "remote server management controller 116 is implemented using

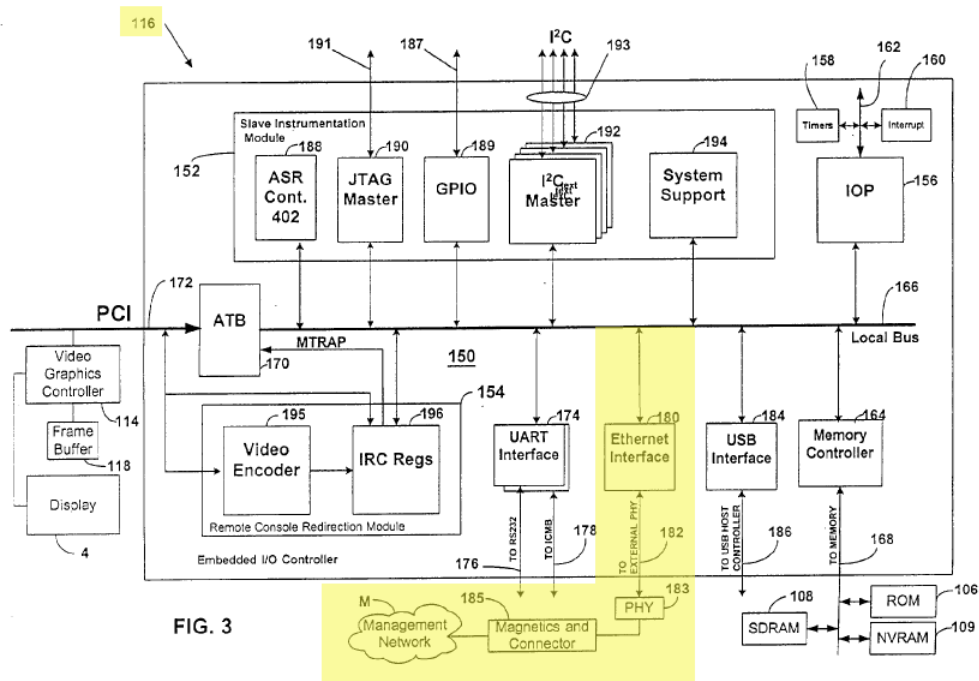
a single ASIC for the embedded I/O controller 150, which may be incorporated into the motherboard of the managed server 2.” EX1005 ¶[0051]; EX1046, 120. It would have been obvious to a POSITA to include the memories recited in claim 2 in this implementation. EX1046, 120.

D. Claim 4

Neufeld would have rendered the limitations of claim 4 obvious to a POSITA. A POSITA would have been familiar with SOC (system-on-chip) and ASIC (application-specific integrated circuit) technology at the time of the 140 patent and would have found it obvious to implement Neufeld’s processors 10 and its remote server management controller 116 including associated RAM, non-volatile RAM and flash memories as discussed above in Ground 2 in a single integrated circuit using such technology. EX1005, ¶[0044]; EX1046, ¶121. When these components are implemented on a single chip, the memories are embedded in a main processor on the managed server 2 as required by this claim. EX1046, ¶122. A POSITA would have been motivated to do so in order to reduce chip count and associated manufacturing costs. EX1046, ¶123. A POSITA would have had a reasonable expectation of success in doing so because ASIC and SOC technologies were known and commercially available at the time of the 140 patent and involved no more than the exercise of routine skill. EX1005, ¶[0050]; EX1046, ¶124.

E. Claim 6

Neufeld discloses the limitations of this claim to render obvious claim 6. Neufeld's management network M constitutes the claimed "communication system," and Neufeld's Ethernet Interface 180 and/or PHY 183 is a claimed "secure management access controller interface device." *See* limitation [1.b] in this Ground 1 above; *see also* EX1005, ¶¶[0061]-[0062] (discussing receipt of out-of-band management information at remote server management controller 116 via network M and Ethernet interface 180), Fig. 3 below, EX1046, ¶¶125-126. *See also* limitation [1.b] in this Ground 1 above, discussing out-of-band communications between Neufeld's remote server management controller 116 and remote management PC 5 via a UART 174 connected to an industry standard modem (a claimed "secure management access controller interface device"). EX1046, ¶127.



F. Claim 7

Neufeld discloses and/or renders obvious the limitations of claim 7. See limitation [1.b] and claim 6 in this Ground 1 above, discussing out-of-band communications between Neufeld's remote server management controller 116 and remote management PC 5 via a UART 174 connected to an industry standard modem (a claimed "interface device"). A POSITA would have understood or at least found it obvious, that the industry standard modem could be a modem configured for use on the public switched telephone network (PSTN) to connect to a corresponding modem in the remote management PC 5 (the claimed "communication system"). EX1046, ¶128. See also discussion of out-of-band communications between Neufeld's remote server management controller 116 and

remote management PC 5 via Ethernet interface 180 (a claimed “interface device”). A POSITA would have understood or at least found it obvious, to implement the management network M as a broadband network and that the Ethernet interface 180 would provide a broadband connection to the management network M (together with the devices in network M, a claimed “communication system”). EX1046, ¶129.

G. Claim 10

Neufeld discloses and/or renders obvious the limitations of claim 10. See discussion of VPN tunneling to provide logical separation of user data and management data and the forwarding of the management communications to Neufeld’s remote server management controller 116 in limitation [1.c] in this Ground 1 above. EX1046, ¶130.

H. Claim 11

Neufeld discloses and/or renders obvious the limitations of claim 11. As discussed in limitation [1.c] above, Neufeld discloses a VPN which is the claimed “virtual management interface connection means.” Under the district court’s construction, a VPN is also corresponding structure for the “protection means.” See Section III.E.5. Neufeld’s VPN performs the claimed function performed by the “protection means,” i.e., protecting management data due to its use of encryption, and has identical or at least equivalent structure to the 140 patent’s VPN. EX1046,

¶131. With respect to other corresponding structures for this limitation, see Ground 2 below. *Id.*

I. Claim 13

Neufeld discloses this limitation to render obvious claim 13. As discussed in Section III.E.6, the function performed by the “monitoring means” is “monitoring the status of at least one computer network component,” and the first corresponding structure for performing that function is “a processor performing an algorithm to monitor network components for loss of connectivity by testing the network connection.” EX1042, 5; EX1046, ¶132.

Neufeld discloses that the remote server management controller 116 “may be adapted to snoop video traffic via PCI bus 172, which is merely an extension of the PCI bus 16.” EX1005, ¶[0058]. Such snooping constitutes testing of the bus connection for the video graphics controller and display. EX1046, ¶133. Neufeld further discloses that the IOP 156 of the remote management controller 116 controls IRC registers 154 to function as a virtual communication device that may be used to intercept UART communications or communications through other sources. EX1005, ¶[0072]. Such interception constitutes testing of a connection to the UART. In both cases, the function is the same, monitoring the status of at least one component of the managed server (the bus 172 or the UART), which is also a network component. EX1046, ¶134. And the structure is equivalent, because it

includes performing an algorithm for testing a communication connection (i.e., on the PCI bus 172 or via the UART). EX1046, ¶134.

Neufeld also discloses that data intercepted in this manner may be redirected to other outputs of the remote server management controller 116 such as to a remote user via the Ethernet interface 180. EX1005, ¶[0072]. This redirected data is indicative of the status of the bus 172 or the UART. The Ethernet interface 180 is therefore a network interface that is used for reporting the status of the video graphics controller, display and UART to a network management station, *i.e.*, the remote management PC 5 used by the user. EX1046, ¶135.

J. Claim 16

Neufeld discloses this limitation to render claim 16 obvious. As discussed in Section III.E.9, the function performed by the claimed “means for monitoring” is “monitoring connection attempts made through the management access controller” and the corresponding structure for performing the above-stated function is (i) an Access Control Server (ACS) using protocols to authenticate and authorize access (19:44-64), or (ii) a processor running one or more of RADIUS, TACACS+ and/or LDAP. EX1046, ¶138.

Neufeld discloses structure (i) above. Specifically, Neufeld’s managed server 2 includes a “security manager that includes a security sign-on system that may be stored and operated on the remote server management controller 116 to

provide for ‘lights out’ management.” EX1005, ¶[0076]. Neufeld further discloses that “the security sign-on system includes authentication of services to prove the identity of each user, a directory service to provide each user with entry into each appropriate function or resource, and a service, that may include an encryption and certification component, which verifies the user to the directory service.” *Id.* Each time an operation is attempted, the system’s firmware may place a call to the security manager to determine whether the user has sufficient privilege to perform an operation. EX1005, ¶[0091]; EX1046, ¶137.

The security manager disclosed by Neufeld performs the identical function and is the same as, or is at least equivalent to, the corresponding structure (i) for this limitation discussed above. EX1046, ¶138. Neufeld’s security manager is an access control server that uses the PKI protocol or other protocols including ID/password pairs, challenge/response tokens, biometrics, or other methods of ensuring a positive identification as discussed in EX1005, ¶[0076] to authenticate users. Neufeld’s security manager also provides authorization based on a user profile protocol as discussed at EX1005, ¶¶[0077]-[0087], Tables 1-4. EX1046, ¶138.

VI. GROUND 2: NEUFELD IN VIEW OF SYVANNE RENDERS OBVIOUS CLAIMS 11 AND 12

Claim 1 (from which claims 11 and 12 depend) is obvious in view of Neufeld for the reasons discussed above in Ground 1. Claim 11 recites the “system

of claim 10 wherein the virtual management interface includes a protection means for protecting the management data,” and one of the corresponding structures for the “protection means” is a firewall as discussed in Section III.E.5 above. Neufeld in combination with Syvanne renders obvious the limitations of claim 11. As discussed in further detail below in connection with claim 12 in this Ground 2, a POSITA would have found it obvious to improve the security of Neufeld’s remote management controller 116 by implementing “a firewall to protect the at least one computer management access controller from unauthorized access” as claimed on the IOP 156 of Neufeld’s remote management controller 116 in view of Syvanne. EX1046, ¶139. Such a firewall performs the identical function of the protection means (i.e., “protecting the management data”), and is the identical or at least equivalent structure. EX1046, ¶139.

Claim 12 recites “The system of claim 10 wherein the virtual management interface includes a secure transmission tunnel to protect management communications and a firewall to protect the at least one computer management access controller from unauthorized access.” With respect to the secure transmission tunnel limitation, see discussion of the virtual management interface and VPN tunneling to provide logical separation of user data and management data in limitation [1.c] in Ground 1 above. EX1046, ¶140.

A POSITA would have found it obvious to implement “a firewall to protect the at least one computer management access controller from unauthorized access” on the IOP 156 of Neufeld’s remote management controller 116 in view of Syvanne. EX1046, ¶141.

Syvanne discloses protecting a computing device by installing a “personal firewall,” which is a firewall implemented in software that executes locally on the device, *in addition to* or instead of a firewall on an internal network. EX1016, 1:35-50, 5:35-44. Such locally executing software firewalls were well-known to a POSITA. An example of such a firewall is the free firewall named IP Filter, but other locally executing software firewalls such as ipfw and ipchains were also well-known in the art. EX1022 at 1; EX1046, ¶141. Syvanne discloses the use of a personal firewall on a laptop that will be exposed to a foreign network such as the Internet. EX1016, 1:35-50. A POSITA would have understood that, with respect to Neufeld’s remote management controller 116, the managed server 2 including the NIC 110 and bus 172 (via which in-band management messages from the Network N are received) would constitute a foreign network. EX1046, ¶142. In view of Syvanne’s teaching of adding an additional locally-executing firewall to a device exposed to a foreign network, a POSITA would have been motivated to implement such a firewall on the IOP 156 of Neufeld’s remote management controller 116 (in addition to any firewall that may be implemented in the managed server 2) to

further protect the remote management controller from exposure to such a foreign network. EX1046, ¶143. A POSITA would have had a reasonable expectation of success as doing so would have involved only routine skill and such firewalls were well-known in the art. EX1046, ¶143.

VII. GROUND 3: NEUFELD IN VIEW OF FOWLER RENDERS OBVIOUS CLAIM 14

Claim 1 (from which claim 14 depends) is obvious in view of Neufeld for the reasons discussed above in Ground 1. Fowler discloses a “Method and System for Monitoring Computer Networks and Equipment.” EX1040, Title. Fowler’s system includes a device that is powered by a regulated 5-volt power supply that receives 120-volt power from a typical wall outlet, and that is also connected to a combined power fail detector and uninterruptable power supply (UPS). Fowler’s power fail detector detects the failure of the power supply from the wall outlet switches the device to receive power from the UPS, and notifies the device’s CPU of the power failure. EX1040, 12:14-18; EX1046, ¶144. A POSITA would have found it obvious to include Fowler’s UPS with power fail detector in Neufeld’s managed server 2 and configure it to detect a loss of power to the managed server 2 and supply power to the remote management controller 116 when power to the managed server 2 is lost as discussed in Neufeld. EX1005, ¶[0052]; EX1046, ¶145. The combination of Neufeld and Fowler (EX1040) renders obvious the limitations of claim 14 for the reasons discussed in further detail below. EX1046, ¶145.

A. Limitation [14.a]

Neufeld discloses that the “remote management controller 116 may be implemented so that it is powered up and capable of operation whether or not the managed server 2 is powered up (turned on) or online.” EX1005, ¶[0052]. In light of this disclosure, a POSITA would have understood or at least would have found obvious that Neufeld’s system includes a network power supply (a power supply that provides power to a network component such as the managed server 2) in addition to an additional power supply for the remote management controller 116. EX1046, ¶146. Thus, Neufeld discloses and renders obvious this limitation.

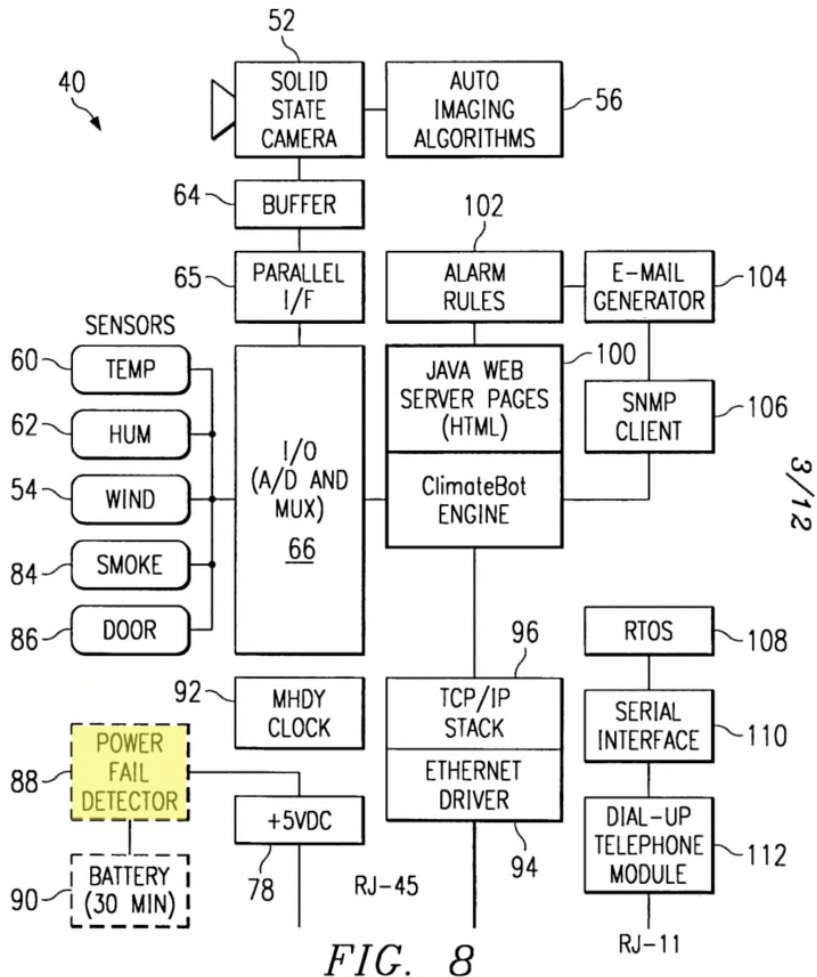
To the extent the foregoing discussion in Neufeld is found to be insufficient to disclose a network power supply, Fowler discloses a “[f]ive volt power supply 78 [that] can receive and transform electrical power from a wall-mounted receptacle to power circuit 50.” EX1040, 12:1-2 and Figs. 7-8; EX1046, ¶147. The power supply 78 constitutes a network power supply as required by limitation [14.a]. It would have been obvious to combine Neufeld with Fowler by including Fowler’s five-volt regulated power supply 78 (or a power supply with whatever voltage is required) in Neufeld’s managed server 2 to provide power to that device. EX1046, ¶147. Further, in order to ensure that Neufeld’s remote management controller 116 was available even when power to the managed server 2 was not available, a POSITA would have found it obvious to include Fowler’s UPS with

the power fail detector 88 into Neufeld's managed server 2 and to configure the power fail detector 88 to detect a loss of utility company power to power supply 78 in the managed server 2 and switch the UPS to supply power to the remote management controller 116 as discussed in Neufeld. EX1005, ¶[0052]; EX1046, ¶147. Motivation for this modification comes from the disclosure in Neufeld in EX1005, ¶[0052]. EX1046, ¶148. A POSITA would further have been motivated to make this combination to prevent Neufeld's managed server 2 and remote management controller 116 from shutting down and denying management services to remote administrators. A POSITA would have had a reasonable expectation of success in so doing because power fail detectors and UPSs were well-known in the art and implementing a UPS in this fashion would have involved no more than ordinary skill. EX1046, ¶148.

B. Limitation [14.b]

The combination of Neufeld and Fowler renders obvious this limitation. As discussed in Section III.E.7, the function performed by this limitation is “monitoring the status of the network power supply” and the corresponding structure is a UPS that monitors network components for loss of power. Fowler's uninterruptable power supply including the power fail detector 88 highlighted in yellow in Figure 8 below performs the identical function (monitoring the status of the power provided by the utility company through the wall mounted receptacle to

the power supply 78 supplying power to Neufeld’s managed server) and includes identical or at least equivalent structure (a UPS that monitors network components, i.e., the managed server, for the loss of power). EX1046, ¶149.



C. Limitation [14.c]

Neufeld and Fowler render obvious this limitation. As discussed in Section III.E.8, the function performed by this limitation is “reporting the status of the network power supply” and the corresponding structure for performing the above-stated function is a processor performing the algorithm disclosed at 20:24-29 or the

algorithm disclosed at 21:3-12 of the 140 patent. Fowler discloses that power fail detector 88 in the UPS “provides a means of . . . notifying the CPU of the power failure.” EX1040, 12:16-18; EX1046, ¶50. In the combined Neufeld-Fowler system, it would have been obvious to a POSITA to configure Fowler’s power fail detector 88 to notify Neufeld’s remote management controller 116 of the power failure to the managed server 2 because only the remote management controller 116 in the managed server would have power if the five-volt regulated power supply 78 loses utility company power. EX1046, ¶150.

It would further have been obvious to a POSITA to configure Neufeld’s remote management controller 116 to report the power failure for the managed server 2 to Neufeld’s remote console 5 via the out-of-band connection on the management network M in light of (a) Neufeld’s disclosure that the remote management controller 116 functions to allow monitoring of “a wide range of system problems” on the managed server 2 from the remote console 5, and (b) Fowler’s disclosure of a net bot” that has the ability to detect a power failure and provide a dial-up telephone notification of the power. EX1005, ¶¶[0043], [0052]; EX1040, 9:26-10:2. A POSITA would have understood that a power failure at the managed server 2 would be a significant event for which a remote administrator would want to be informed. EX1046, ¶151. Reporting the power failure by the remote management controller 116 using the out-of-band channel on management

network M is the identical function for the claimed reporting means, and is at least equivalent structure to the algorithm disclosed in the 140 patent at 20:24-29, which discloses reporting a loss of main external power to a power supply via a “secondary network resistant to the affects of a power failure.” EX1046, ¶152.

VIII. GROUND 4: NEUFELD IN VIEW OF FOWLER RENDER OBVIOUS CLAIM 13

Neufeld in view of Fowler renders obvious the “wherein the at least one the [sic] management access controller includes a monitoring means for monitoring the status of at least one computer network component” limitations of claim 13 under the second disclosed structure for the “monitoring means” (the uninterruptable power supply that monitors network components for loss of external power) for the reasons discussed below for limitation [14.b] in Ground 3 above. EX1046, ¶153 (noting that monitoring the power supply for the remote management controller 116 constitutes monitoring the status of at least one computer network component).

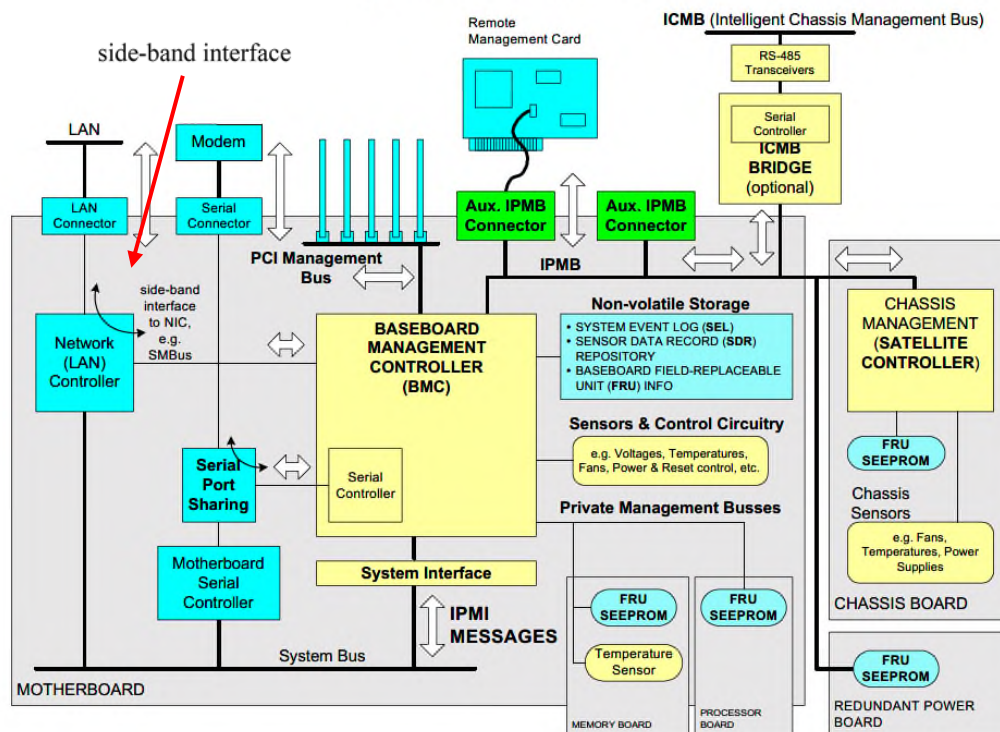
With respect to the “a network interface for reporting a status of the at least one computer network component to a network management system” limitation of claim 13, *see* limitation [14.c] in Ground 3. EX1046, ¶154.

IX. GROUND 5: IPMI IN COMBINATION WITH LAWRENCE RENDERS OBVIOUS CLAIMS 1-3, 6, 7, 10 AND 11

A. Introduction

As discussed above and shown in annotated Figure 1-2 below, IPMI discloses a management processor referred to as the BMC and further discloses a Network (LAN) controller with a side-band interface through which in-band management data is exchanged between a user at remote management system on a LAN and the BMC. EX1046, ¶155. IPMI does not detail or limit how to implement the side-band interface for this in-band communication, and therefore a POSITA would have looked to other sources for information as to how to implement IPMI's side-band interface. EX1046, ¶156.

Figure 1-2, IPMI Block Diagram



Lawrence discloses a method and system for providing in-band management. EX1043, 1:1-3. Lawrence specifically discusses in-band management for a router but is not limited to routers and expressly states that the techniques disclosed therein may be used with other types of network devices. EX1043, 3:54-64; EX1046, ¶157. Lawrence discusses the advantages of in-band communication of management data but explains that prior art in-band systems were carried on non-secure data links and were therefore “susceptible to unauthorized management entry or interception of management commands.” EX1043, 2:20-58. Lawrence discloses embodiments for secure in-band communication of management information, including the embodiment shown in Figure 7 below in which management data is communicated to a router configuration management module 610 via a dedicated management VPN module 655 and an internal management VPN link 711 (with highlighting).

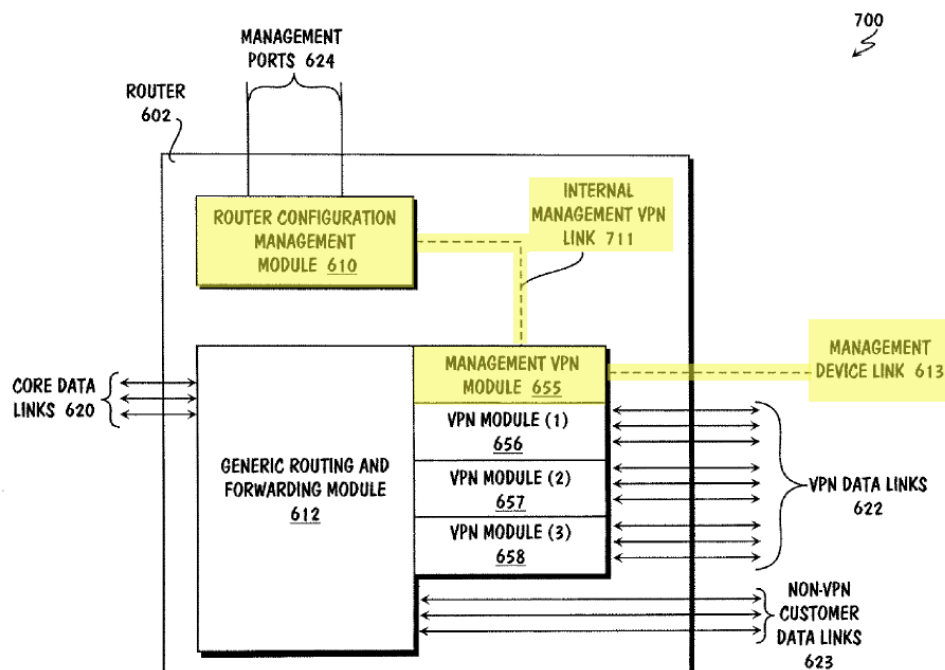


FIG. 7

EX1043, 5:37-47; EX1046, ¶158. Lawrence further discloses that the dedicated management VPN module 655 performs VPN encapsulation, routing and forwarding functions and may include encryption using an IPsec or other process. EX1043, 5:15-30. The disclosure of encapsulation indicates VPN tunneling. EX1046, ¶159.

A POSITA would have recognized Lawrence's Internal Management VPN Link 711 in Figure 7 as a desirable and convenient way in which to implement IPMI's side-band interface, and thus would have found it obvious to include Lawrence's VPN tunneling technology in IPMI's Network (LAN) controller in order to implement IPMI's side-band interface (corresponding to Lawrence's Internal Management VPN link 711). EX1046, ¶160.

A POSITA would have been motivated to do so as IPMI does not detail how to implement the side-band interface for in-band communications, and so would have looked to references like Lawrence to prevent the security problems associated with communication of in-band information over non-secure links as discussed above, including unauthorized management command entry and/or interception of management commands. EX1046, ¶161. A POSITA would have had a reasonable expectation of success in doing so, as this would have involved the exercise of no more than ordinary skill. For example, such VPN technology was well-known, and software implementations of such VPN technology were available at the time of the 140 patent. EX1046, ¶161.

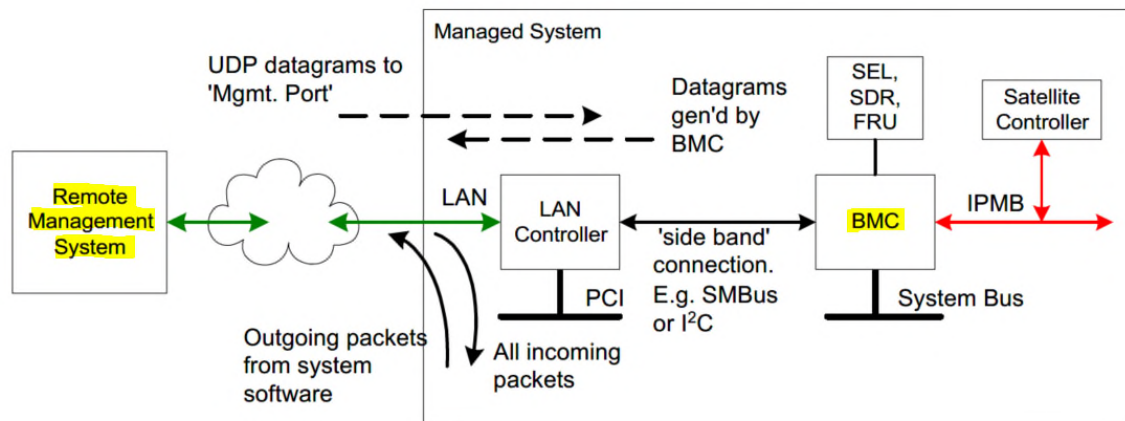
B. Claim 1

1. Limitation [1.pre]

To the extent the preamble is limiting, IPMI discloses it. The claimed “remote device management communication system” is (i) IPMI’s “managed system” in which the Baseboard Management Controller (BMC) resides and (ii) IPMI’s “remote management system” that executes software referred to as a “remote console,” together with the network that connects these two devices. EX1020, 40; EX1046, 182. The BMC manages the interface between system management software that performs the claimed “management applications” and

platform management hardware. EX1020, 8. *See also* Figure 12-1 below (with highlighting). EX1046, ¶162.

Figure 12-1, Embedded LAN Controller Implementation



IPMI’s Intelligent Platform Management includes monitoring, event logging, and recovery control functions, which are the claimed “management applications.” EX1020, 8. IPMI’s monitoring and logging functions include monitoring and logging of critical events and system events. EX1020, 161. Critical events are those that indicate “failure” conditions, such as out-of-range temperature and voltage events and hardware failures such as power supply or fan failures. EX1020, 161; EX1046, ¶163. IPMI discloses a System Event Log for logging such critical events, and also discloses sending alerts on the network, presenting local pop-up messages, and shutting down an application. EX1020, 19 and 161. IPMI further discloses a “Slot/Connector sensor for monitoring hot-plug slot status, and

ACPI System Power State sensor to support out-of-band monitoring of the system power state.” EX1020, 7; EX1046, ¶164.

The claimed “distributed computer network” is IPMI’s managed system and the remote management system as well as gateways, routers, and proxies in the network. EX1020, 9 and 118. IPMI further discloses a Dynamic Host Configuration Protocol (DHCP) Server on the network. EX1020, 118. DHCP is a TCP/IP protocol that enables a DHCP server on the network to assign a temporary IP address to a client (e.g., IPMI’s managed platform and the BMC) automatically when the client connects to the network. EX1046, ¶185. IPMI also discloses a LAN which inherently includes a collection of devices and commonly includes client computers such as PCs, printers, large hard disks, and other devices. EX1020, Figs. 1-2 and 12-1, EX1046, ¶165.

IPMI discloses “network services” including access functions. EX1020, 8; EX1046, 166. IPMI also discloses other “network services” such as DHCP services. EX1020, 118. These services are of the same type discussed in the 140 patent at 4:63-66 (e.g., access control server (ACS), Domain Name Service (DNS), and network time protocol (NTP)).

The claimed “managed network device” is IPMI’s managed system and the claimed “secure management access controller” is the BMC as shown in Figure 1-2 and Figure 12-1 below. The BMC provides the system interface to the platform

management subsystem, including message handling, control of a LAN interface for in-band management messages and control of a serial/modem interface that allows for out-of-band management messages. EX1020, 25-26; EX1046, ¶167.

Figure 1-2, IPMI Block Diagram

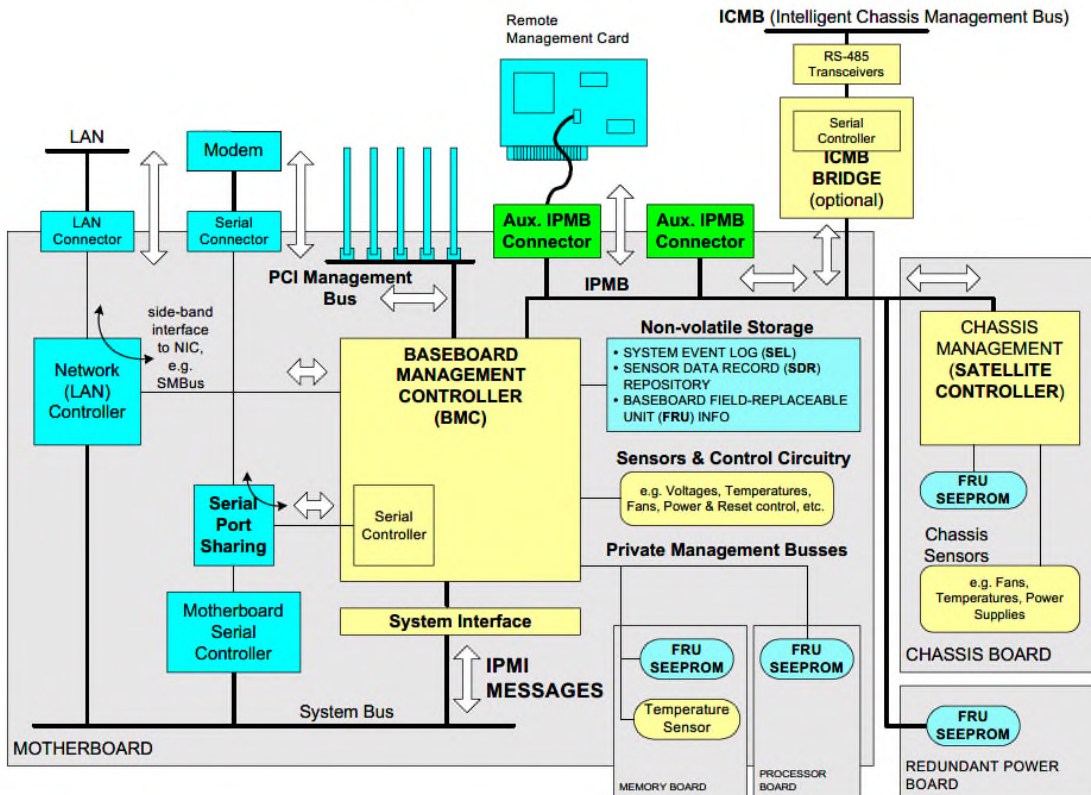
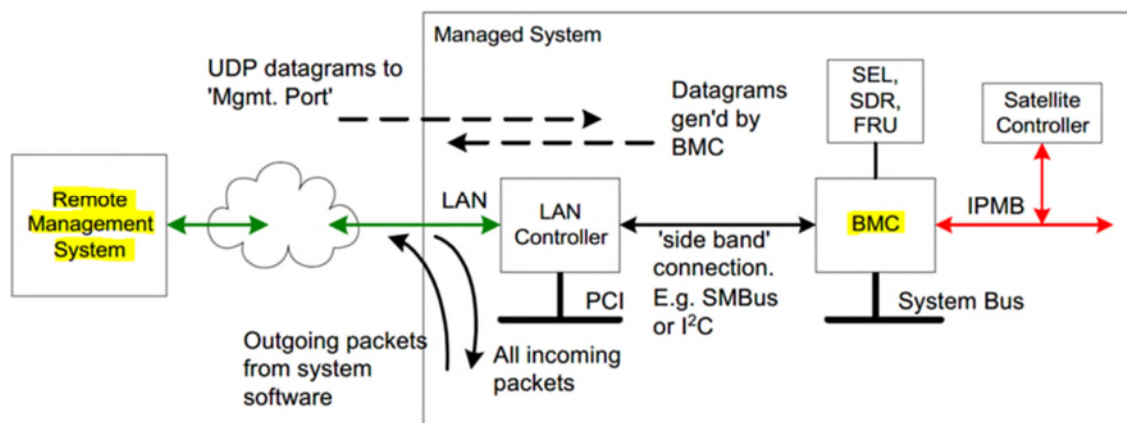


Figure 12-1, Embedded LAN Controller Implementation



2. Limitation [1.a]

As discussed above for limitation [1.pre], IPMI's BMC is the claimed "secure management access controller," and IPMI's managed system is the claimed "managed network device." IPMI discloses that the BMC is connected in one embodiment to an I²C bus or SMBus as shown in the embedded LAN controller implementation of Fig. 12-1, or to a PCI management bus as shown in the PCI management bus implementation of Fig. 12-2 below. In both embodiments, the BMC is also connected to the system bus. As shown in Fig. 12-2, the LAN Controller is implemented as a PCI add-in card connected to the BMC via a PCI Management Bus Connection. The PCI Management bus allows the BMC to send and receive IPMI messages. EX1020, 29. *See also*, EX1020, 16, Figs. 1-2, 12-1 and 12-2. Any of these busses are the claimed "one or more data bus of said managed network device" configured to send IPMI messages (the claimed "device management data"). EX1046, ¶168.

Figure 1-2, IPMI Block Diagram

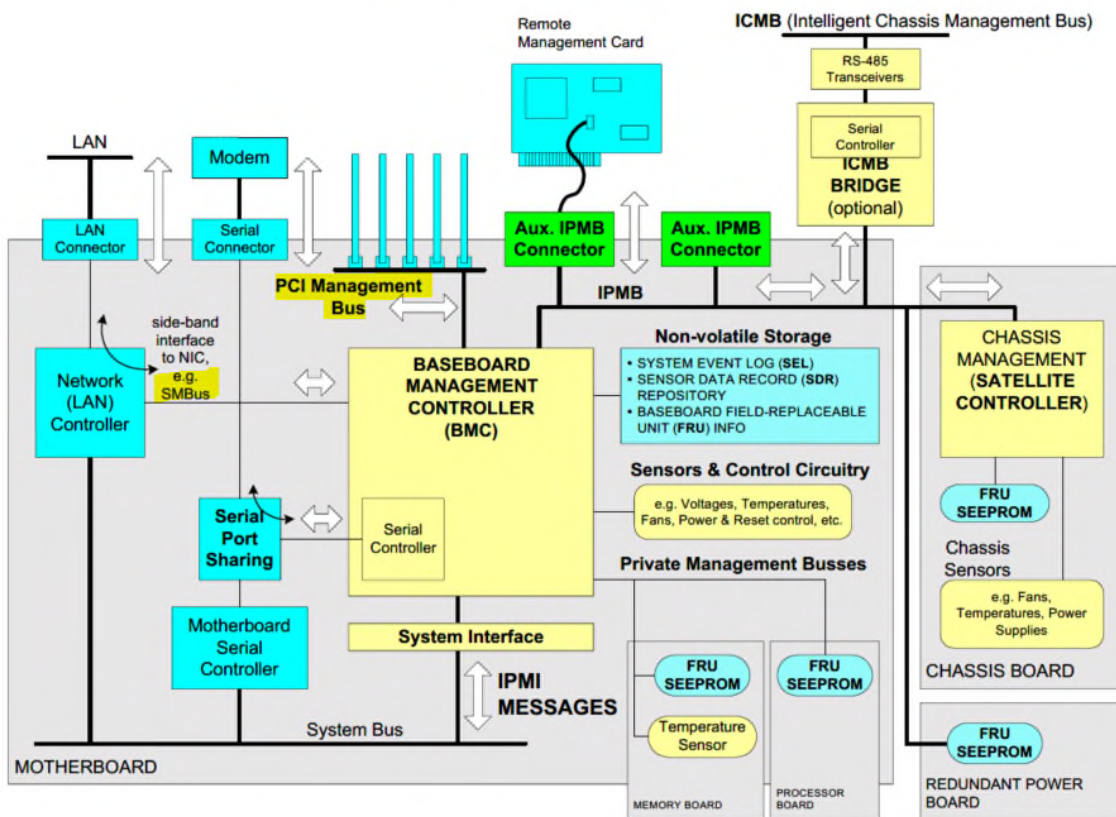


Figure 12-1, Embedded LAN Controller Implementation

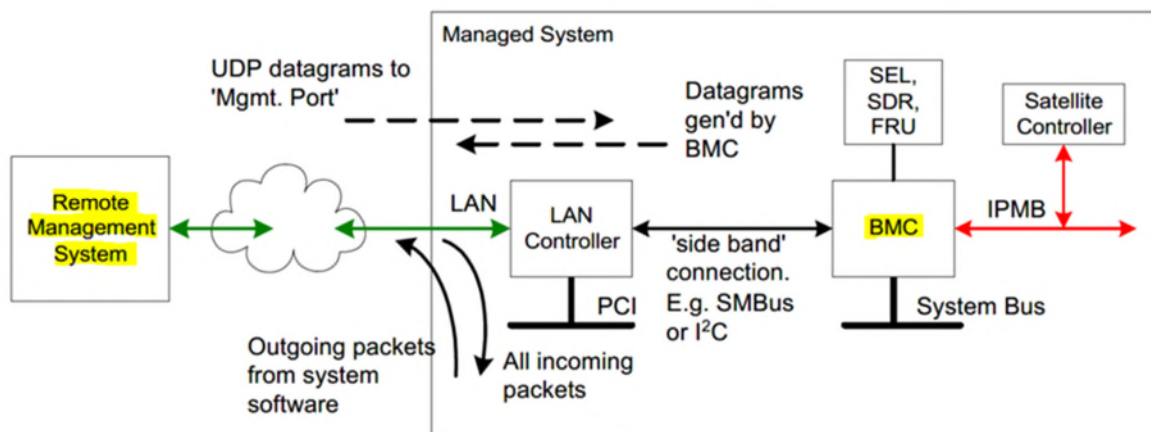
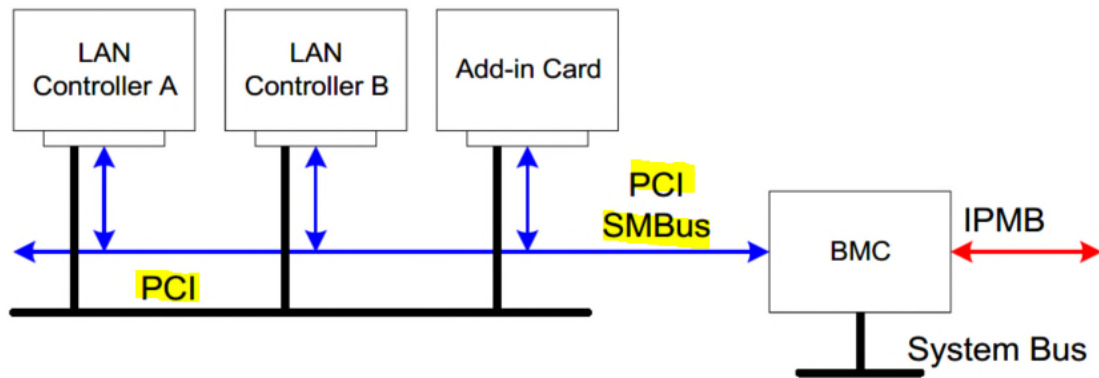


Figure 12-2, PCI Management Bus Implementation



3. Limitation [1.b]

The function performed by the claimed “out-of-band access connection means” and the corresponding structure for that function are discussed in Section III.E.3.

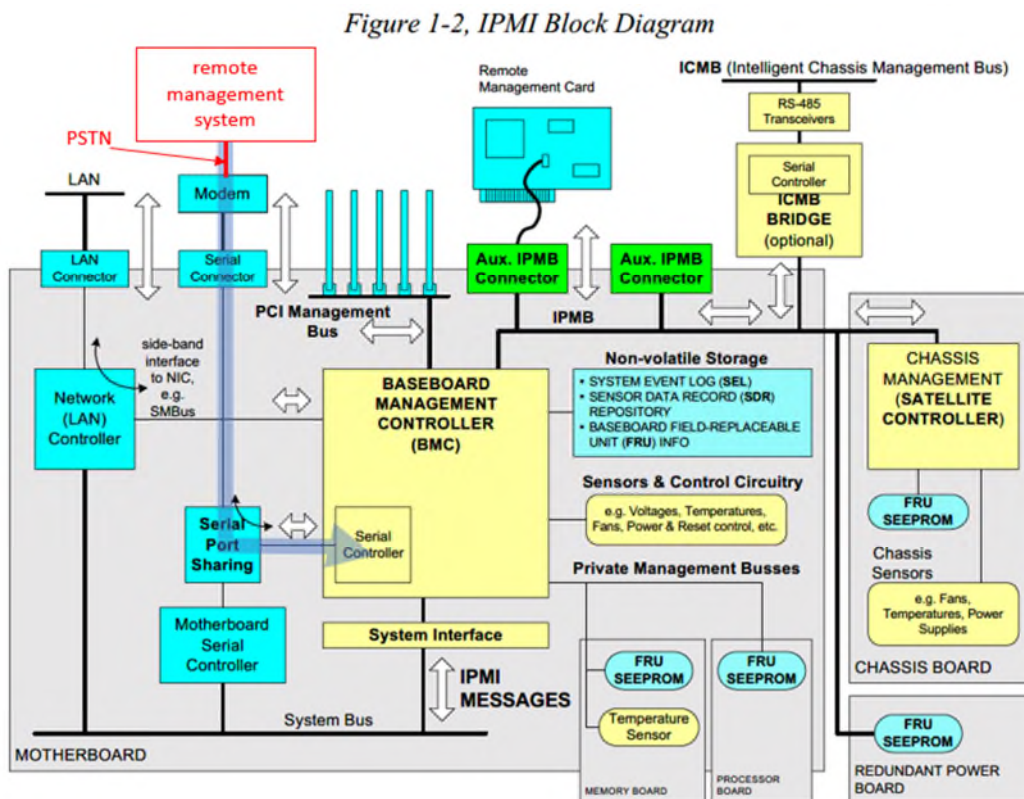
The corresponding structure includes the PSTN. EX1046, ¶169.

IPMI discloses that users may transfer IPMI management messages with the BMC through out-of-band communication interfaces via the serial port such as a modem.³ EX1020, 7 and 122. As disclosed by IPMI, BMC uses command

³ IPMI discloses an optional “serial port sharing” capability in which the serial port for the modem is used by both the BMC and the managed system. EX1020, 124.

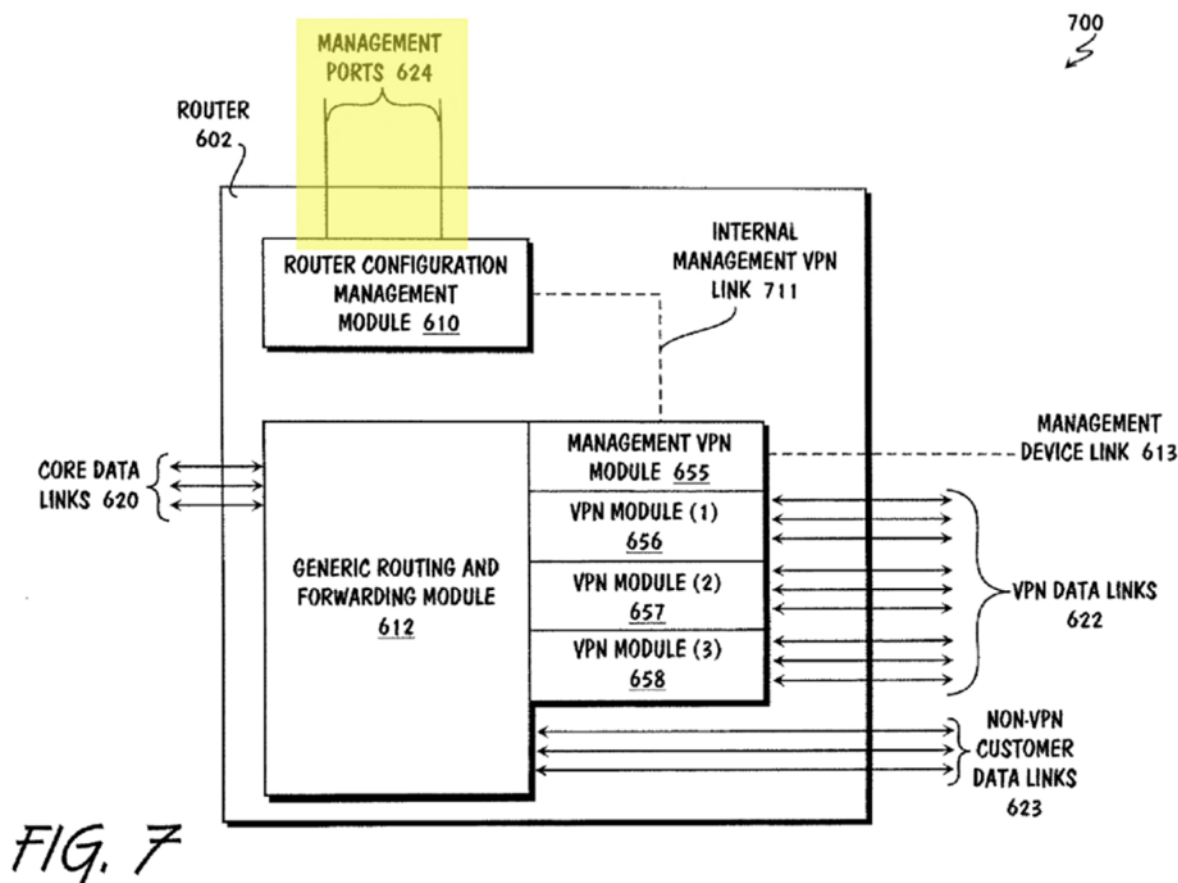
Because IPMI discloses that this feature is optional, a POSITA would understand that IPMI also discloses a dedicated serial port used only by the BMC. *Id.*; EX1046, ¶171. Petitioner relies on an IPMI embodiment without that feature.

“strings” to configure the modem for out-of-band access. EX1020, 133. Annotated Figure 1-2 below shows this out-of-band path between the remote management system and the BMC using a modem attached to a serial connector. EX1046, ¶170.



As discussed in further detail in connection with claims 6 and 7 below, IPMI discloses that the modem can be configured for communication over a telephone system/PSTN, which is one of the corresponding structures for this limitation. EX1020, 15, 122-123; *see also id.*, 131 (disclosing details on how to use the modem for out-of-band management), 133 n.1 (discussing variations in national phone systems), Table 15-4 at 174 (referring to destination phone numbers for use with serial/modem), EX1046, ¶172. Lawrence similarly discloses out-of-band

communication of management information via management ports 624 (shown in Figure 7 below) connected to a serial port in communication with a terminal for providing a command line interface, which a POSITA would have understood and found obvious to implement over a telephone line (PSTN). EX1043, 5:9-15; EX1046, ¶172.



This serial interface/modem/PSTN structure disclosed by IPMI performs the identical function of connecting a remote user at the remote management system with the BMC for out-of-band communication of management data, and is the

same structure or at least equivalent structure to one of the corresponding structures for this limitation disclosed by the 140 patent, the PSTN. EX1046, ¶173.

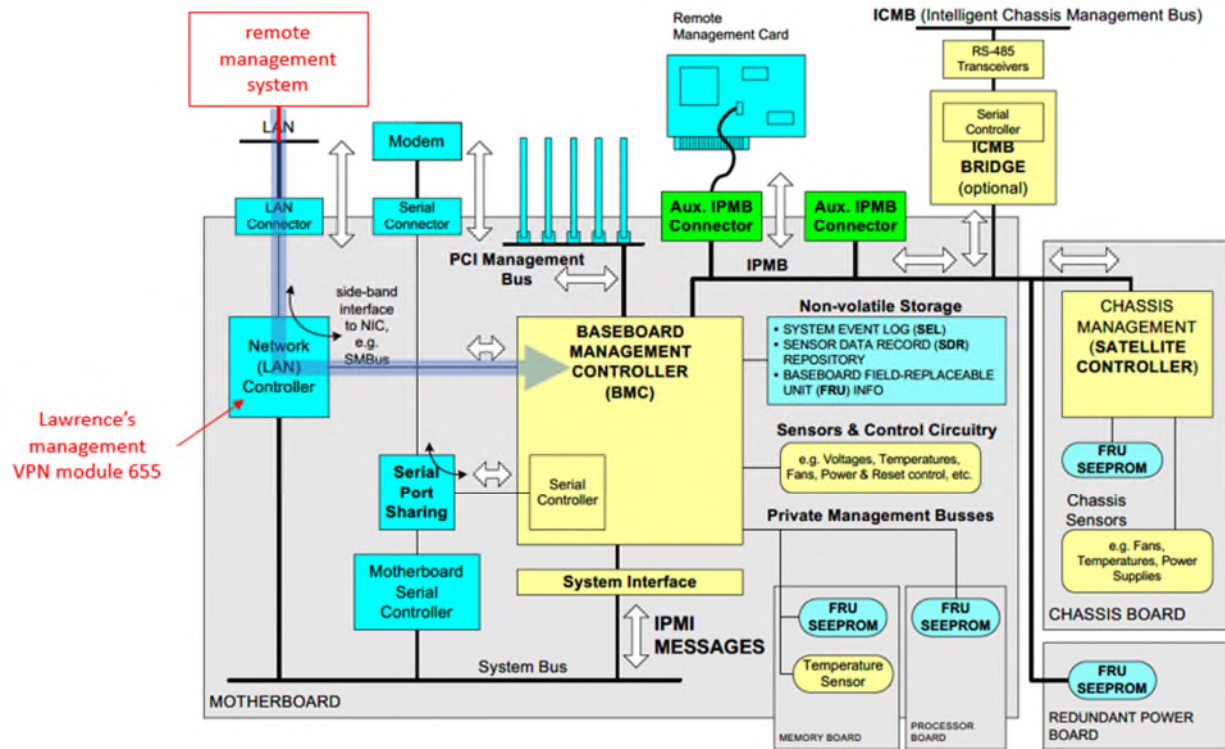
4. Limitation [1.c]

The functions performed by the claimed “virtual management interface connection means” and the corresponding structure for that function are discussed in Section III.E.4. As discussed there, that structure is a VPN. EX1046, ¶174.

In the combination of IPMI and Lawrence discussed in the Introduction above (Section IX.A), a POSITA would have found it obvious to include Lawrence’s VPN and tunneling technology in IPMI’s Network (LAN) controller in order to implement IPMI’s side-band interface (corresponding to Lawrence’s Internal Management VPN link 711). Since IPMI discloses in-band communication from the physical LAN connector to the LAN Controller, a POSITA would have found it obvious to incorporate Lawrence’s VPN module 655 into IPMI’s LAN Controller to separate the IPMI UDP datagrams from other user traffic and send the IPMI UDP datagrams over the side-band interface to the BMC. EX1020, 106; EX1046, ¶175. In the IPMI-Lawrence combination, those packets are processed by Lawrence’s dedicated management VPN module 655 (which employs tunneling technology as discussed in the Introduction to Ground 5 above) in the IPMI LAN Controller. The IPMI LAN Controller then directs those packets via Lawrence’s Internal Management VPN link 711 to IPMI’s BMC, which

corresponds to Lawrence's configuration management module 610, as indicated by the blue arrow shown in the annotated Figure 1-2 below. EX1046, ¶175.

Figure 1-2, IPMI Block Diagram

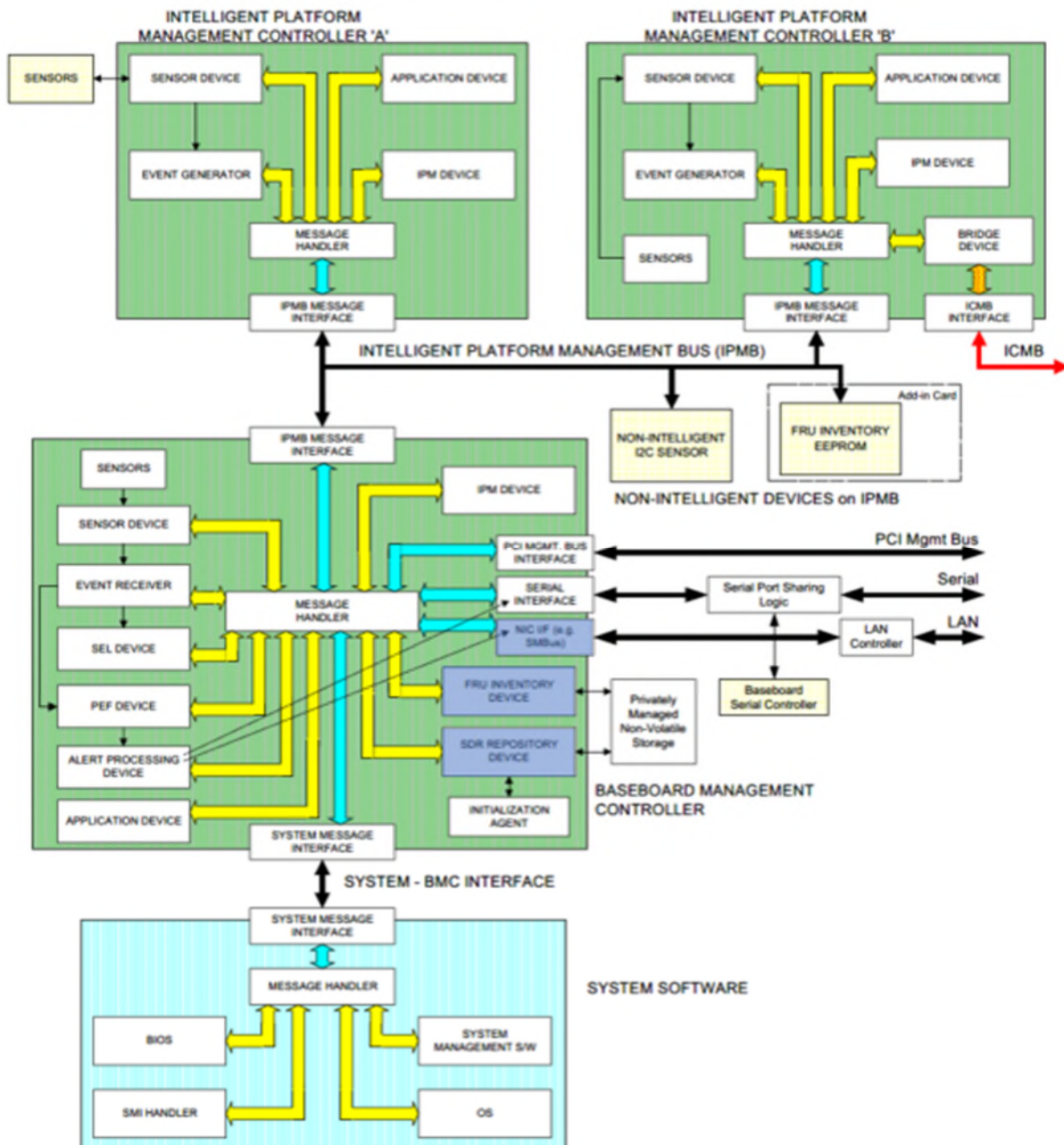


This implementation of IPMI's side-band interface using Lawrence's VPN technology is the identical structure for this limitation disclosed in the 140 patent, namely a VPN. Both structures perform the identical claimed functions – connecting remote users (e.g., on IPMI's remote management system) with the BMC and providing logical separation of IPMI management data from user data utilizing the same LAN interface of the managed system and the network connected thereto. EX1046, ¶176.

C. Claim 2

IPMI renders obvious the limitations of this claim. IPMI discloses on-chip RAM used to implement interface buffers as part of the “Host to BMC Interface,” which is part of the BMC (the claimed secure management access controller). EX1020, 100. The “Host to BMC Interface” is shown in Fig. 2-1 as the NIC interface that is connected to the LAN controller (purple highlighting to “NIC IF” added). Thus, IPMI discloses a secure management access controller that includes RAM. EX1046, ¶177.

Figure 2-1, Intelligent Platform Management Logical Devices



IPMI further discloses a Field Replaceable Unit (FRU) inventory device which includes information for each system board. EX1020, 12. As shown highlighted in purple in Figure 2-1 above, the BMC includes such an FRU inventory device. IPMI uses 24C02-compatible EEPROM (a serial electrically

erasable programmable ROM) for storing the FRU information. EX1020, 13. SEEPROM is a form of non-volatile random access memory. EX1046, ¶178. To the extent that non-volatile random access memory is construed in a manner that excludes SEEPROM, the use of non-volatile random access memory to store information in computer systems such as management devices would have been obvious to a POSITA. See, e.g., EX1005, ¶[0055], EX1046, ¶179. IPMI further discloses that the BMC must know the sensor and event type so it can place the information on the Event Message, and for this purpose BMC includes a sensor data record (SDR, also highlighted in purple above) which provides platform management sensor information (type, location...etc.). Ex 1020, 5 and 11. A modal SDR Repository may be stored in a flash device that also holds BMC code. EX1020, 311; EX1046, ¶180. Accordingly, it would have been obvious to a POSITA that the BMC includes all three types of memory required by claim 2. EX1046, ¶180.

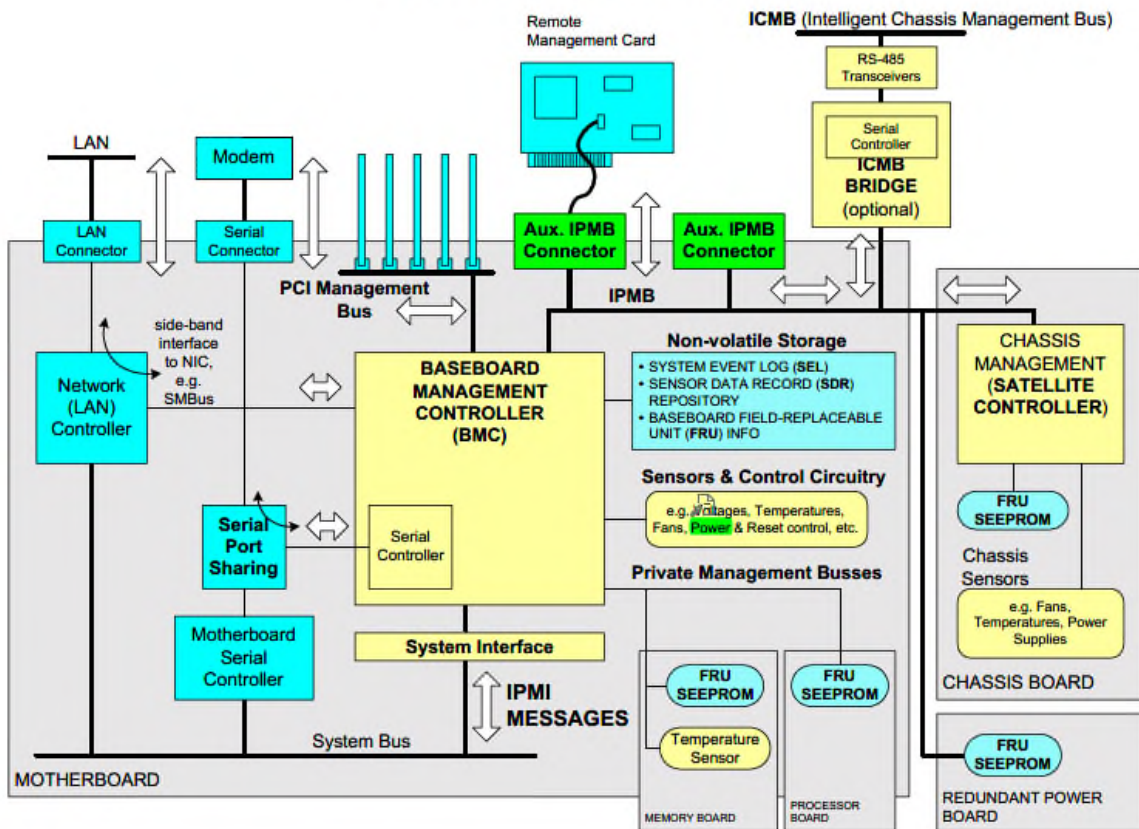
D. Claim 3

IPMI discloses the limitations of claim 3. IPMI discloses a BMC embedded in a motherboard. EX1020, Fig. 1-2. IPMI further discloses that “platform management” is used to refer to the monitoring and control functions that are built into the platform hardware and primarily used for the purpose of monitoring the health of the system hardware.” EX1020, 1. A POSITA would have understood

these disclosures as indicating that the BMC is embedded into the managed device.

EX1046, ¶181.

Figure 1-2, IPMI Block Diagram



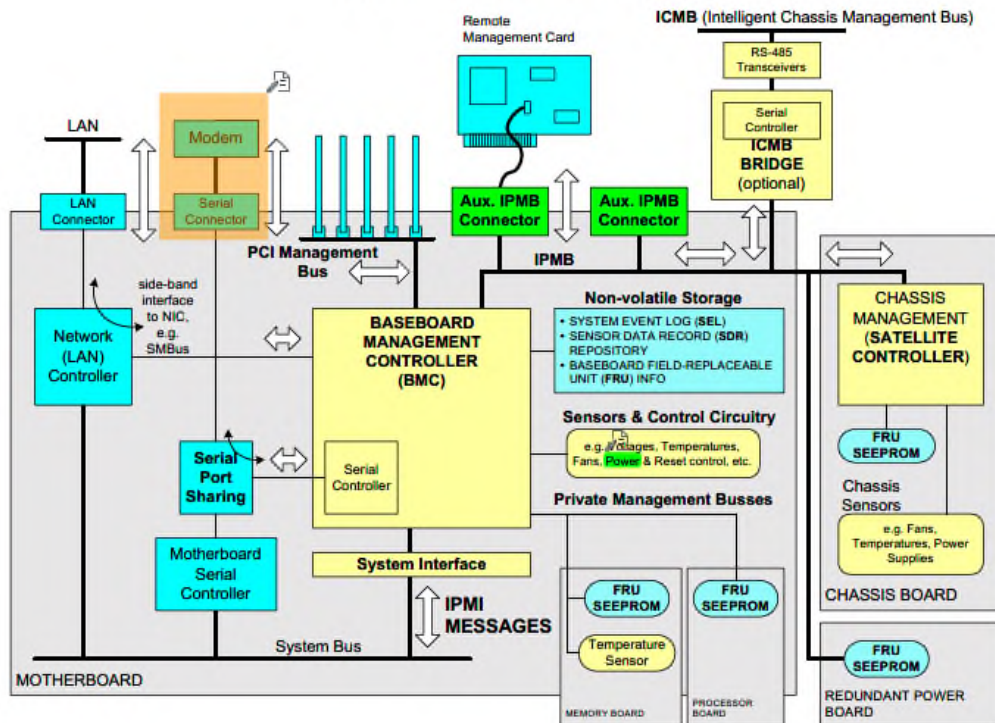
E. Claim 6

IPMI discloses the limitations of claim 6. The serial/modem interface in IPMI’s managed system in which the BMC resides, and which is configured for use on a telephone network, constitutes the claimed “secure management access controller interface device.” A telephone network that connects that serial/modem interface to devices such as IPMI’s “remote management system” that executes software referred to as a “remote console” constitutes the claimed “communication

system.” EX1020, 15, 122-123; *see also id.*, 131 (disclosing details on how to use the modem for out-of-band management), 133 n.1 (discussing variations in national phone systems), Table 15-4 at 174 (referring to destination phone numbers for use with serial/modem), EX1046, ¶182. The BMC manages the interface between system management software and platform management hardware. EX1020, 8. *See also id.*, Figure 1-2 (orange highlighting added, showing serial/model interface).⁴ EX1046, ¶183.

⁴ As discussed above, the serial port sharing feature illustrated in Figure 1-2 is optional and Petitioner relies on an embodiment of IPMI without that feature, in which case a POSITA would have understood and found obvious that the “Serial Connector” in Figure 1-2 would be connected directly to the BMC’s “Serial Controller.”

Figure 1-2, IPMI Block Diagram



F. Claim 7

IPMI discloses the limitations of this claim. See limitation [1.b] and claim 6 above in this Ground 5. EX1046, ¶184. A POSITA would have recognized the discussion of telephone calls and national telephone systems in IPMI to refer to the PSTN and IPMI's serial/modem to refer to an analog modem suitable for use on such networks. EX1046, ¶184.

G. Claim 10

IPMI in combination with Lawrence renders obvious the limitations of claim 10. See limitation [1.c] above in this Ground 5, including discussion of integrating Lawrence's VPN module 655 in IPMI's LAN controller for implementing a side-band interface, including separating remote management data from user data and

sending the remote management data to the BMC via the sideband interface as discussed in IPMI. EX1020, 106; EX1046, ¶185. It would have been obvious to a POSITA to modify IPMI by including IPMI's LAN interface (the claimed "virtual management interface") in the BMC to provide additional security by keeping the physical sideband interface between the LAN controller and the BMC processor entirely within the BMC. Doing so would provide additional physical security if, for example, the BMC were implemented as a system on chip because the sideband interface would not be exposed outside the system on chip and thus would be more difficult to access by unauthorized personnel. EX1046, ¶185.

H. Claim 11

The combination of IPMI and Lawrence render obvious the limitations of claim 11. The function and corresponding structure for the "protection means" is discussed above in Section III.E.5, which identifies a VPN as one corresponding structure. See limitation [1.c] above in this Ground 5, including discussion of integrating Lawrence's VPN module 655 in IPMI's LAN controller for IPMI's side-band interface. When integrated into the BMC as discussed at Claim 10 in this Ground 5, Lawrence's VPN module 655 (the claimed "protection means") performs the identical function of protecting the management data due to its use of encryption, and has identical or at least equivalent structure to the 140 patent VPN. EX1046, ¶186.

X. GROUND 6: IPMI AND LAWRENCE IN COMBINATION WITH LEEDY RENDER OBVIOUS CLAIM 4

Claim 1 (from which claim 4 depends) is obvious over the references cited above in Ground 5 for the reasons stated therein. The limitations of claim 4 are obvious over IPMI and Lawrence in combination with Leedy. IPMI discloses a managed platform that includes a main processor and a BMC, but does not disclose many implementation details for the managed platform. For example, IPMI does not disclose any particular processor integrated circuit for the main processor(s) or the BMC, and discloses types of memories but not any particular integrated circuits for the memories used by either the main processor(s) or the BMC. EX1046, ¶187. A POSITA would therefore look elsewhere for information as to how to implement the managed platform including the main processor(s), the BMC, their associated memories, the LAN controller, and other components. EX1046, ¶188.

Leedy discloses a “Vertical System Integration (VSI) method for integration of disparate electronic and other technologies into a single integrated circuit die or component.” EX1045, Abstract. Leedy’s “VSI method of integration lowers the cost difference between lower volume custom electronics products and high volume generic use electronic products by eliminating or reducing circuit design, layout, tooling and fabrication costs.” *Id.*, EX1046, ¶189. Leedy’s VSI fabrication methods “enable the integration as one IC or die that are currently system assemblies of discreet circuits with the benefit that performance limiting circuit

interconnect structures such as long [] on-IC interconnections, IC carriers and sockets, PCBs and PCB edge connectors are eliminated.” EX1045, 2:1-3. The benefits of VSI include a “reduction in complexity of IC manufacturing, testing, packaging and an increased circuit yield resulting in a nominal reduction in manufacturing costs of approximately 10x and commensurate with an approximate nominal 5x increases in net circuit operating performance.” EX1045, 2:4-7. Leedy specifically discloses using VSI to integrate into a single multi-layer component multiple types of devices including microprocessors and memory. *E.g.*, EX1045, 22:17-23:11. Among the types of memory that can be integrated into a single component using Leedy’s VSI technology are DRAM, flash, EEPROM, and SRAM. EX1045, 21:19-20. EX1046, ¶¶190-191.

In light of these disclosures in Leedy, a POSITA would have found it obvious to integrate functional components of IPMI’s managed platform, including at least the main processor(s), the BMC, and the memory used by both the main processor(s) and the BMC, into a single component using Leedy’s VSI methods. EX1046, ¶192. A POSITA would have been motivated to do so in order to obtain the benefits disclosed by Leedy as discussed above, including reduction in manufacturing costs and increases in operating performance, and a POSITA would have had a reasonable expectation of success in so doing. EX1046, ¶193.

As discussed above for Ground 5, claim 2, IPMI discloses that the BMC accesses flash, non-volatile random access memory, and random access memory. In such a single component implementation, all of these components are embedded in each other, and thus all of the aforementioned memory is embedded in the main processor. EX1046, ¶194. Thus, all of these memories accessed by the BMC are embedded into the main processor by virtue of being incorporated into a single component using Leedy's VSI technology. EX1046, ¶195.

XI. GROUND 7: IPMI AND LAWRENCE IN COMBINATION WITH SYVANNE RENDER OBVIOUS CLAIMS 11 AND 12

Claim 1 (from which claim 11 depends) and claim 10 (from which claim 12 depends) are obvious over the references cited above in Ground 5 for the reasons stated therein. Claims 11 and 12 are obvious over those references in combination with Syvanne for reasons similar to those discussed in Ground 2. A POSITA would have found it obvious modify IPMI by implementing a locally-executing firewall in the LAN controller in the BMC to protect management communications by removing unauthorized messages. EX1046, ¶196. A POSITA would have been motivated to do so because IPMI's BMC (like Neufeld's remote management controller 116) can be reached in-band via a public network such as the Internet, and a POSITA would therefore have recognized the desirability of further improving security of the IPMI system by adding a locally executing firewall to IPMI's BMC. EX1046, ¶196. A POSITA would have had a reasonable expectation

of success in modifying IPMI in this manner as such modifications would have involved no more than routine skill and such firewall technology was well-known in the art. EX1046, ¶196.

With respect to claim 11, such a firewall performs the identical function identified in Section III.E.5, and is identical or at least equivalent to the firewall structure identified in Section III.E.5, for the “protection means” limitation. With respect to claim 12, Syvanne’s firewall protects management communications, and the secure transmission tunnel limitation is discussed above in connection with the VPN in limitation [1.c] of Ground 5. EX1046, ¶197.

XII. GROUND 8: IPMI AND LAWRENCE IN COMBINATION WITH FOWLER RENDER OBVIOUS CLAIMS 13 AND 14

Claim 1 (from which claims 13 and 14 depend) is obvious over the references cited above in Ground 5. Claims 13 and 14 are obvious over the combination of those references further in combination with Fowler. EX1046, ¶198. As discussed above in Ground 3, Fowler discloses a network device having a regulated five-volt power supply 78 connected to power via a wall outlet. EX1040, 12:14-18. Fowler further discloses a power fail detector 88 that monitors the power supply 78 and switches over to an uninterruptable power supply (UPS) in the event that the power supply 78 loses power. *Id.* It would have been obvious to a POSITA to integrate Fowler’s power fail detector 88 and UPS into the combined IPMI-Lawrence system by including them in the BMC, and by configuring the power

supply 78 to supply power to the IPMI managed platform and configuring the power fail detector 88 to monitor the power supply 78 and switch the BMC over to the UPS in event of a power failure in power supply 78. EX1046, ¶200. A POSITA would have been motivated to do so in order to ensure that the BMC and its functionality, including the ability to report the power failure to a remote administrator, remain available to remote administrators in the event of a loss of power to the IPMI managed platform. EX1046, ¶201. A POSITA would have had a reasonable expectation of success in so doing because power fail detectors and UPSs were well-known in the art and implementing a UPS in this fashion would have involved no more than ordinary skill. EX1046, ¶201.

Claim 14 will be discussed first below, followed by claim 13.

A. Claim 14

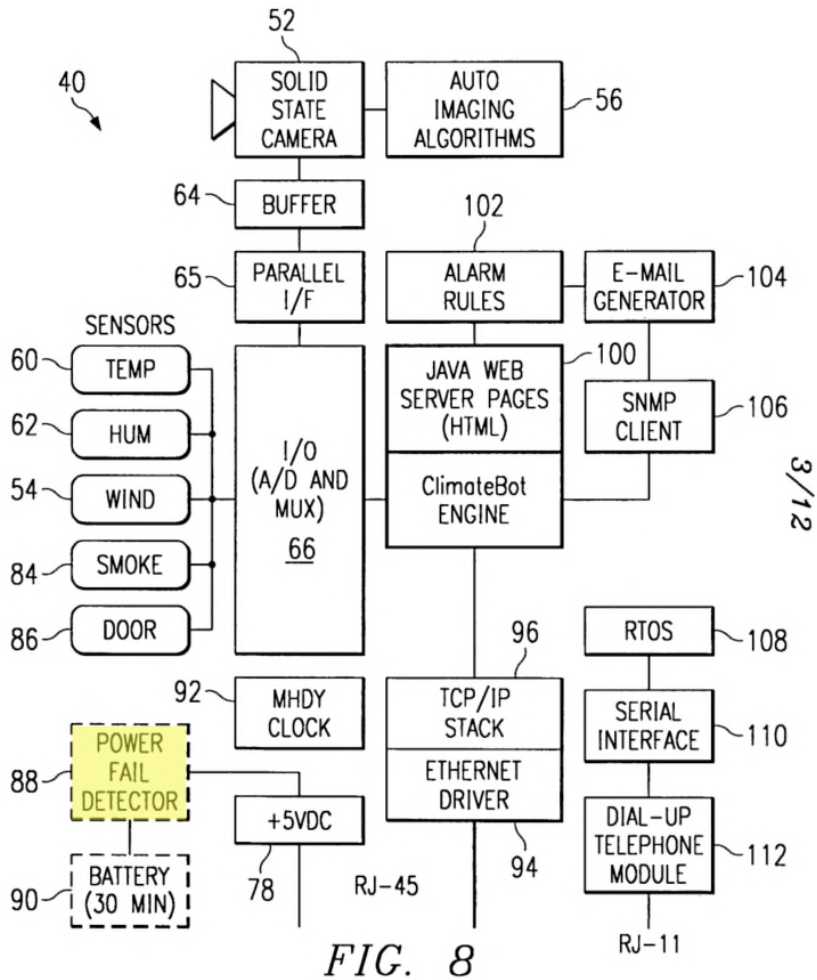
1. Limitation [14.a]

Fowler discloses a “[f]ive volt power supply 78 [that] can receive and transform electrical power from a wall-mounted receptacle to power circuit 50.” EX1040, 12:1-2 and Figs. 7-8; EX1046, ¶203. The power supply 78 constitutes a network power supply as required by limitation [14.a]. It would have been obvious to combine IPMI and Lawrence with Fowler by including Fowler’s five volt regulated power supply 78 in IPMI’s managed platform to provide power to that device. Further, to ensure that the IPMI BMC was available even when power to

the managed platform was not available, a POSITA would have found it obvious to include Fowler's UPS with the power fail detector 88 into the BMC and to configure the power fail detector 88 to detect a loss of power to power supply 78 and switch the UPS to supply power to the BMC for the reasons discussed above. EX1046, ¶204.

2. Limitation [14.b]

The combination of IPMI, Lawrence and Fowler render obvious this limitation. As discussed in Section III.E.7, the function performed by this limitation is "monitoring the status of the network power supply" and the corresponding structure is a UPS that monitors network components for loss of power. Fowler's UPS including the power fail detector 88 highlighted in yellow in Figure 8 below performs the identical function (monitoring the status of the power provided to the power supply 78 supplying power to IPMI's managed platform), and includes identical or at least equivalent structure (a UPS that monitors network components, i.e., the IPMI managed platform, for the loss of power). EX1046, ¶205.



3. Limitation [14.c]

IPMI, Lawrence and Fowler render obvious this limitation for reasons similar to those discussed in Section VII.C (Ground 3, limitation [14.c] in the Neufeld-Fowler combination), with IPMI's remote console taking the place of Neufeld's remote console 5 and IPMI's BMC taking the place of Neufeld's remote management controller 116. EX1046, ¶206. In this combination, Fowler's power fail detector 88 would be configured to notify the IPMI BMC of the failure of

power supply 78 and the BMC would be configured to report the failure to the IPMI remote console. EX1046, ¶206.

B. Claim 13

IPMI and Lawrence in view of Fowler renders obvious the “wherein the at least one the [sic] management access controller includes a monitoring means for monitoring the status of at least one computer network component” limitations of claim 13 under the second disclosed structure for the “monitoring means” (the UPS that monitors network components for loss of external power) for the reasons discussed below for limitation [14.b] in Section XII.A.2 above. EX1042, 5; EX1046, ¶207 (noting that the power supply 78 for the BMC and managed platform constitutes monitoring the status of at least one computer network component).

With respect to the “a network interface for reporting a status of the at least one computer network component to a network management system” limitation of claim 13, see limitation [14.c] in Section XII.A.3 above. EX1046, ¶208.

XIII. GROUND 9: IPMI IN COMBINATION WITH LAWRENCE AND RFC1492 RENDERS OBVIOUS CLAIM 16

A. Claim 16

IPMI and Lawrence render obvious claim 1 from which claim 16 depends for the reasons discussed above in Ground 5. The combination of IPMI and Lawrence together with RFC1492 renders obvious the additional limitations of

claim 16. As discussed in Section III.E.9, the function performed by this claim is “monitoring connection attempts made through the management access controller” and one corresponding structure for performing the above-stated function includes a processor running one or more of RADIUS, TACACS+ and/or LDAP. EX1046, ¶209.

A POSITA would have found it obvious to employ an access server including a processor running the RADIUS protocol to perform authentication for remote users attempting to access the BMC remote management purposes. EX1046, ¶210. The use of access servers such as RADIUS servers as described in RFC1492 was very well-known in the art at the time of the 016 patent for such purposes and thus would have been an obvious choice for a POSITA. EX1046, ¶210. A POSITA would have had a reasonable expectation of success in so doing because implementing access control servers such as RADIUS servers was well within the skill level of a POSITA and involved no more than ordinary skill. EX1046, ¶210.

XIV. DISCRETIONARY DENIAL IS NOT WARRANTED

A. 35 U.S.C. § 314(a) Analysis

The Board should not exercise its discretion to deny institution as the challenges in this Petition present compelling evidence of unpatentability, and because Petitioner hereby stipulates that, if institution is granted, Petitioner will not

raise in the parallel district court litigation identified below any defense based on the same grounds raised, or that could have been raised, in this Petition. “Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation” dated June 21, 2022, at 4-5 and 7-8 (“the PTAB will not discretionarily deny institution if Petitioner presents a *Sotera* stipulation.”).

B. 35 U.S.C. § 325(d) Analysis

The Board should not exercise its §325(d) discretion to deny institution as none of the references relied on for the challenges in this Petition were considered by the examiner. EX1002, front cover. To the extent that the references relied on in this Petition are found to be cumulative of prior art that has been considered by the examiner, the examiner made a material error by not rejecting the claims over the references relied on herein because these references establish unpatentability for the reasons discussed in this Petition.

XV. COMPLIANCE WITH FORMAL REQUIREMENTS

A. Mandatory Notices Under 37 C.F.R. §§ 42.8(b)(1)-(4)

1. Real Party-In-Interest

Petitioner hereby names Lenovo (United States) Inc. as a real-party-in-interest and further identifies Lenovo Group Ltd. as a real party-in-interest solely because Lenovo Group Ltd. is named as a defendant in the parallel district court case listed below.

2. Related Matters

The 140 patent is subject to the following action: *Intellectual Ventures II LLC v. Lenovo Group Ltd.*, Case No. 6:23-cv-00307-ADA-DTG, filed on April 26, 2023 (the “Related Litigation”).

3. Lead and Backup Counsel

Lead Counsel	Backup Counsel
James Heintz Reg. No. 41,828 DLA Piper LLP One Fountain Square 11911 Freedom Drive, Suite 300 Reston, VA 20190-5602 Phone: + 1 703 773 4000 Fax: + 1 703 773 5000 Jim.heintz@us.dlapiper.com	Gianni Minutoli Reg. No. 41,198 DLA Piper LLP One Fountain Square 11911 Freedom Drive, Suite 300 Reston, VA 20190-5602 Phone: + 1 703 773 4000 Fax: + 1 703 773 5000 gianni.minutoli@us.dlapiper.com

4. Service Information

Service information for lead and backup counsel is provided in the designation of lead and backup counsel above. Petitioner agrees to accept electronic service at the email addresses above and at DLA-LenovoIPR-IV@us.dlapiper.com.

B. Proof of Service on the Patent Owner

As identified in the attached Certificate of Service, a copy of this Petition in its entirety is being served by emailing a copy of same (by agreement) to the attorneys of record for the Patent Owner.

C. Power of Attorney

Powers of attorney are being filed with designation of counsel in accordance with 37 C.F.R. § 41.10(b).

D. Standing

In accordance with 37 C.F.R. §42.104(a), Petitioner certifies that 140 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the patent claims on the grounds identified in this Petition.

E. Fees

The undersigned authorizes the Director to charge the fee specified by 37 C.F.R. § 42.15(a) and any additional fees that might be due in connection with this Petition to Deposit Account No. 50-3266.

XVI. PRESERVATION OF RIGHTS

Petitioner reserves all rights to any benefit of changes resulting from challenges based on the recent Supreme Court decision in *Loper Bright. Loper Bright Enters. v. Raimondo*, No. 22-451, slip op. at 35 (U.S. June 28, 2024).

XVII. CONCLUSION

All challenged claims of the 140 patent should be found unpatentable for the reasons discussed in this Petition.

Dated: August 2, 2024

Respectfully submitted,

/James M. Heintz 41,828/

James M. Heintz
Reg. No. 41,828
DLA Piper LLP
One Fountain Square
11911 Freedom Drive, Suite 300
Reston, VA 20190-5602
Phone: + 1 703 773 4000
Fax: + 1 703 773 5000
jim.heintz@us.dlapiper.com

*Attorney for Petitioner Lenovo (United States)
Inc.*

CERTIFICATION UNDER 37 CFR § 42.24(d)

Under the provisions of 37 CFR § 42.24(d), the undersigned hereby certifies that the word count for the foregoing Petition for *Inter Partes* Review totals 13,300 as calculated by Microsoft Word, which is less than the 14,000 allowed under 37 CFR § 42.24(a)(i).

Dated: August 2, 2024

Respectfully submitted,

/James M. Heintz 41,828/

James M. Heintz
Reg. No. 41,828
DLA Piper LLP
One Fountain Square
11911 Freedom Drive, Suite 300
Reston, VA 20190-5602
Phone: + 1 703 773 4000
Fax: + 1 703 773 5000
jim.heintz@us.dlapiper.com

*Attorney for Petitioner Lenovo (United States)
Inc.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned hereby certifies that a copy of the foregoing Petition for *Inter Partes* Review and all Exhibits was provided to Patent Owner by emailing a copy of same (by agreement) to the following attorneys of record for the Patent Owner:

Brian M. Seeve
Bseeve@princetonobel.com

Jonathan DeBlois
Jdeblois@princetonobel.com

Matthew D. Vella
Mvella@princetonobel.com

Robert R. Gilman
Rgilman@princetonobel.com

Karl Anthony Rupp
Krupp@soreylaw.com

Dated: August 2, 2024

Respectfully Submitted,

/ James Heintz 41,828/

James M. Heintz
Reg. No. 41,828

Attorney for Petitioner Lenovo (United States) Inc.