

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

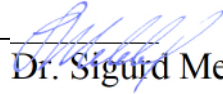
---

**DECLARATION OF SIGURD MELDAL, Dr. Scient.**

I declare under penalty of perjury under the laws of the United States of America that the following is true and correct, that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on August 2, 2024.

---

  
Dr. Sigurd Meldal

## TABLE OF CONTENTS

|                                                                                                                                                                                                                              | Page |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
|                                                                                                                                                                                                                              | Page |
| I. INTRODUCTION .....                                                                                                                                                                                                        | 1    |
| A. Background and Qualifications.....                                                                                                                                                                                        | 1    |
| B. Information Considered.....                                                                                                                                                                                               | 7    |
| II. Legal Standards .....                                                                                                                                                                                                    | 7    |
| A. Legal Standards for Prior Art.....                                                                                                                                                                                        | 7    |
| B. Legals Standards for Anticipation.....                                                                                                                                                                                    | 8    |
| C. Legals Standards for Obviousness .....                                                                                                                                                                                    | 9    |
| III. Overview of THE 140 PATENT .....                                                                                                                                                                                        | 14   |
| A. Summary of the 140 Patent .....                                                                                                                                                                                           | 14   |
| B. Overview of the 140 Patent’s File History.....                                                                                                                                                                            | 15   |
| C. Priority Date of the 140 patent .....                                                                                                                                                                                     | 17   |
| D. Person of Ordinary Skill in the Art .....                                                                                                                                                                                 | 17   |
| E. Claim Construction Under 37 C.F.R. § 42.104(b)(3) .....                                                                                                                                                                   | 17   |
| 1. “said managed network element” (claim 1).....                                                                                                                                                                             | 18   |
| 2. Means-Plus-Function Terms (claims 1, 11, 13, 14 and 16)....                                                                                                                                                               | 18   |
| 3. Claim [1.b]: “an out of band access connection means for<br>connecting said one or more network services or remote<br>users with said secure management access controller for<br>management of said network device” ..... | 19   |
| a. Function: .....                                                                                                                                                                                                           | 19   |
| b. Structure:.....                                                                                                                                                                                                           | 19   |

|     |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |    |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.  | Claim [1.c]: “at least one virtual management interface connection means”: (i) “for connecting said one or more network services or remote users with said secure management access controller”; and (ii) “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 controllers.” ..... | 19 |
| a.  | Function: .....                                                                                                                                                                                                                                                                                                                                                                                                                                               | 20 |
| b.  | Structure.....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 20 |
| 5.  | Claim 11: “protection means for protecting the management data” .....                                                                                                                                                                                                                                                                                                                                                                                         | 20 |
| a.  | Function .....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 20 |
| b.  | Structure.....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 20 |
| 6.  | Claim 13: “monitoring means for monitoring the status of at least one computer network component” .....                                                                                                                                                                                                                                                                                                                                                       | 21 |
| a.  | Function .....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 21 |
| b.  | Structure.....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 21 |
| 7.  | Claim [14.b]: “a monitoring means for monitoring the status of the network power supply” .....                                                                                                                                                                                                                                                                                                                                                                | 21 |
| a.  | Function .....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 21 |
| b.  | Structure.....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 21 |
| 8.  | [14.c] “a reporting means for reporting the status of the network power supply” .....                                                                                                                                                                                                                                                                                                                                                                         | 22 |
| a.  | Function .....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 22 |
| b.  | Structure.....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 22 |
| 9.  | Claim 16: “means for monitoring connection attempts made through the management access controller.” .....                                                                                                                                                                                                                                                                                                                                                     | 22 |
| a.  | Function .....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 22 |
| b.  | Structure.....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 22 |
| IV. | Prior Art References .....                                                                                                                                                                                                                                                                                                                                                                                                                                    | 23 |
| A.  | Patents.....                                                                                                                                                                                                                                                                                                                                                                                                                                                  | 23 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |    |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| B. | 2. Patent Publications .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | 23 |
| C. | 3. Non-Patent Publications .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | 23 |
| V. | GROUND 1: NEUFELD RENDERS OBVIOUS CLAIMS 1-4, 6, 7,<br>10, 11, 13 AND 16.....                                                                                                                                                                                                                                                                                                                                                                                                                                          | 24 |
| A. | Claim 1 .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 28 |
| 1. | [1.pre] A remote device management communication<br>system for securely controlling access to management<br>applications and communications to and from said<br>management applications on network devices in a<br>distributed computer network that includes one or more<br>network services, one or more secure management access<br>controllers, and one or more managed network devices.....                                                                                                                       | 28 |
| 2. | [1.a] at least one secure management access controller<br>connected to one or more data bus of said managed<br>network device for the communication of device<br>management data; .....                                                                                                                                                                                                                                                                                                                                | 33 |
| 3. | [1.b] an out-of-band access connection means for<br>connecting said one or more network services or remote<br>users with said secure management access controller for<br>management of said network device;.....                                                                                                                                                                                                                                                                                                       | 35 |
| 4. | [1.c] at least one virtual management interface<br>connection means for connecting said one or more<br>network services or remote users with said secure<br>management access controller; wherein said virtual<br>management interface connection means provides logical<br>separation of management data from user data and<br>utilizes user interfaces of said managed network element<br>for connecting said one or more network services or<br>remote users with said secure management access<br>controller. .... | 40 |
| B. | Claim 2: The system of claim 1 wherein the at least one secure<br>management access controller includes a flash chip, non-volatile<br>random access memory and random access memory. ....                                                                                                                                                                                                                                                                                                                              | 43 |
| C. | Claim 3: The system of claim 1 wherein the at least one secure<br>management access controller is embedded in the network device<br>to be managed.....                                                                                                                                                                                                                                                                                                                                                                 | 46 |

|      |                                                                                                                                                                                                                                                                                                                                                                                                          |    |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| D.   | Claim 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. ....                                                                                                                                                                   | 46 |
| E.   | Claim 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.....                                                                                                                                                                                                                        | 47 |
| F.   | Claim 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 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. .... | 48 |
| G.   | Claim 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. least one network component to a network management station. ....                         | 49 |
| H.   | Claim 11: The system of claim 10 wherein the virtual management interface includes a protection means for protecting the management data.....                                                                                                                                                                                                                                                            | 50 |
| I.   | Claim 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 network component to a network management station. ....                                                                                    | 50 |
| J.   | Claim 16: The system of claim 1 further comprising a means for monitoring connection attempts made through the management access controller. ....                                                                                                                                                                                                                                                        | 52 |
| VI.  | GROUND 2: NEUFELD IN VIEW OF SYVANNE AND IPFILTER RENDER OBVIOUS CLAIM 12.....                                                                                                                                                                                                                                                                                                                           | 53 |
| VII. | Ground 3: Neufeld in View of FOWLER RENDER OBVIOUS CLAIM 14 .....                                                                                                                                                                                                                                                                                                                                        | 55 |

|       |                                                                                                                                                                                                                                                                                                                                                                                           |    |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| A.    | Limitation [14.a] The system of claim 1 further comprising: a network power supply; .....                                                                                                                                                                                                                                                                                                 | 56 |
| B.    | Limitation [14.b] a monitoring means for monitoring the status of the network power supply; .....                                                                                                                                                                                                                                                                                         | 58 |
| C.    | Limitation [14.c] a reporting means for reporting the status of the network power supply. ....                                                                                                                                                                                                                                                                                            | 59 |
| VIII. | Ground 4: Neufeld in view of Fowler renders obvious claim 13.....                                                                                                                                                                                                                                                                                                                         | 61 |
| IX.   | GROUND 5: IPMI in Combination with Lawrence renders obvious claims 1-3, 6, 7, 10 and 11.....                                                                                                                                                                                                                                                                                              | 61 |
| A.    | Introduction .....                                                                                                                                                                                                                                                                                                                                                                        | 61 |
| B.    | Claim 1 .....                                                                                                                                                                                                                                                                                                                                                                             | 65 |
| 1.    | Limitation [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..... | 65 |
| 2.    | Limitation [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; .....                                                                                                                                                                                                 | 69 |
| 3.    | Limitation [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; .....                                                                                                                                                                       | 70 |

|       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |    |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 4.    | Limitation [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. .... | 73 |
| C.    | Claim 2: .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 76 |
| D.    | Claim 3: .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 78 |
| E.    | Claim 6: .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 79 |
| F.    | Claim 7 .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 81 |
| G.    | Claim 10 .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 81 |
| H.    | Claim 11 .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 82 |
| X.    | Ground 6: IPMI and Lawrence in Combination With Leedy Render Obvious Claim 4 .....                                                                                                                                                                                                                                                                                                                                                                                                                     | 82 |
| XI.   | GROUND 7: IPMI AND LAWRENCE IN COMBINATION WITH SYVANNE RENDERs OBVIOUS CLAIMs 11 and 12 .....                                                                                                                                                                                                                                                                                                                                                                                                         | 85 |
| XII.  | Ground 8: IPMI and Lawrence in Combination With Fowler render obvious claims 13 and 14 .....                                                                                                                                                                                                                                                                                                                                                                                                           | 86 |
| A.    | Claim 14 .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 87 |
| 1.    | Limitation [14.a] The system of claim 1 further comprising: a network power supply;.....                                                                                                                                                                                                                                                                                                                                                                                                               | 87 |
| 2.    | Limitation [14.b] a monitoring means for monitoring the status of the network power supply; .....                                                                                                                                                                                                                                                                                                                                                                                                      | 88 |
| 3.    | Limitation [14.c] a reporting means for reporting the status of the network power supply. ....                                                                                                                                                                                                                                                                                                                                                                                                         | 89 |
| B.    | Claim 13 .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 90 |
| XIII. | Ground 9: IPMI in Combination with Lawrence and RFC1492 Renders Obvious Claim 16.....                                                                                                                                                                                                                                                                                                                                                                                                                  | 90 |
| A.    | Claim 16 .....                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 90 |

## 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 (“Hrastar”)                                                                                   |
| 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                                                                                               |

| <b>Exhibit No.</b> | <b>Description</b>                                                    |
|--------------------|-----------------------------------------------------------------------|
| 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<br>(“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 (this<br>document) |
| 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**

1. I have been retained by counsel for Lenovo (United States) Inc. (“Petitioner”) as an expert witness in the above-captioned proceeding. I have been asked to provide my opinion about the patentability of claims of U.S. Patent No. 8,474,016 (“the ’016 patent,” EX1001) and claims of U.S. Patent No. 8,325,140 (“the ’140 patent,” EX1002).

2. I have been retained at my normal rate of \$550 per hour. No part of my compensation is dependent on the outcome of this proceeding or the specifics of my testimony.

### **A. Background and Qualifications**

3. A detailed record of my professional qualifications, including a list of publications, awards, and professional activities are set forth in my current Curriculum Vitae, a copy of which is attached as Appendix A. This Curriculum Vitae lists many of the publications that I have authored or co-authored.

4. I received a Dr. Scient. in Informatics in 1986 from the University of Oslo, Norway and a thesis-based Cand. Scient. (Master of Science equivalent) with minor in mathematics and statistics in 1982 from the University of Oslo, Norway. My doctoral thesis was “On Hierarchical Abstraction and Partial Correctness of Concurrent Structures.”

5. My professional background is in the design of computer programs and software development spanning a career of over 30 years in the field. Relevant expertise includes cybersecurity and the design and operation of embedded, server and networked systems, with handheld systems such as mobile devices and phones, and with user interfaces and secure architecture and protocol design for such systems.

6. I was on the faculty in the department of Informatics at the University of Bergen in Bergen, Norway, from 1987 to 1998, first as “førsteamanuensis” (Associate Professor equivalent) and then awarded the rank of full Professor in 1990. I served as Department Chair of Informatics between 1993 and 1995. I was also a visiting and consulting Professor at Stanford University from 1989 to 1998 in its Electrical Engineering Department. In 1997, I also served as the Director of the Computer Science Program at the College of Notre Dame.

7. I was on the faculty in the Department of Computer Science at California Polytechnic State University in San Luis Obispo, California, from 1997 to 2002—first as an Associate Professor, then as Associate Chair in 1999, and lastly as Professor and Chair of the Computer Science Department from 2000 to 2002.

8. I was also on the faculty in the departments of Computer Engineering and Computer Science at San Jose State University in San Jose, California, from

2002 to 2022 as a tenured Professor. I served as Chair of the Computer Engineering Department from 2002 to 2013, and as Director of the Cybersecurity + Big Data Initiative at San Jose State University from 2013 to 2014.

9. I was also the Founding Director of the Silicon Valley Big Data and Cybersecurity Center at San Jose State University from 2014 to 2016. I was in charge of the development of the Cloud Computing and Virtualization and the Enterprise Software Technologies specializations within the MS Software Engineering degree program. The specializations were introduced in 2011 and built on our deep background in enterprise systems development coupled with a close engagement with the software engineering communities of Silicon Valley. Besides the consultative processes of industry engagement in the development, the specializations benefited from the employment of cloud computing and virtualization practitioners as lecturers for core courses. Recognizing the importance of the subject matter to future software engineers, we also included it as part of the undergraduate BS Software Engineering degree.

10. Over the course of my career, I have worked with remote-accessed computer systems for some three decades, starting with the very early systems (such as based on the X Window Systems in the late 1980s).

11. I have served as Co-Director of the National Science Foundation (NSF) Center for Research in Ubiquitous Secure Technologies at the University of

California-Berkeley in Berkeley, California from 2005 to 2016. I also have served as a member of the California Task Force on Cyber Security from 2014 to 2016.

12. I also have extensive consulting experience in the design of computer programs and software development. My consulting experience has involved middleware systems analysis, systems risk evaluation, mobile device technologies, networked military command-and-control systems, satellite and land-based information and communication systems, secure systems and networks design, network security and supporting protocols, networked media systems and user interface designs among others. A recurring theme in my work has been the design of reliable and secure systems in a networked enterprise context.

13. I have received several honors and awards over the course of my career, including the Fulbright-Hayes Fellowship, the Carl-Erik Fröberg Award, a Certificate of Recognition from the California State Assembly, and a Certificate of Special Recognition from the U.S. House of Representatives.

14. I have served on many professional committees and organizations. For example, I am a member of the Fulbright Association, and a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE) and of the Association for Computing Machinery (ACM). I also serve as Vice Chair of Operations of the international Engineering Accreditation Commission of ABET, Inc. The Engineering Accreditation Commission of ABET defines the global standards for

engineering education and determines whether programs are up to those standards or not.

15. I have authored or co-authored more than 50 publications including technical paper, textbooks, textbook chapter, and article, and have delivered numerous presentations including keynotes at several international conferences and workshops. These publications of topics including, but not limited to: cyber security, network security and protocols, privacy, architecture of programming languages, software design prototyping and engineering, distributed system design and architecture, concurrent processing, and user interfaces.

16. Examples of publications I have authored or co-authored on the topic of security are:

- Sigurd Meldal, Kristen Gates, Russell Smith, and Xiao Su. “Security, Safety and Privacy – Pervasive Themes for Engineering Education.” In *Proceedings of the International Conference on Engineering Education (ICEE)*, March 2008.
- Daniel Manson, Sigurd Meldal, Carol Sledge, Stephen M. Maurer, John C. Mitchell, Erich Spengler, Janos Sztipanovits, and Javier Torner. “Learning Modules for Security, Privacy and Information Assurance in Undergraduate Engineering Education.” In *Proceedings of the 36th Annual Frontiers in Education Conference (FIE)*, October 2006.
- Sigurd Meldal and David C. Luckham. “NSA’s MISSI Reference Architecture – From Prose to Precise Specification.” In *Requirements Targeting Software and Systems Engineering, Lecture Notes in Computer Science (LNCS) 1526*, pp. 293–329. Springer-Verlag, 1998.

- Peter C. Ölveczky and Sigurd Meldal. “Specification and Prototyping of Network Protocols in Rewriting Logic.” In *Proceedings of Norsk Informatikkonferanse (NIK ‘98)*, November 1998.

17. I have authored numerous publications in system architecture and design. Relevant examples of such publications include:

- David C. Luckham, James Vera, and Sigurd Meldal. “Key Concepts in Architecture Definition Languages.” In *Foundations of Component Based Systems*, pp. 23–46. Cambridge University Press, 2000.
- Sigurd Meldal and A. I. Vermesan. “Verification Oriented Development of Knowledge Based Systems.” In *New Review of Applied Expert Systems*, vol. 2, pp. 91–104. 1996.
- Sigurd Meldal. “Reference Architectures and Conformance.” In *Proceedings of the International Workshop on Requirements Targeting Software and Systems Engineering (RTSE)*, April 1998.
- Sigurd Meldal. “Supporting Architecture Mappings in Concurrent Systems Design.” In *Proceedings of the 1990 Australian Software Engineering Conference (ASWEC ‘90)*, May 1990.

18. I have also authored several publications in software design and implementation. Relevant examples of such publications include:

- Sigurd Meldal, Gene L. Fisher, Daniel J. Stearns, and Peter C. Ölveczky. “Software Prototyping.” In *Wiley Encyclopedia of Electrical and Electronics Engineering*. Wiley Online Library, 1999.
- John Mitchell, Sigurd Meldal, and Neel Madhav. “An Extension of Standard ML Modules with Subtyping and Inheritance.” In *Information and Control*, vol. 71, pp. 95–130. 1991.
- Daniel J. Stearns, C. S. Turner, and Sigurd Meldal. “Ten Pounds in a Five-Pound Sack: Providing Software Engineering Students with Management Experience.” In *Proceedings of the International Conference on Engineering Education (ICEE)*, August 2001.

- Neel Madhav and Sigurd Meldal. “An Object-Oriented Approach to Formal Specification of Reactive Systems.” In *Proceedings of the 11th International Conference on Distributed Computing Systems (ICDCS)*, May 1991.

**B. Information Considered**

19. My opinions are based on my years of education, research, and experience, as well as my study of relevant materials. In forming my opinions, I have considered the material identified in this declaration and in the Petition.

20. I may rely upon these materials and/or additional materials to respond to arguments raised by Intellectual Ventures (“PO”). I may also consider additional documents and information in forming any necessary opinions, including documents that may not yet have been provided to me.

21. My analysis of the materials is ongoing, and I will continue to review any new material as it is provided. This declaration represents only those opinions I have formed to date. I reserve the right to revise, supplement, or amend my opinions stated herein based on new information and on my continuing analysis of the materials provided.

**II. LEGAL STANDARDS**

**A. Legal Standards for Prior Art**

22. I understand that a patent or other publication must first qualify as prior art before it can be used to invalidate a patent claim.

23. I understand that a U.S. or foreign patent qualifies as prior art asserted patent if the date of issuance of the patent is prior to the invention of the asserted patent. I further understand that a printed publication, such as an article published in a magazine or trade publication, qualifies as prior art to an asserted patent if the date of publication is prior to the invention of the asserted patent.

24. I understand that a U.S. or foreign patent also qualifies as prior art to an asserted patent if the date of issuance of the patent is more than one year before the filing date of the asserted patent. I further understand that a printed publication, such as an article published in a magazine or trade publication, constitutes prior art to an asserted patent if the publication occurs more than one year before the filing date of the asserted patent.

25. I understand that a U.S. patent qualifies as prior art to the asserted patent if the application for that patent was filed in the United States before the invention of the asserted patent.

**B. Legals Standards for Anticipation**

26. I understand that documents and materials that qualify as prior art can be used to invalidate a patent claim via anticipation or obviousness.

27. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a

comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

28. I understand that a prior art reference "anticipates" an asserted claim, and thus renders the claim invalid, if all elements of the claim are disclosed in that prior art reference, either explicitly or inherently (i.e., necessarily present).

29. I understand that anticipation in an inter partes review must be shown by a preponderance of the evidence.

### **C. Legals Standards for Obviousness**

30. I understand that even if a patent is not anticipated, it is still invalid if the differences between the claimed subject matter and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the pertinent art.

31. I understand that a person of ordinary skill in the art provides a reference point from which the prior art and claimed invention should be viewed. This reference point prevents one from using his or her own insight or hindsight in deciding whether a claim is obvious.

32. I also understand that an obviousness determination includes the consideration of various factors such as (1) the scope and content of the prior art, (2) the differences between the prior art and the asserted claims, (3) the level of

ordinary skill in the pertinent art, and (4) the existence of secondary considerations such as commercial success, long-felt but unresolved needs, failure of others, etc.

33. I understand that an obviousness evaluation can be based on a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but other times the nexus linking two or more prior art references is simple common sense. I further understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

34. I understand that if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

35. I also understand that practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I further understand that a person of ordinary skill in the art looking to overcome a problem will often be able to fit together the teachings of multiple publications. I understand that obviousness

analysis therefore takes into account the inferences and creative steps that a person of ordinary skill in the art would employ under the circumstances.

36. I understand that a particular combination may be proven obvious merely by showing that it was obvious to try the combination. For example, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp because the result is likely the product not of innovation but of ordinary skill and common sense.

37. The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, the patent claim is likely obvious.

38. It is further my understanding that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill in the art, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

39. I understand that a proposed obviousness combination does not need to be the preferred, or most desirable, combination available, in order to render a claim obvious. Instead, there must be something that suggests the desirability of the proposed combination, not necessarily something that suggests that the proposed combination is the most desirable combination available.

40. Similarly, I understand that for purposes of obviousness, when a motivating benefit comes at the expense of another benefit, that does not nullify the proposed obviousness combination or modification. Likewise, a proposed obviousness combination does not fail merely because it may be inferior to other systems used for the same use.

41. I also understand that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements between the multiple references. Likewise, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. Instead, the test is whether a claim is rendered obvious by the teachings of the prior art as a whole.

42. I understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art.

43. I understand that secondary indicia of non-obviousness may include: (1) a long felt but unmet need in the prior art that was satisfied by the invention of the patent; (2) commercial success of processes covered by the patent; (3) unexpected results achieved by the invention; (4) praise of the invention by others skilled in the art; (5) taking of licenses under the patent by others; (6) deliberate copying of the invention; (7) failure of others to find a solution to the long felt need; and (8) skepticism by experts.

44. I also understand that there must be a relationship between any such secondary considerations and the invention. I further understand that contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

45. In sum, my understanding is that prior art teachings are properly combined where a person of ordinary skill in the art having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

46. I understand that obviousness in an inter partes review must be shown by a preponderance of the evidence.

### **III. OVERVIEW OF THE 140 PATENT**

#### **A. Summary of the 140 Patent**

47. 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 such as routers in a secure manner. EX1002, 1:19-45 and 2:1-7.

48. The 140 patent discloses including 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.

49. 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**

50. 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).

51. 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.

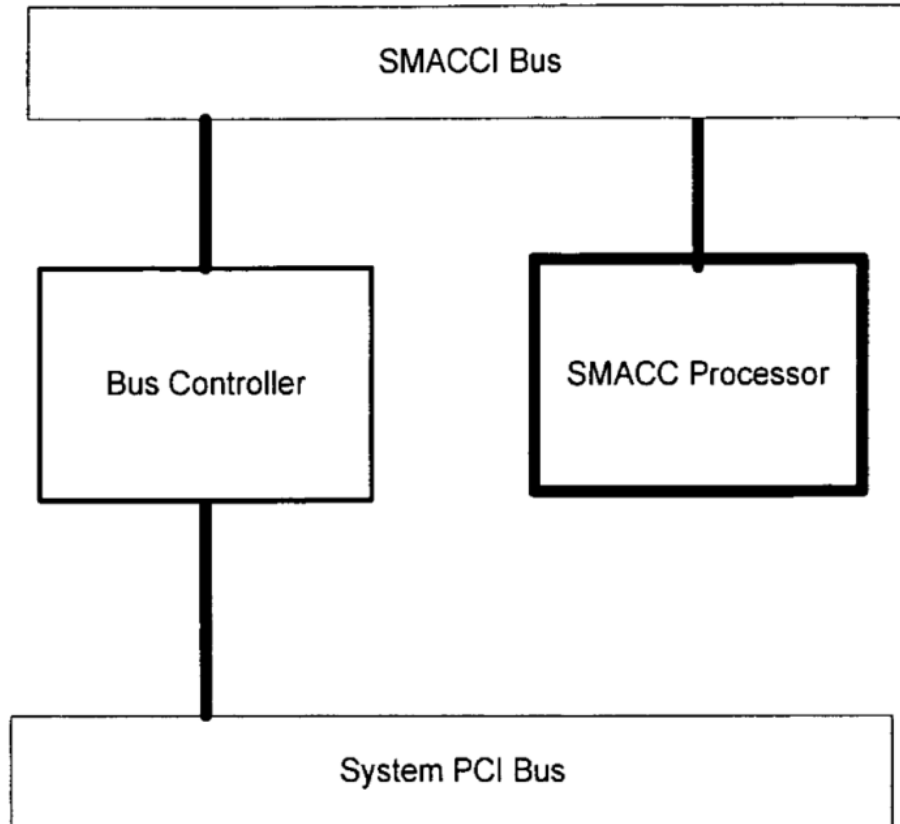


Fig. 28

52. 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**

53. I have been instructed by counsel for Petitioner that the 140 patent is not entitled to any priority date earlier than October 21, 2003, and I have applied that instruction in my analysis when forming my opinions.

**D. Person of Ordinary Skill in the Art**

54. In my opinion, 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.

55. In this regard, all of the technologies, including Neufeld, IPMI, Lawrence, Fowler, Leedy, and all other references described below, would have been within the knowledge of such a person of ordinary skill in the art.

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

56. I understand from counsel for Petitioner that claims in this IPR should be construed in accordance with their "ordinary and customary meaning" as understood by one of ordinary skill in the art at the time of the invention.

57. In this declaration, I apply the claim language's ordinary and customary meaning, unless indicated otherwise below.

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

58. For the purposes of this IPR, I have been asked to address unpatentability of this term as meaning “said managed network device.” I have been informed that this is how PO has indicated that this term should be construed in the parallel district court litigation (the “Related Litigation”).

59. I have complied with that request. I have been informed that, because I addressed unpatentability under both constructions, it is not necessary to address indefiniteness for the purposes of this IPR. However, I reserve the right to form and offer an opinion as to whether this term is indefinite if asked to do so in another proceeding, including but not limited to a district court proceeding involving the 140 patent.

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

60. I have been informed that the district court in the Related Litigation has construed each of the following limitations as a means-plus-function limitation subject to 35 U.S.C. § 112, ¶ 6 as described below. I have been asked by counsel for Petitioner to follow that construction for the purposes of my analysis, and I have done so.

61. I understand from counsel for Petitioner that 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.

**3. Claim [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”**

**a. Function:**

62. 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:**

63. 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. Claim [1.c]: “at least one virtual management interface connection means”: (i) “for connecting said one or more network services or remote users with said secure management access controller”; and (ii) “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 controllers.”**

**a. Function:**

64. 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**

65. 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 for protecting the management data”**

**a. Function**

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

**b. Structure**

67. The corresponding structures include a firewall, VPN secure tunnels, and authentication and authorization applications. EX1002, 6:34-7:6; EX1042, 4.

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

**a. Function**

68. 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**

69. The corresponding structure is 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. Claim [14.b]: “a monitoring means for monitoring the status of the network power supply”.**

**a. Function**

70. 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**

71. 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. [14.c] “a reporting means for reporting the status of the network power supply”**

**a. Function**

72. 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**

73. 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**

74. 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**

75. 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. PRIOR ART REFERENCES

76. The prior art references in the challenges for which I have offered an opinion, and the basis on which those references qualify as prior art, are as follows:

##### A. Patents

77. I have been informed that the patents listed below qualify as prior art under the statutory bases shown in the corresponding row of the table.

| 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)          |

##### B. 2. Patent Publications

78. I have been informed that the patent publications listed below qualify as prior art under the statutory bases shown in the corresponding row of the table.

| 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)          |

##### C. 3. Non-Patent Publications

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

80. 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).

81. 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.

82. 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).

83. 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 the date specified by [https://web.archive.org/web/20031002054319/http://www.intel.com/design/servers/ipmi/RMCP+\\_and\\_SOL\\_Proposals.pdf](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**

84. 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 modem, a serial port or an Ethernet interface. EX1005, ¶¶[0011]-[0012].

85. 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].

86. 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:

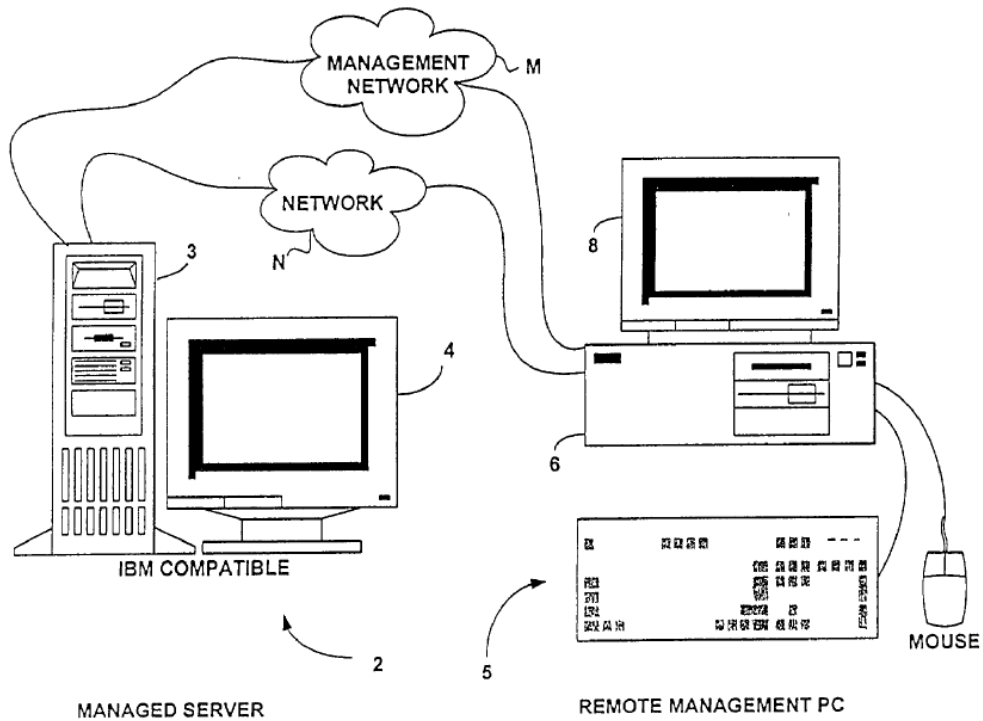
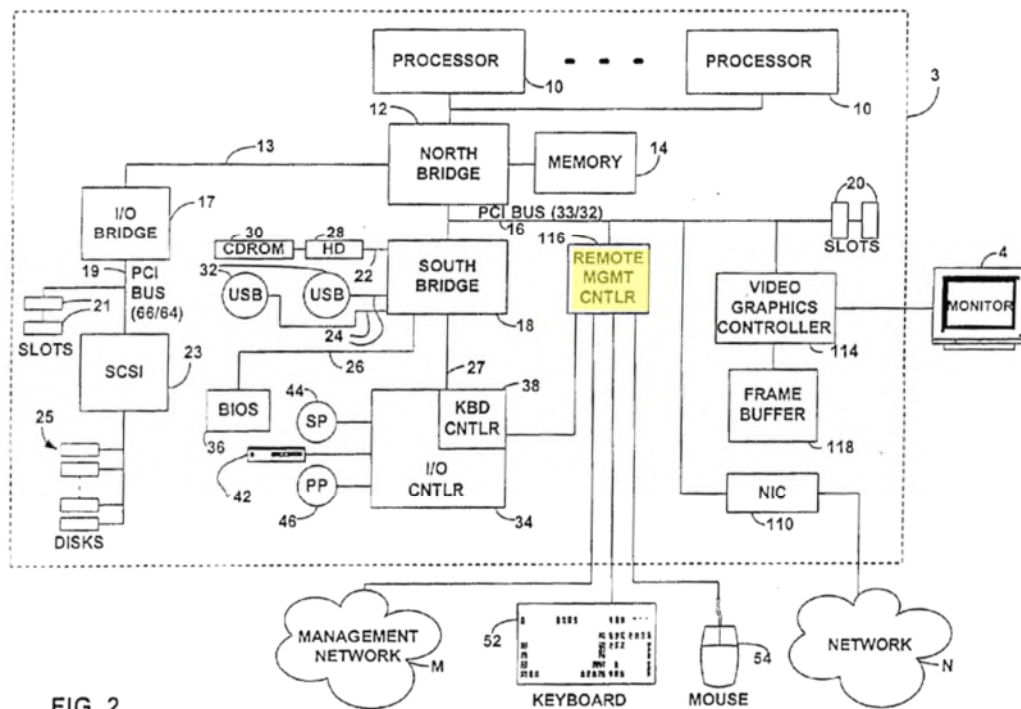
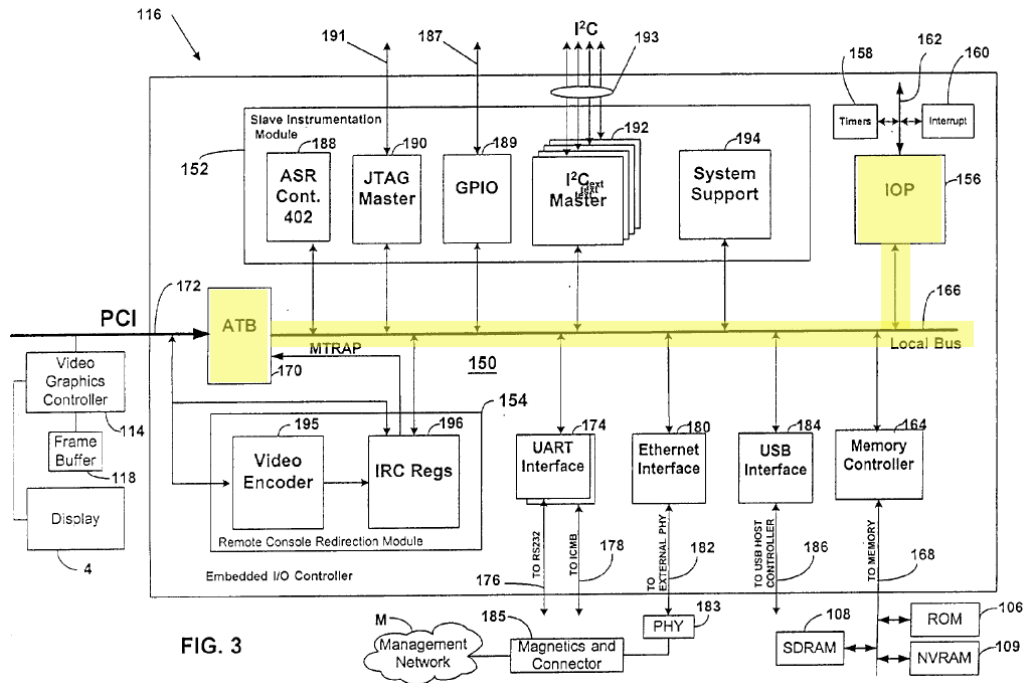


FIG. 1

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



88. The remote management controller 116 includes a processor, IOP 156, which is connected to a local bridge 166 that in turn is connected to an 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 (with highlighting). The server's Network Interface Controller ("NIC") 110 is also connected to the PCI bus 172 as shown above.



89. Also connected to the local bus 166 are a slave instrumentation panel 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.

#### A. Claim 1

1. [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.

90. 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. The network N can be virtually any sort of network capable of transmitting data between two devices. EX1005, ¶[0035].

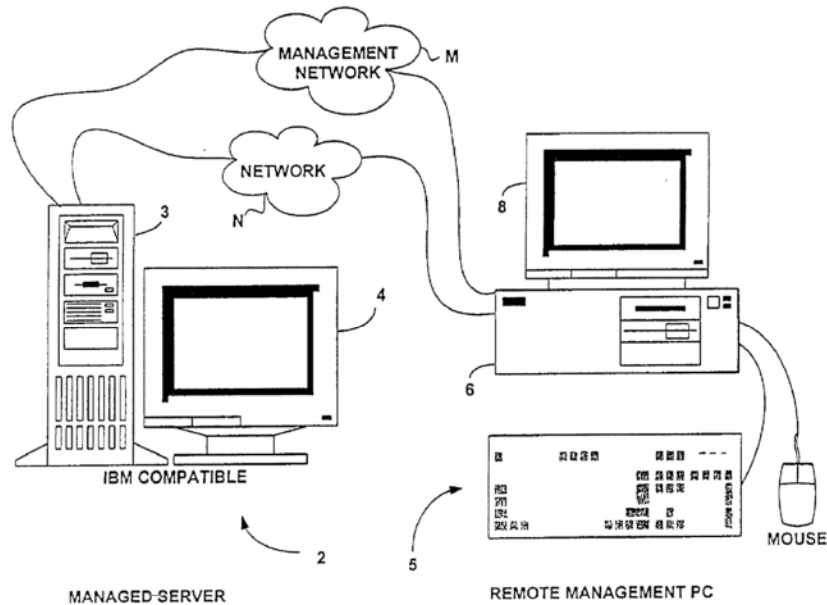


FIG. 1

91. The managed server 2 includes 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] and Figs. 2 and 3. The remote server management controller 116 is the claimed “secure management access controller.”

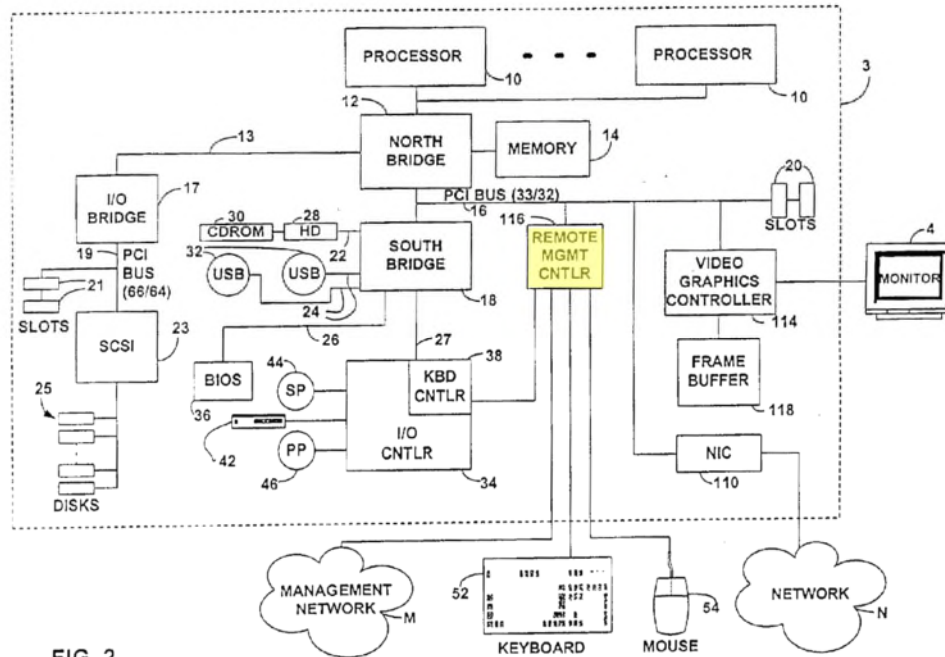


FIG. 2

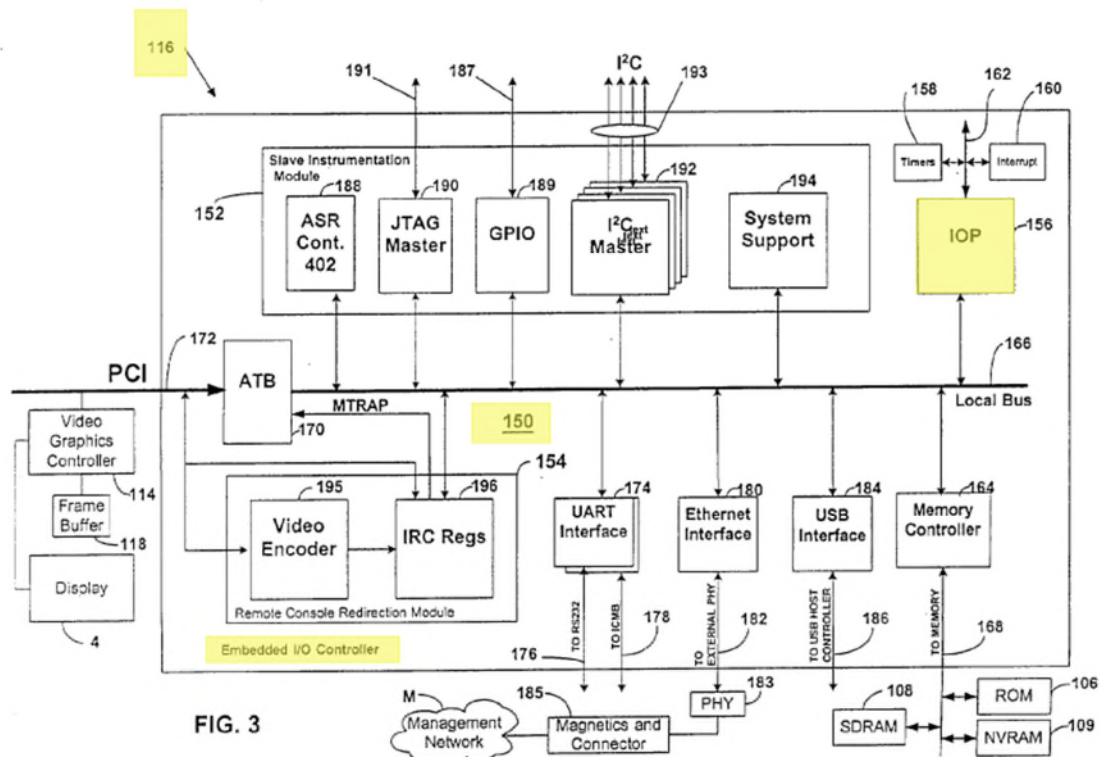


FIG. 3

92. 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].

93. 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] and 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.

94. 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].

95. Neufeld further discloses that the 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].

96. 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* ¶[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].

97. 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]. Each device directly connected to the Internet has a unique IP address which other machines use to find that device. DNS translates domain names to IP addresses. This translation eliminates the need for a human being to remember an IP address and instead allows a human being to remember only human readable domain names. For example, instead of remembering IP addresses, such as 93.184.215.14, a user can remember the domain name “www.example.com.”

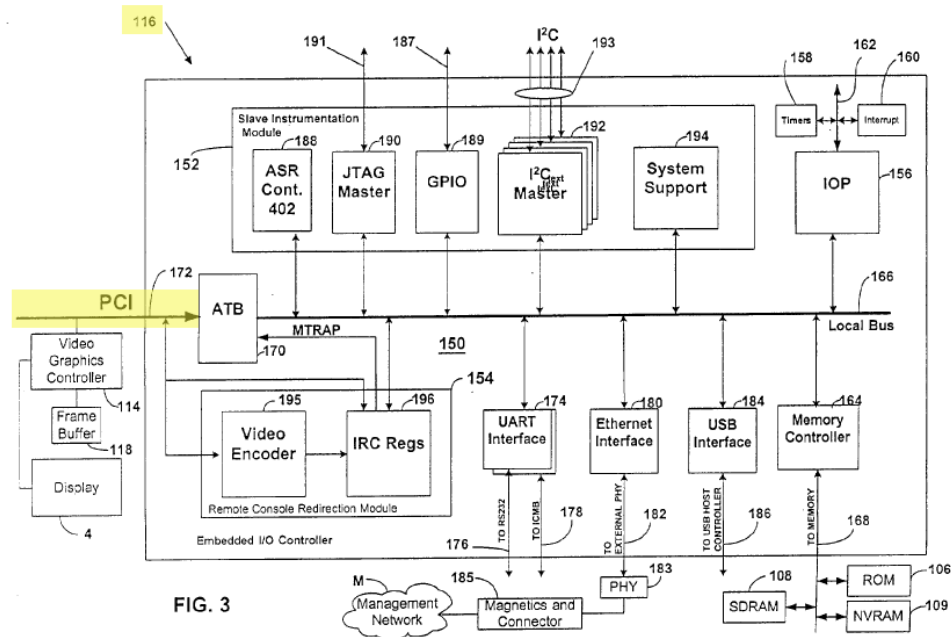
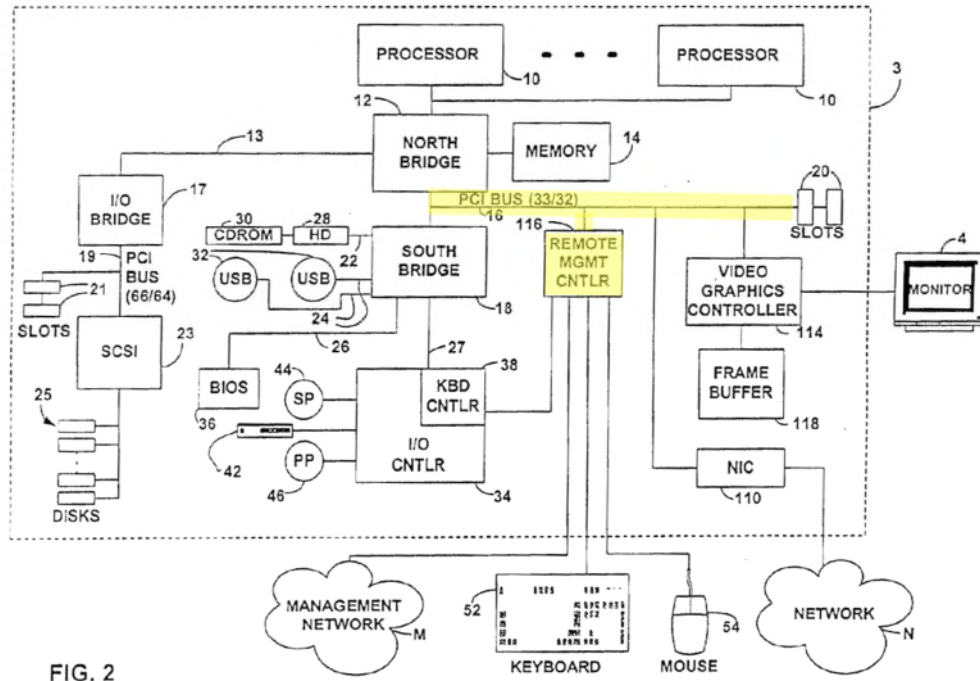
98. As recited by the preamble, the claimed “managed network devices” are Neufeld’s managed servers 2, and the claimed “secure management access controllers” are Neufeld’s remote server management controller 116 which includes IOP 156 as discussed above.

**2. [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;**

99. 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, which is “one or more data bus” of the managed sever 2.

EX1005, ¶¶[043], [0057] and Figs. 2 and 3 (highlighting added).



100. Neufeld further discloses that device management data is communicated to the remote server management controller 116 via the PCI bus 16/172. Neufeld discloses that NIC 110 is connected to PCI bus 16/172 as well as the network N as shown in Fig. 2 above and discussed at ¶[0045], and that the “remote management controller 116 connects to . . . the network N . . . to provide functionality for accessing interacting, and monitoring the managed server 2 from the remote console 5.” EX1005, ¶[0043]; *see also* ¶¶[0014]-[0015] (discussing in-band communication of management data) and [0022] (discussing network administrator accessing managed server 2 from home or while traveling, either of which would occur via the public Internet).

101. Because Neufeld discloses that a management request may be received in-band via Network N/NIC 110, and because Neufeld discloses that NIC110 is attached to the same PCI bus 16/172 as the remote server management controller 116, Neufeld 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.

3. **[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;**

102. 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.” The corresponding structure for performing this function includes an Ethernet network or the PSTN.

103. 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].

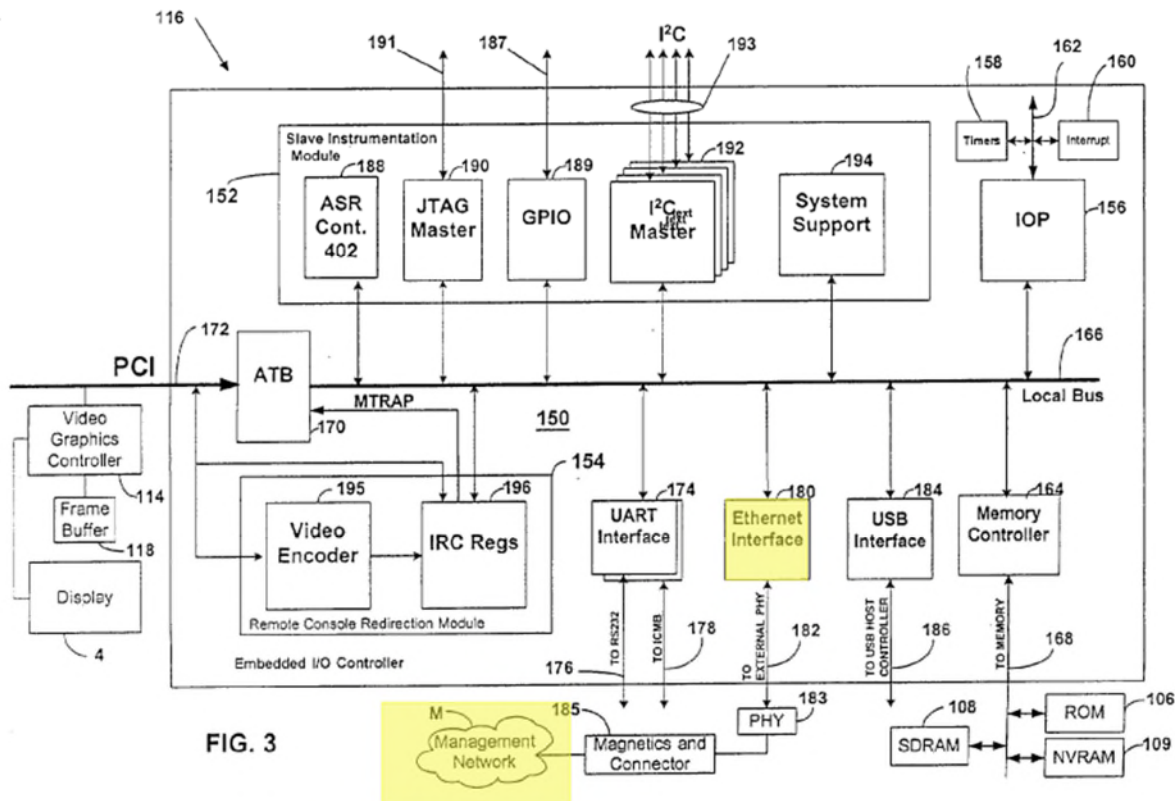
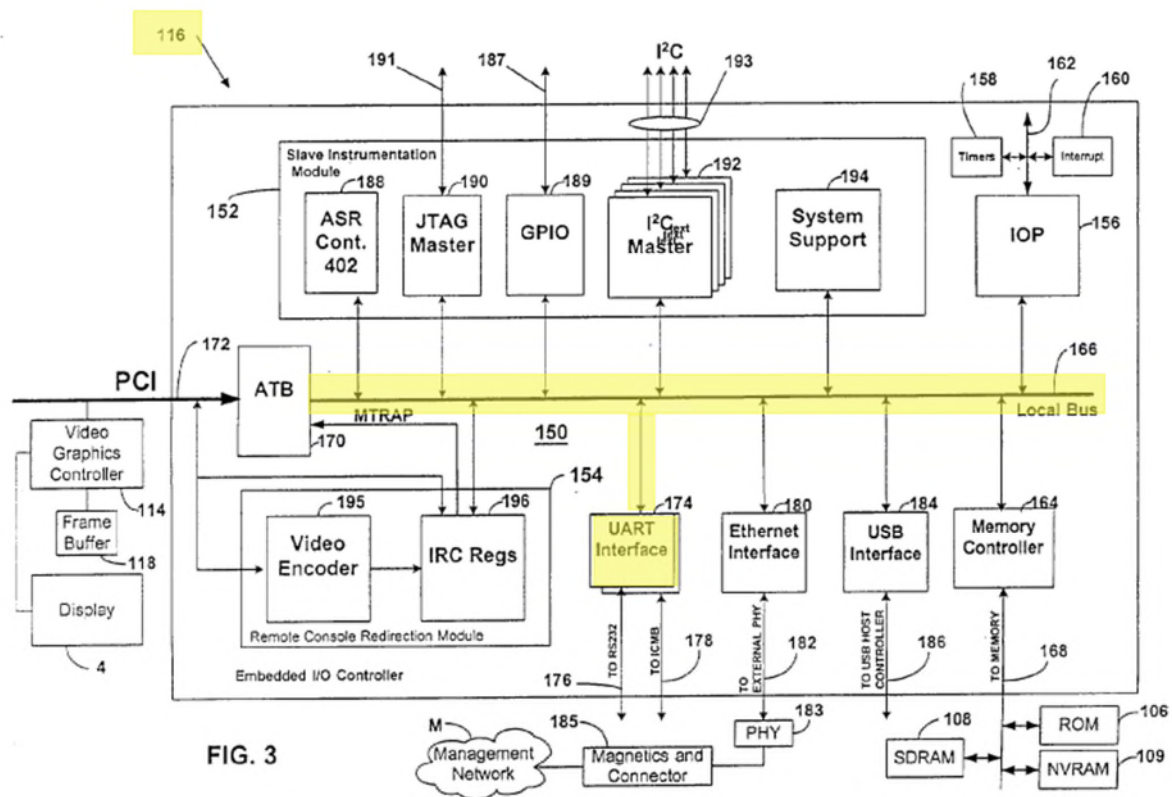


FIG. 3

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, an Ethernet network. EX1002, 12:37-46.

104. 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 PC5 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.

105. 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.



106. 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. Neufeld's UART interface module 174 and modem performs the identical function of connecting a remote user at remote management PC5 with the remote server management controller 116 for the communication of management data. EX1005, ¶[0059].

107. 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. 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.

4. **[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.**

108. 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.

109. 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].

110. Neufeld further discloses that in order for a network administrator to access the server (which a POSITA would have understood involves communications with Neufeld's remote server management controller 116 given that it is a network administrator that is accessing the server) from a remote terminal located outside of work, the administrator must typically use a virtual private network. EX1005, ¶[0022]; *see also* ¶[0088, Table 4, User Id 7]. 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.

111. 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.

112. 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. POSITA would have had knowledge of point-to-point VPN tunneling at the time of invention, and would have found it obvious to configure Neufeld's managed server to employ such tunneling to implement Neufeld's VPN 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. Moreover, L2TP/IPsec (Layer Two Tunneling Protocol (L2TP) with Internet Protocol Security (IPSEC) is a tunneling protocol used to support VPNs or as part of the delivery of services by ISPs. It uses encryption ('hiding') only for its own control messages (using an optional pre-shared secret). L2TP does not provide any encryption or confidentiality of content by itself. Rather, it provides a tunnel for Layer 2 (which may be encrypted), and the tunnel itself may be passed over the Layer 3 encryption protocol IPsec.

113. 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 identical function

performed by the VPN technology of the 140 patent, namely providing logical separation of user data and management data.

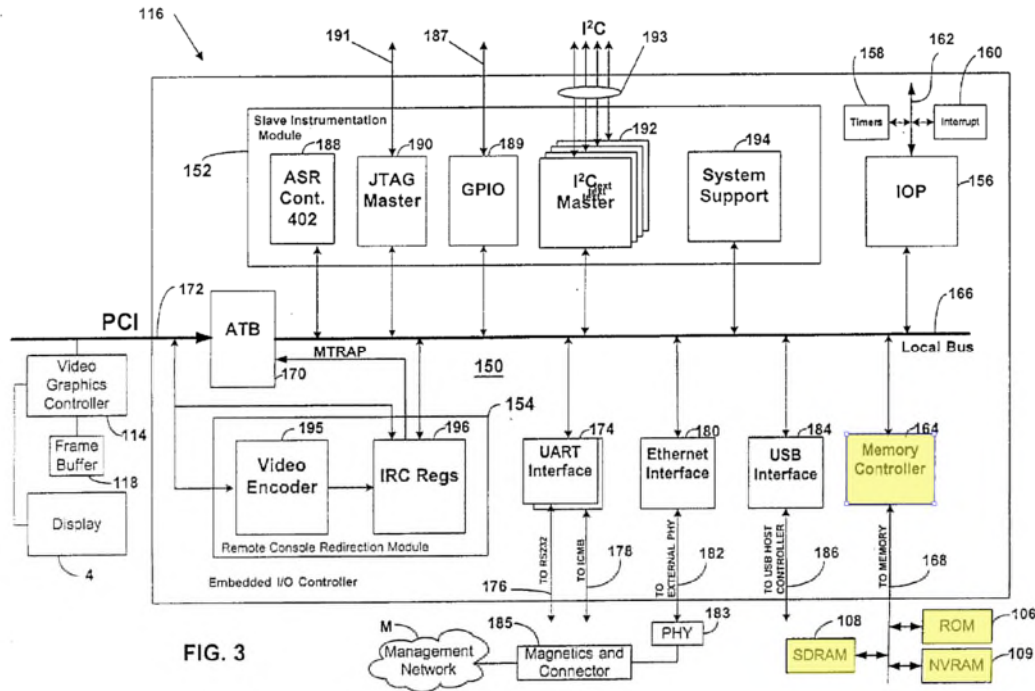
114. The use of a dedicated VPN necessarily provides for logical separation because the VPN tunneling necessarily differentiates traffic for the dedicated VPN from other traffic.

115. 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.

**B. Claim 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.**

116. Neufeld renders obvious claim 2. Neufeld discloses that the remote server management controller 116 includes a memory controller 164 that is coupled to an internal local bus 166 which is coupled to the IOP 156. The memory controller 164 is, in turn, 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].



117. SDRAM is a form of random access memory. NVRAM is an acronym that stands for non-volatile random access memory. ROM is also a form of non-volatile random access memory: it is non-volatile memory because its contents are maintained even if power is removed from the device, and is a form of random access memory because its contents may be accessed in any order, which is distinct from types of memory such as magnetic tape where such access is not possible.

118. 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.

119. 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 is a simple 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. *See also* the following discussion of claim 3.

**C. Claim 3: The system of claim 1 wherein the at least one secure management access controller is embedded in the network device to be managed.**

120. 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]. It would have been obvious to a POSITA to include the memories recited in claim 2 in this implementation.

**D. Claim 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.**

121. 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 ¶126) in a single integrated circuit using such technology. EX1005, ¶[0044].

122. 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.

123. A POSITA would have been motivated to do so in order to reduce chip count and associated manufacturing costs.

124. 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].

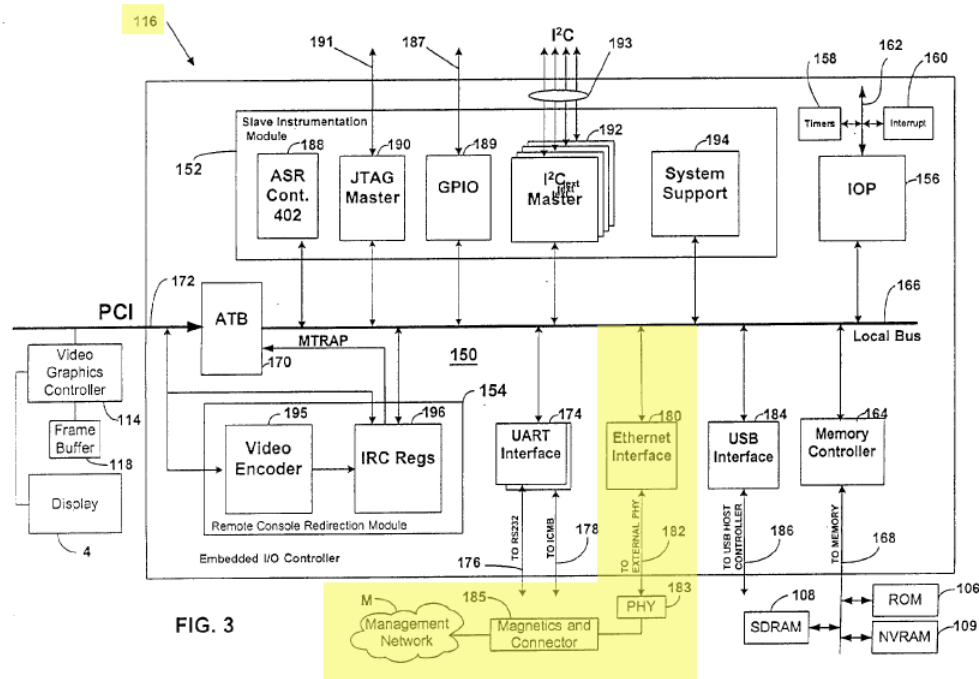
**E. Claim 6: The system of claim 1 wherein the out-of-band access connection means comprises: a communication system; and a secure management access controller interface device.**

125. Neufeld discloses this limitation of this claim to render obvious claim 6. Neufeld's management network M and the devices in that network including Neufeld's remote management PC 5, constitute the claimed "communication system," and Neufeld's Ethernet Interface 180 and/or PHY 183 is a claimed "secure management access controller interface device."

126. 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) and Fig. 3 below (with highlighting).

127. 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 (also a claimed “secure management access controller interface device”).



**F. Claim 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 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.**

128. 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 to connect to a corresponding modem in the remote management PC 5 (the claimed “communication system”).

129. Additionally, see 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”).

**G. Claim 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. least one network component to a network management station.**

130. Neufeld discloses and/or renders obvious the limitations of this claim. 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.

**H. Claim 11: The system of claim 10 wherein the virtual management interface includes a protection means for protecting the management data.**

131. Neufeld discloses and/or renders obvious the limitations of this claim.

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 VPN. With respect to other corresponding structures for this limitation, see Ground 2 below.

**I. Claim 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 network component to a network management station.**

132. Neufeld discloses this limitation to render obvious claim 13. As discussed in Section III.E.6 above, 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.

133. 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 monitoring of the of the video graphics controller and display.

134. 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. 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).

135. Neufeld also discloses that data intercepted in this manner may be redirected to other outputs of the 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. For example, at a minimum, the presence of data on the bus indicates the bus and the transmitter of the data are working. 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.

**J. Claim 16: The system of claim 1 further comprising a means for monitoring connection attempts made through the management access controller.**

136. Neufeld discloses this limitation to render claim 16 obvious. As discussed in Section III.E.7, 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.

137. Neufeld discloses structure (i) above. Neufeld discloses that 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].

138. 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. 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] and Tables 1-4.

## **VI. GROUND 2: NEUFELD IN VIEW OF SYVANNE AND IPFILTER RENDER OBVIOUS CLAIM 12**

139. 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. 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.

140. 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, including the use of L2TP/IPsec to create a secure L2TP tunnel protected by IPsec, to provide logical separation of user data and management data in limitation [1.c] in Ground 1 above.

141. A POSITA would have found it obvious to implement a firewall on the IOP 156 of Neufeld’s remote management controller 116 in view of Syvanne. 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 and 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 known in the art. EX1022 at 1.

142. 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.

143. A POSITA therefore 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 in view of Syvanne's teaching of using locally executing software firewalls as disclosed in IPFILTER on devices exposed to foreign networks. 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.

## **VII. GROUND 3: NEUFELD IN VIEW OF FOWLER RENDER OBVIOUS CLAIM 14**

144. 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 utility company 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 utility company, switches the device to receive power from the UPS, and notifies the device's CPU of the power failure. EX1040, 12:14-18.

145. 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]. The combination of Neufeld and Fowler (EX1040) renders obvious the limitations of claim 14 for the reasons discussed in further detail below.

**A. Limitation [14.a] The system of claim 1 further comprising: a network power supply;**

146. 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. Thus, Neufeld discloses and renders obvious this limitation.

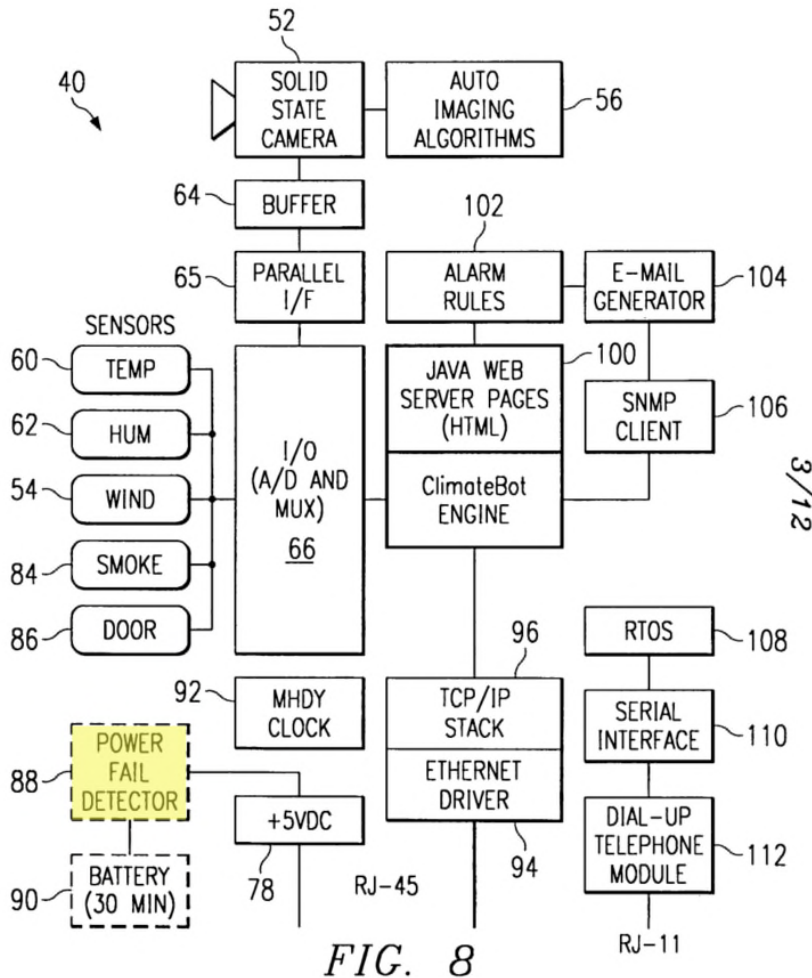
147. To the extent the foregoing discussion in Neufeld is found to be insufficient to disclose a network power supply, Fowler discloses a “[f]ive volt power supply 78 [that] can receive and transform electrical power from a wall-mounted receptacle to power circuit 50.” EX1040, 12:1-2 and Figs. 7-8. The 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. 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].

148. Motivation for this modification comes from the disclosure in Neufeld in EX1005, ¶[0052]. 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.

**B. Limitation [14.b] a monitoring means for monitoring the status of the network power supply;**

149. The combination of Neufeld and Fowler renders obvious this limitation. As discussed in Section III.E.5, 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, ¶¶167-168.



**C. Limitation [14.c] a reporting means for reporting the status of the network power supply.**

150. Neufeld and Fowler render obvious this limitation. As discussed in Section III.E.6, 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. 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.

151. 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.

152. 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.”

#### **VIII. GROUND 4: NEUFELD IN VIEW OF FOWLER RENDERS OBVIOUS CLAIM 13**

153. 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. In this regard, I note that monitoring the power supply for the remote management controller 116 constitutes monitoring the status of at least one computer network component).

154. 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.

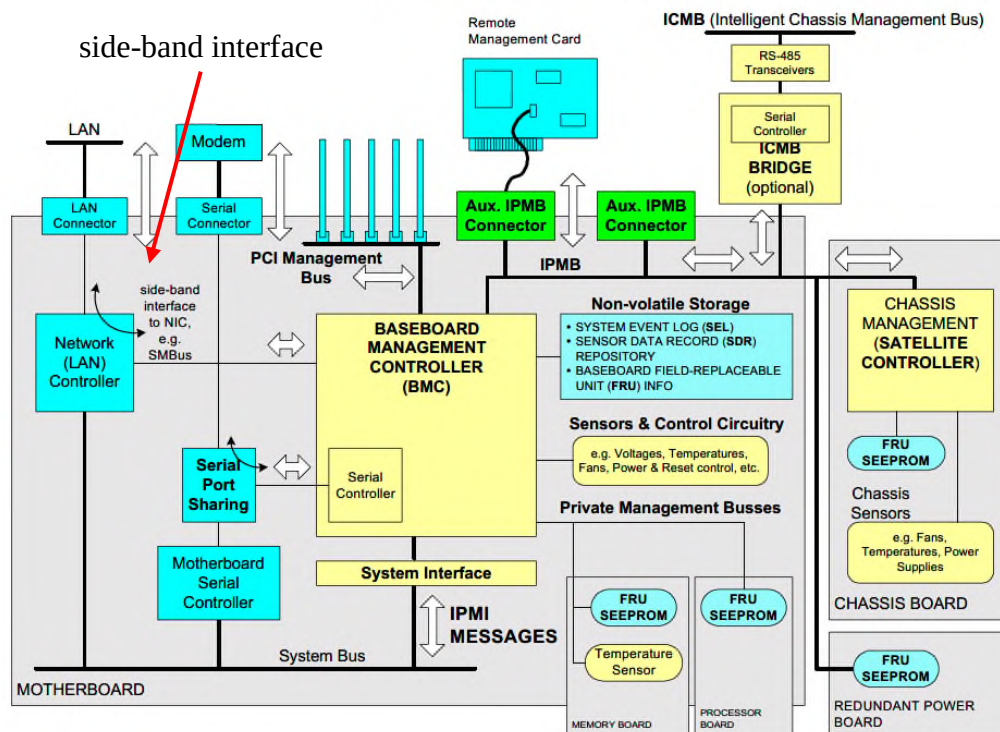
#### **IX. GROUND 5: IPMI IN COMBINATION WITH LAWRENCE RENDERS OBVIOUS CLAIMS 1-3, 6, 7, 10 AND 11**

##### **A. Introduction**

155. 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.

Figure 1-2, IPMI Block Diagram



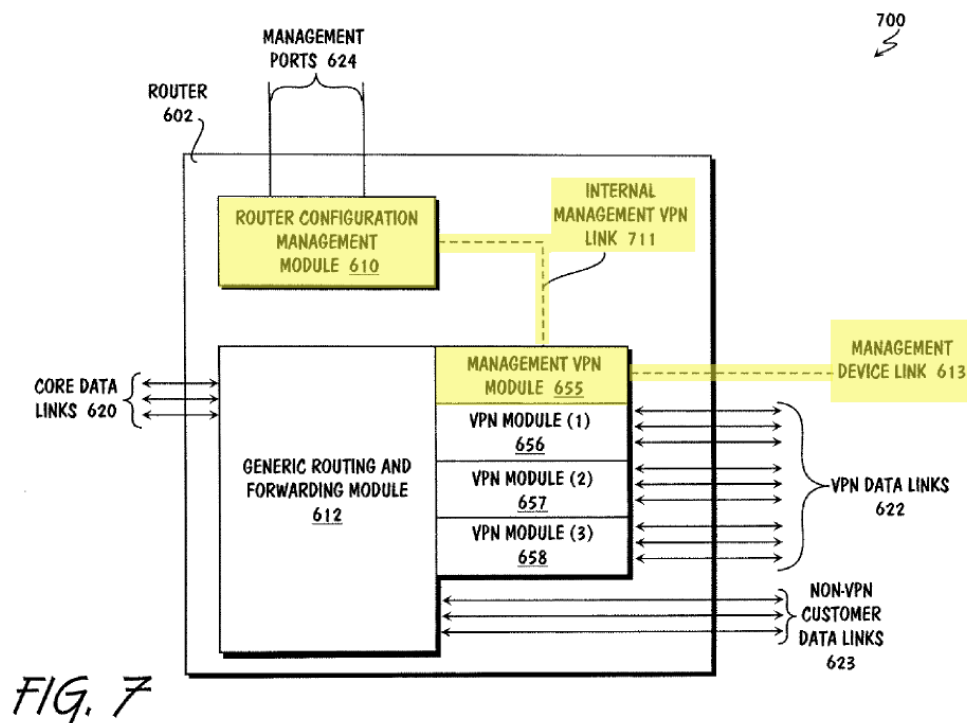
156. IPMI does not detail or limit how to implement the side-band interface for this in-band communication. A POSITA would therefore have looked to other sources for information as to how to implement IPMI's side-band interface.

157. 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.

158. 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):



EX1043, 5:37-47.

159. Lawrence further discloses that such dedicated management VPN modules 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.

160. 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).

161. 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 in order to avoid the security problems associated with communication of in-band information disclosed in Lawrence as discussed above (i.e., unauthorized entry of management commands and interception of management commands). 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

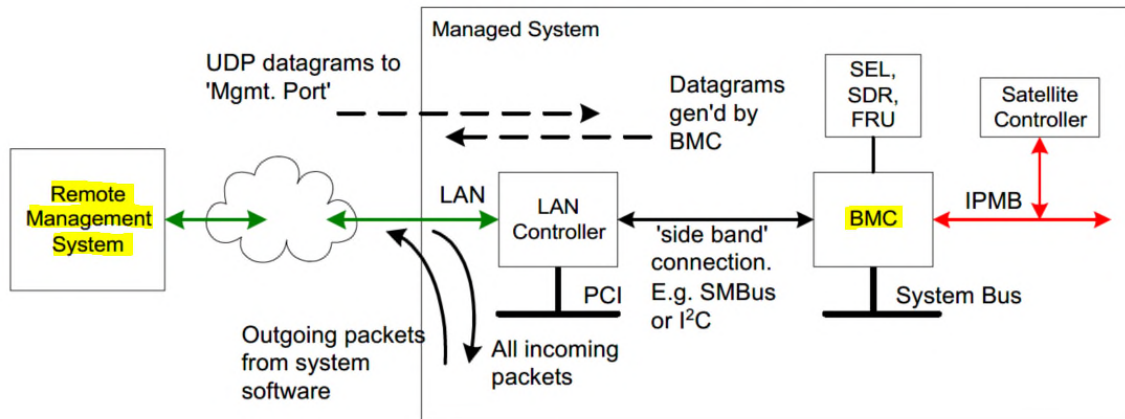
well-known at the time of the 140 patent. Additionally, software implementations of such VPN technology were available at that time.

**B. Claim 1**

- 1. Limitation [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.**

162. To the extent the preamble is limiting, IPMI discloses it. The claimed “remote device management communication system” is IPMI’s “managed system” in which the Baseboard Management Controller (BMC) resides and 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. 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 (with highlighting) below.

Figure 12-1, Embedded LAN Controller Implementation



163. 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 events 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.

164. IPMI discloses a System Event Log for logging such critical events, and also discloses sending alerts on the network, presenting a local pop-up messages, and shutting down an application. EX1020, 19 and 161. IPMI further discloses "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.

165. The claimed “distributed computer network” is IPMI’s managed system and the remote management system as well as gateways, routers and proxys 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. 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.

166. IPMI discloses “network services” including access functions. EX1020, 8. IPMI also discloses other “network services” such as Dynamic Host Configuration Protocol (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)).

167. 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 12-11 below (with highlighting). 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.

Figure 1-2, IPMI Block Diagram

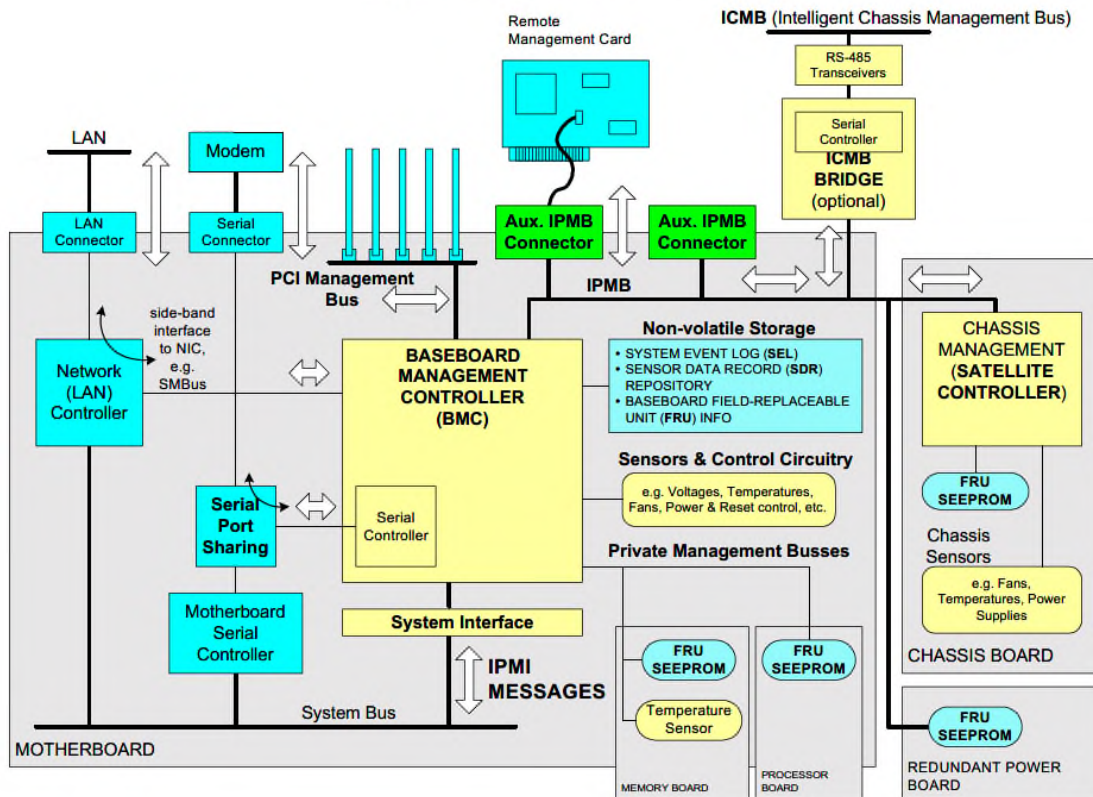
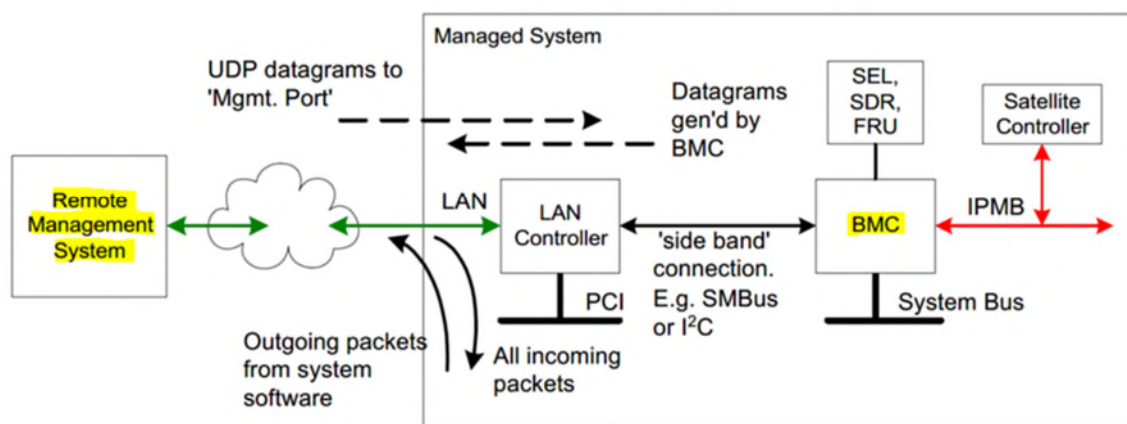


Figure 12-1, Embedded LAN Controller Implementation



**2. Limitation [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;**

168. As discussed above for limitation [1.pre], IPMI's BMC is the claimed "secure management access controller," and IPMI managed system is the claimed "managed network device." IPMI discloses that the BMC is connected in one embodiment to an I<sup>2</sup>C 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. 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 and Figs. 1-2, 12-1 and 12-2 (with highlighting). Any of these busses can be mapped to the claimed "one or more data bus of said managed network device" configured to send IPMI messages (the claimed "device management data").

Figure 1-2, IPMI Block Diagram

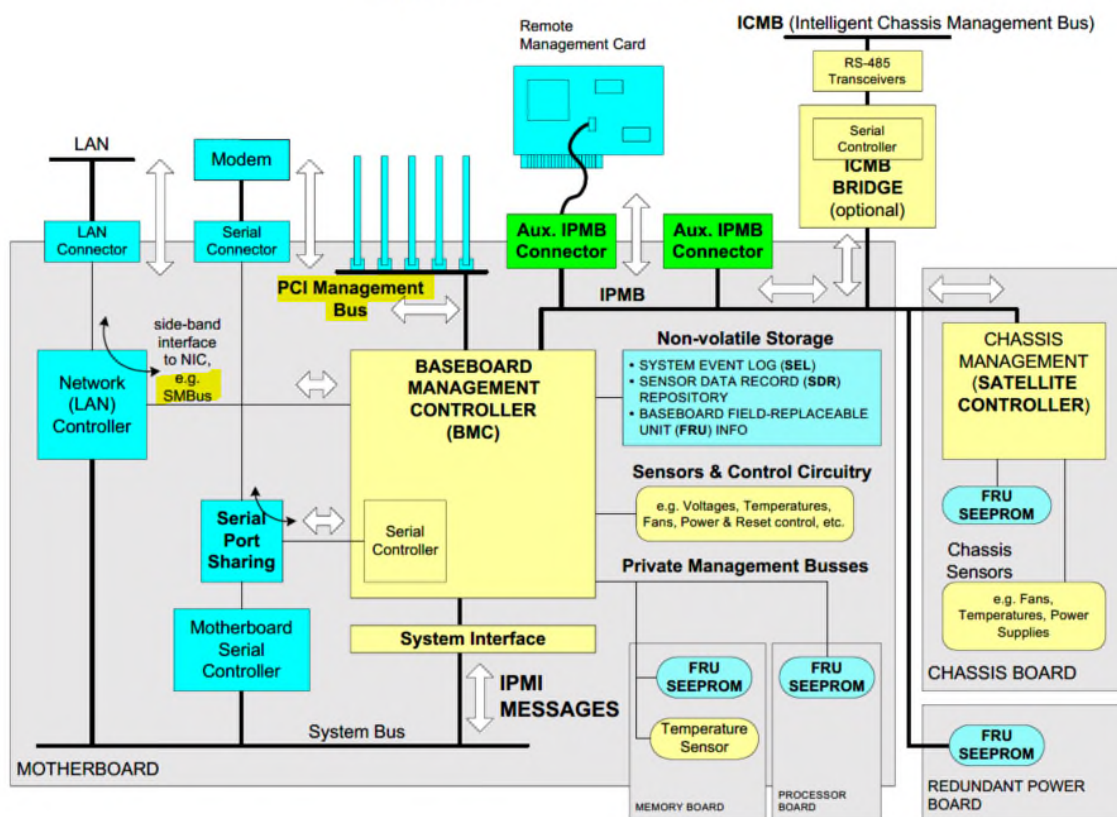
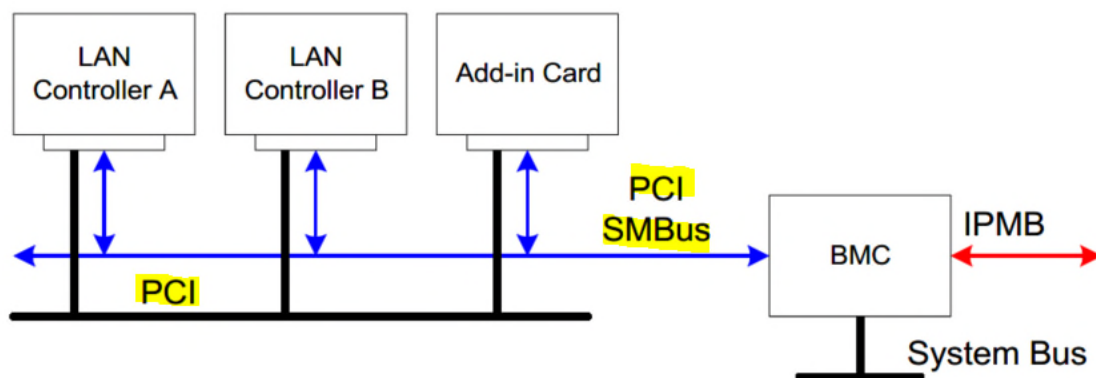


Figure 12-2, PCI Management Bus Implementation



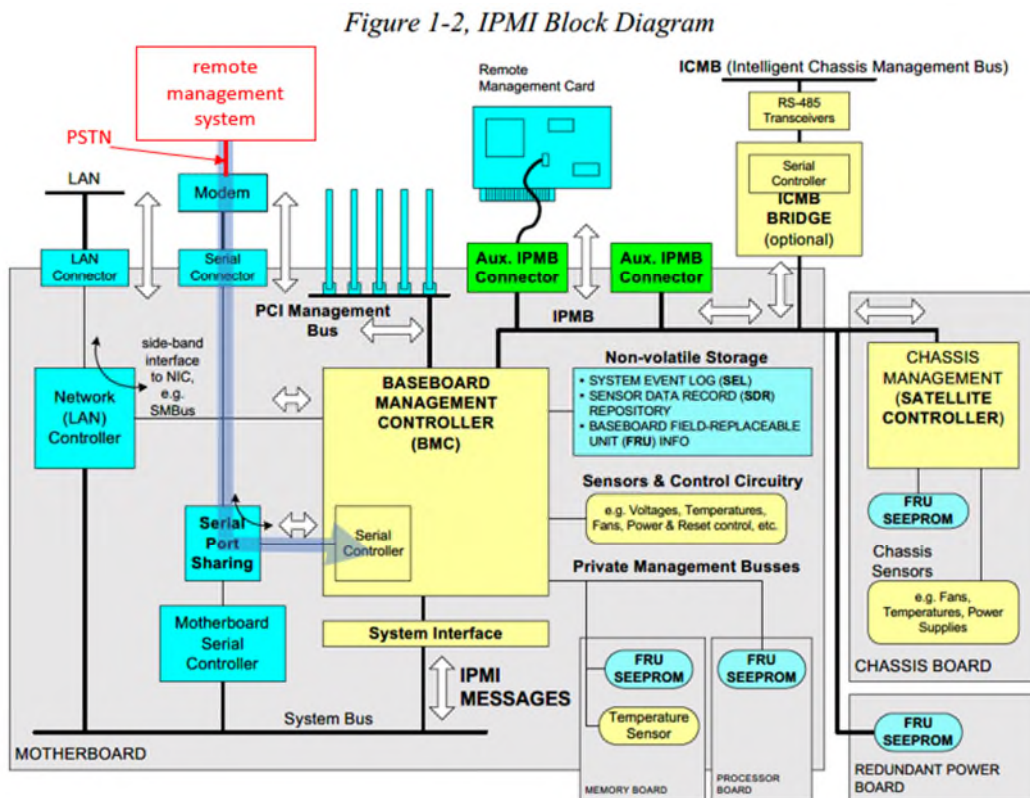
3. **Limitation [1.b] an out-of-band access connection means for connecting said one or more network services or remote**

**users with said secure management access controller for management of said network device;**

169. 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.

170. 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. EX1020, 7 and 122. As disclosed by IPMI, BMC uses command “strings” to configure the modem for out-of-band access use. 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.



171. 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. IPMI discloses that this feature is an option, and thus a POSITA would understand that IPMI also discloses a dedicated serial port used only by the BMC. *Id.*; EX1046, ¶180. Petitioner relies on an IPMI embodiment without that feature.

172. 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 and 122-123; *see also* 131 (disclosing details on how to use the modem for out-of-band management), 133 n.1 (discussing variations in national phone systems) and Table 15-4 at 174 (referring to destination phone numbers for use with serial/modem). Lawrence similarly discloses out-of-band communication of management information via a 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. EX1043, 5:9-15.

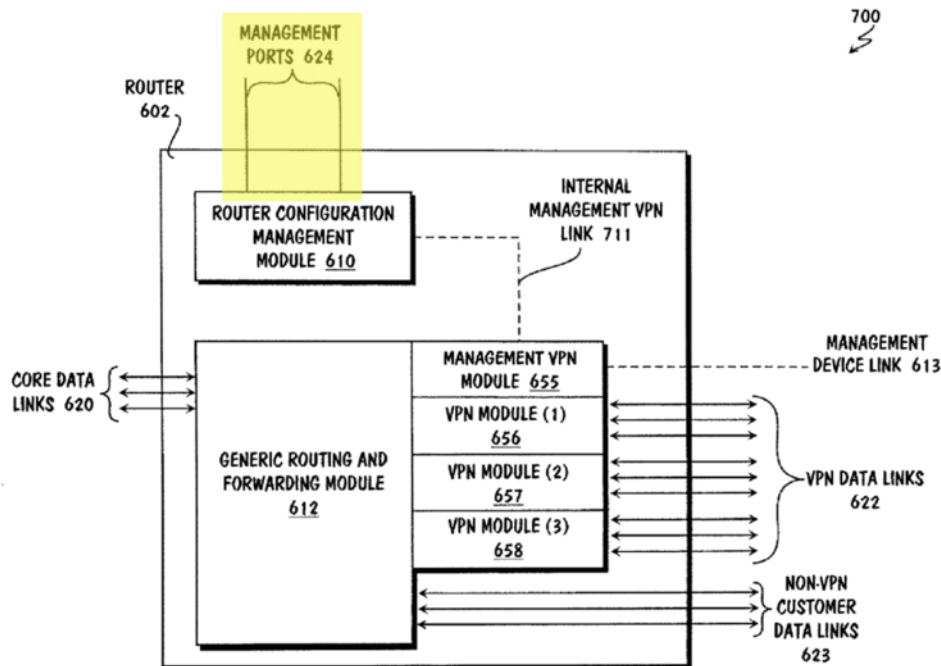


FIG. 7

173. 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.

4. **Limitation [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**

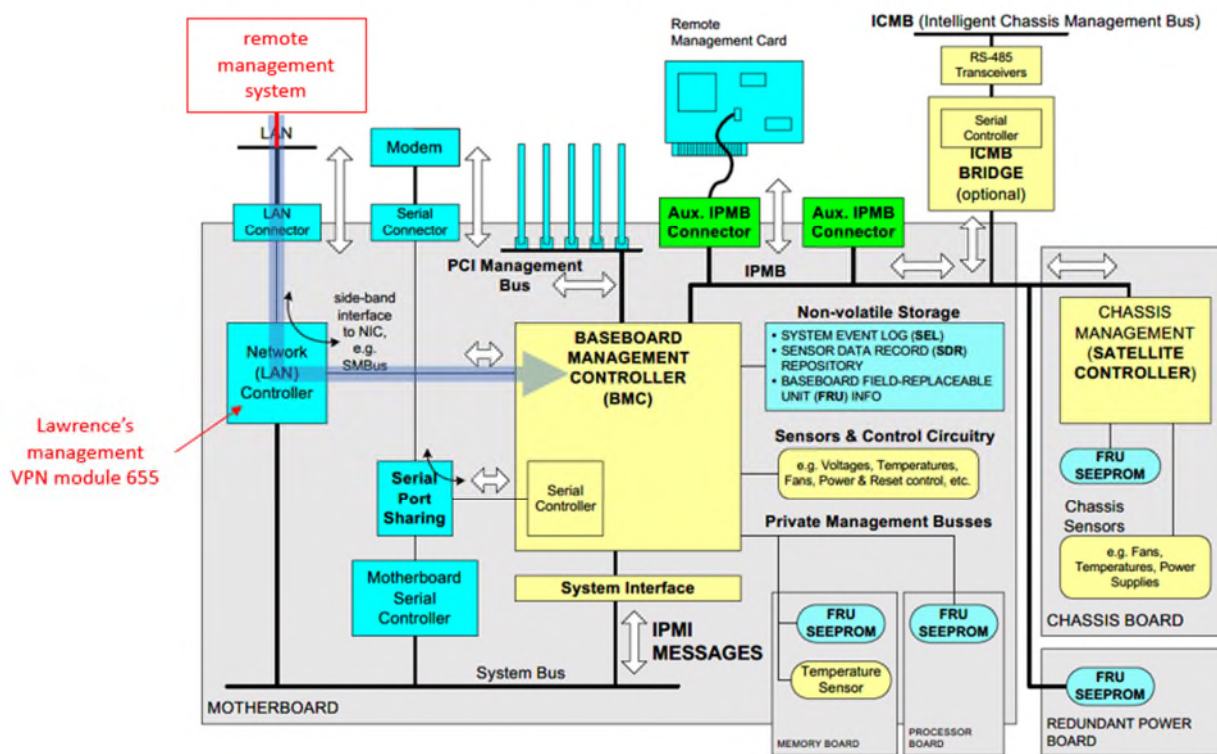
**said one or more network services or remote users with said secure management access controller.**

174. As discussed in Section III.E.4, 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.” As further discussed in Section III.E.4, the corresponding structure is a VPN.

175. In the combination of IPMI and Lawrence that I discuss in the Introduction above, 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, which corresponds 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. 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 (which

corresponds to Lawrence's configuration management module 610), which then directs those packets via Lawrence's Internal Management VPN link 711 to IPMI's BMC as indicated by the blue arrow shown in the annotated Figure 1-2 below.

Figure 1-2, IPMI Block Diagram

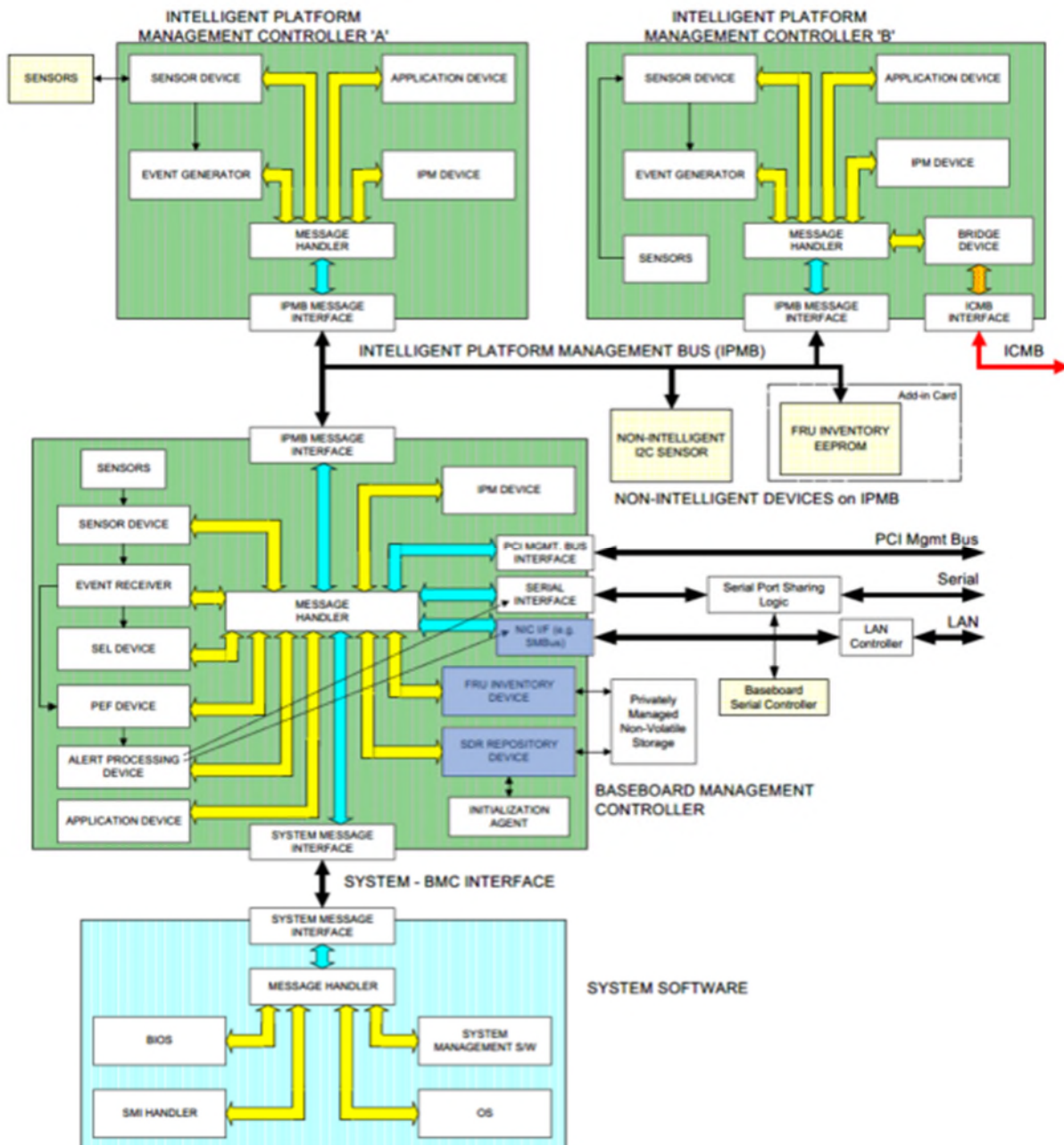


176. This implementation of IPMI's side-band interface using Lawrence's VPN technology is the identical structure for this limitation disclosed in the 140 patent, namely a VPN. Furthermore, the functions performed by these structures are identical – connecting remote users (e.g., on IPMI's remote management 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 to that LAN interface.

**C. Claim 2:**

177. IPMI renders obvious the limitations of this claim. IPMI discloses on-chip user 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.

Figure 2-1, Intelligent Platform Management Logical Devices



178. 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.

179. 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 in view of, e.g., EX1005, ¶[0055].

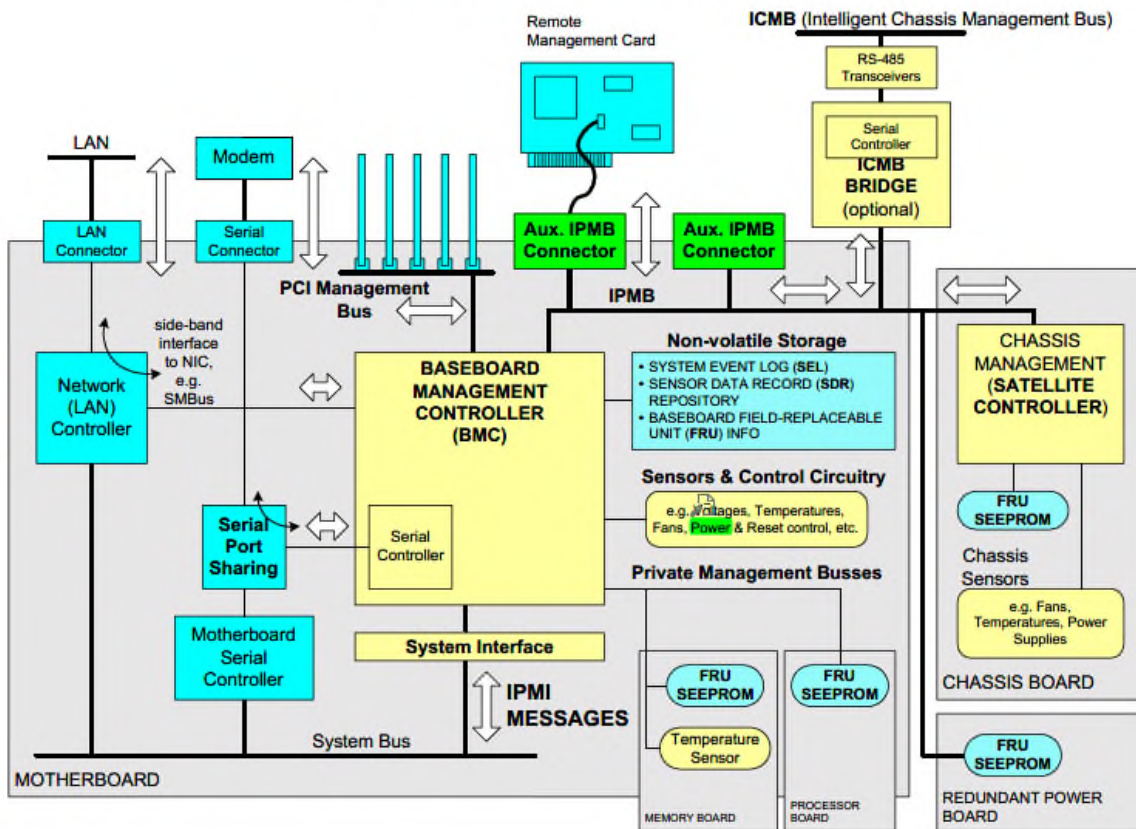
180. IPMI further discloses that the BMC must know the sensor and event type so it can place the information on the Event Message and for this purpose BMC includes a sensor data record (SDR, also highlighted in purple above) which provides platform management sensor information (type, location...etc.). Ex 1020, 5 and 11. A modal SDR Repository may be stored in a flash device that also holds BMC code. EX1020, 311. Accordingly, it would have been obvious to a POSITA that the BMC includes all three types of memory required by claim 2

**D. Claim 3:**

181. IPMI discloses the limitations of this claim. 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.

*Figure 1-2, IPMI Block Diagram*



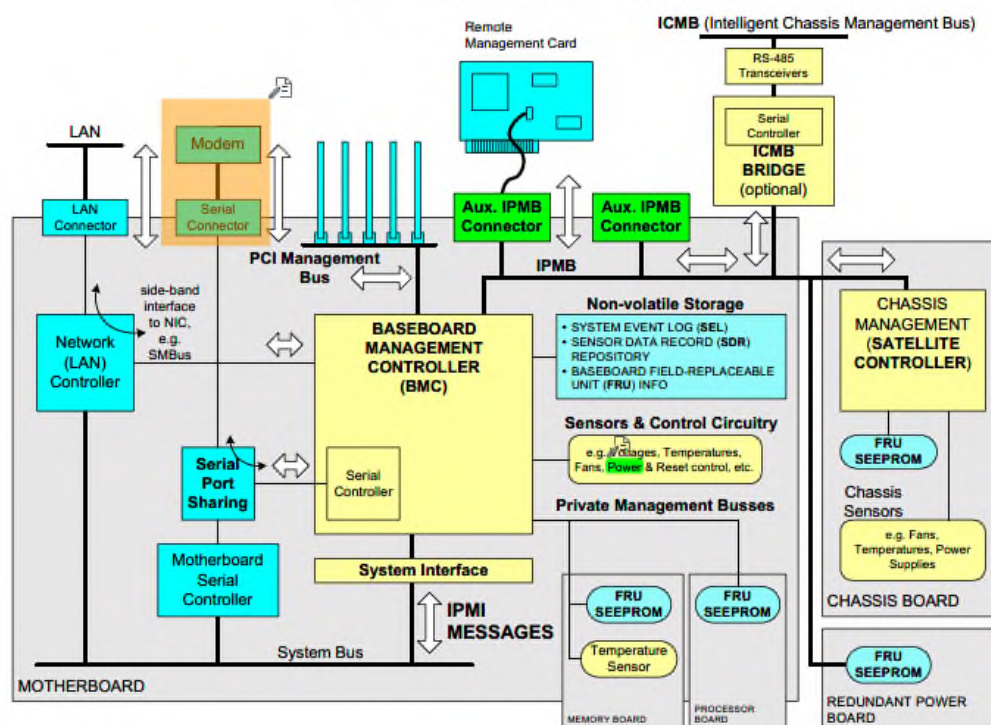
#### E. Claim 6:

182. IPMI discloses the limitations of this claim. 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 device such as IPMI’s “remote management system” that executes software referred to as a “remote console”

constitutes the claimed “communication system.” EX1020, 15 and 122-123; *see also* 131 (disclosing details on how to use the modem for out-of-band management), 133 n.1 (discussing variations in national phone systems) and Table 15-4 at 174 (referring to destination phone numbers for use with serial/modem).

183. The BMC manages the interface between system management software and platform management hardware. EX1020, 8. *See also* Figure 1-2 (orange highlighting added) below (showing serial/model interface).<sup>1</sup>

Figure 1-2, IPMI Block Diagram



<sup>1</sup> 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 or found obvious that the “Serial Connector” in Figure 1-2 would be connected directly to the BMC’s “Serial Controller.”

**F. Claim 7**

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

**G. Claim 10**

185. IPMI in combination with Lawrence renders obvious the limitations of this claim. 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. 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 in order 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.

## **H. Claim 11**

186. The combination of IPMI and Lawrence render obvious the limitations of this claim. 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 inclusion of 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.

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

187. Claim 1 (from which claim 4 depends) is obvious over the references cited above in Ground 4 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.

188. 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.

189. 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.*

190. Leedy’s VSI fabrication methods “enable the integration as one IC or die that are currently system assemblies of discrete 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.

191. 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.

192. 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.

193. 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.

194. As discussed above for Ground 5, claim 2 (incorporated herein by reference), 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.

195. 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.

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

196. 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 I stated there. Claims 11 and 12 are obvious over these references in combination with Syvanne for reasons similar to those I discussed above in Ground 2. Because IPMI's BMC can be reached in-band via a public network such as the Internet like Neufeld's remote management controller 116, and a POSITA would therefore have found it obvious to, and recognized the desirability of, further improving security by adding a locally executing firewall to IPMI's LAN controller in the BMC to protect management communications by removing unauthorized messages. 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.

197. With respect to claim 11, such a firewall performs the identical function identified in Section III.E.3, and is identical or at least equivalent to the firewall structure identified in Section III.E.3, for the "protection means" limitation. With respect to claim 12, above-discussed 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.

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

198. 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 and further in combination with Fowler.

199. As discussed above in Ground 3, Fowler discloses a network device having a regulated five volt power supply 78 connected to utility company 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.*

200. It would have been obvious to a POSITA to integrate Fowler's power supply 78, 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.

201. 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. 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.

202. I will discuss claim 14 first, and then claim 13.

**A. Claim 14**

**1. Limitation [14.a] The system of claim 1 further comprising:  
a network power supply;**

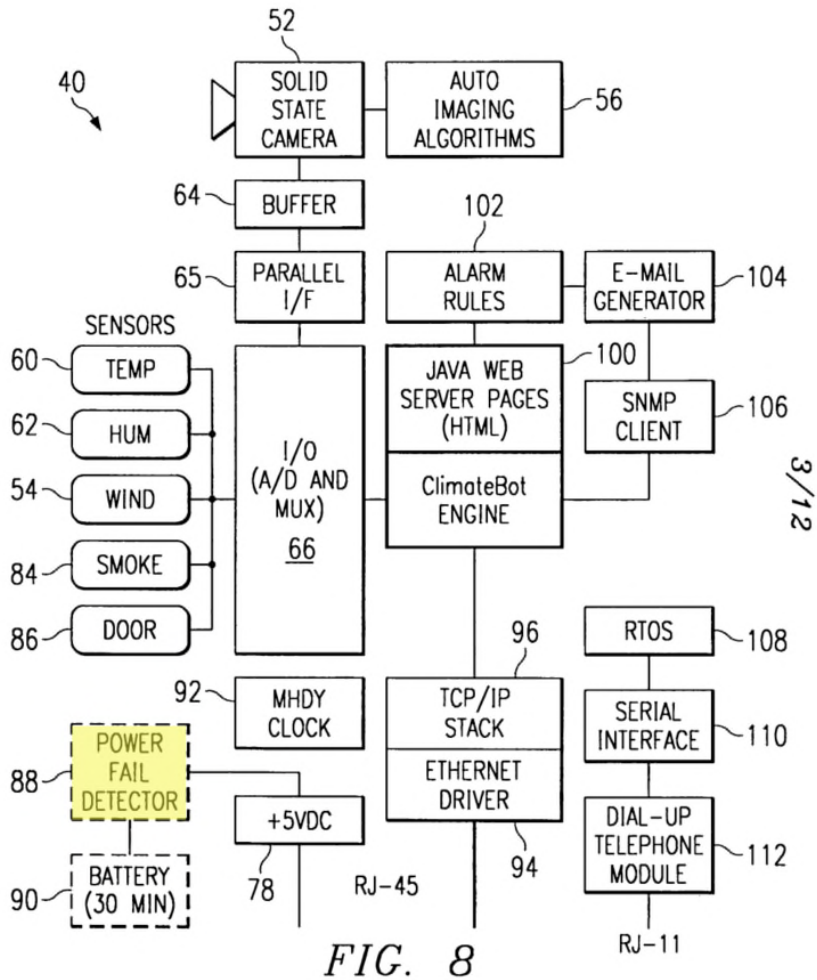
203. Fowler discloses a “[f]ive volt power supply 78 [that] can receive and transform electrical power from a wall-mounted receptacle to power circuit 50.”

EX1040, 12:1-2 and Figs. 7-8. The power supply 78 constitutes a network power supply as required by limitation [14.a].

204. 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, in order 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 utility company power to power supply 78 and switch the UPS to supply power to the BMC for the reasons discussed above.

**2. Limitation [14.b] a monitoring means for monitoring the status of the network power supply;**

205. The combination of IPMI, Lawrence and Fowler render obvious this limitation. As discussed in Section III.E.5, 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 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).



**3. Limitation [14.c] a reporting means for reporting the status of the network power supply.**

206. 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. 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.

**B. Claim 13**

207. 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 uninterruptable power supply 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. The power supply 78 for the BMC and managed platform constitutes monitoring the status of at least one computer network component.

208. 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.

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

**A. Claim 16**

209. 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.

210. 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. 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. 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.

# Appendix A

# CV and Research Statement

## SIGURD MELDAL

### CEO

Mostly Sunny  
413 Claremont Way  
Menlo Park, CA 94025  
Phone: +1.650.823.0653  
Email: Sigurd.Meldal@mostly-sunny.com

### EDUCATION

- Dr. Scient. in Informatics  
1986  
*University of Oslo*
- NATO Advanced Science Institute on Concepts of Distributed Programming, 1984  
*Marktoberdorf*
- Cand. Real. in Informatics 1982  
*University of Oslo*
- Cand. Mag., with Minor in Mathematics and Statistics 1979  
*University of Oslo*

### EXPERIENCE

- Vice Chair of Operations, Engineering Accreditation Commission (EAC) 2024 – present  
*ABET, Inc., Baltimore, MD*
- Commissioner, Engineering Accreditation Commission (EAC) 2016 – 2024  
*ABET, Inc., Baltimore, MD*
- CEO, Mostly Sunny 2012 – Present  
*Menlo Park, CA*
- Member, California Task Force on Cyber Security 2014 – 2016  
*State of California*
- Director, Silicon Valley Big Data and Cybersecurity Center 2013 – 2016  
*San José State University, San José, CA*
- Co-Director, NSF Center for Research in Ubiquitous Secure Technologies 2005 – 2016  
*University of California, Berkeley, CA*
- Professor of Computer Engineering, Software Engineering and Computer Science 2002 – 2020  
*Computer Engineering and Computer Science Departments, San José State University, San José, CA*
- Chair, Computer Engineering Department 2002 – 2013  
*San José State University, San José, CA*
- Chair, Academic Senate 2008 – 2009  
*San José State University, San José, CA*
- Chair, Computer Science Department 2000 – 2002  
*California Polytechnic State University, San Luis Obispo, CA*
- Professor of Computer Engineering and Computer Science 2000 – 2002  
*California Polytechnic State University, San Luis Obispo, CA*

- Associate Chair, Computer Science Department 1999 – 2000  
*California Polytechnic State University, San Luis Obispo, CA*
- Associate Professor, Computer Science Department 1997 – 2000  
*California Polytechnic State University, San Luis Obispo, CA*
- Professor (Consulting/Visiting), Electrical Engineering Department 1989 – 1998  
*Stanford University, Palo Alto, CA*
- Professor, Department of Informatics 1990 – 1998  
*University of Bergen, Bergen, Norway*
- Director, Computer Science Program 1997  
*College of Notre Dame, Belmont, CA*
- Department Chair, Department of Informatics 1993 – 1995  
*University of Bergen, Bergen, Norway*
- Associate Professor (Visiting), Electrical Engineering Department 1989  
*Stanford University, Palo Alto, CA*
- Førsteamanuensis, Department of Informatics 1987 – 1989  
*University of Bergen, Bergen, Norway*
- Fulbright Scholar 1986 – 1987  
*Stanford University, Palo Alto, CA*
- Universitetsstipendiat, Institute of Informatics 1983 – 1986  
*University of Oslo, Oslo, Norway*
- Researcher 1982  
*The Norwegian Computing Center, Oslo, Norway*

## LITIGATION CONSULTING

*International Trade Commission; USPTO Patent Trial and Appeal Board; US District Court for the Central District of California; US District Court for the Northern District of California; US District Court for the Southern District of California; US District Court for the District of Columbia; US District Court for the District of Delaware; US District Court for the Northern District of Illinois; US District Court for the District of Nevada; US District Court for the District of New Jersey; US District Court for the Southern District of New York; US District Court for the Eastern District of Texas; US District Court for the Northern District of Texas; US District Court for the Eastern District of Virginia; Superior Court of the State of California, County of Alameda; Superior Court of the State of California, County of Santa Clara; US Bankruptcy Court for the Southern District of Florida, West Palm Beach Division*

## HONORS AND AWARDS

- Certificate of Special Recognition from the U.S. House of Representatives 2000  
Award given in bipartisan recognition of innovative work in software engineering degree design, in particular the integration of industry partners with academic studies.
- Certificate of Recognition from the California State Assembly 2000  
Award given in partisan recognition of innovative work in software engineering degree design, in particular the integration of industry partners with academic studies.
- The Carl-Erik Fröberg Prize 1987

The Prize is given in odd numbered years to a young Nordic author of a distinguished paper published in the journal BIT.

- Fulbright-Hays Fellowship 1986

The Fulbright Program is one of the most prestigious awards programs worldwide, with a highly competitive, merit-based grant for international educational exchange for scholars and scientists. Fifty-three Fulbright alumni have won Nobel Prizes; seventy-eight have won Pulitzer Prizes. More Nobel laureates are former Fulbright recipients than any other award program.

#### RESEARCH GRANTS, CONTRACTS, AND AWARDS

- Hightail, Inc., Hightail QA Internship Program, \$452,805. 2013 – 2014
- Citrix Systems Silicon Valley, QA Internships, \$218,342. 2012 – 2014
- RingCube, QA Internships, \$940,000. 2007 – 2011
- National Science Foundation (NSF), Science and Technology Center, Team for Research in Ubiquitous Secure Technology (TRUST), \$963,746. 2005 – 2016
- National Science Foundation (NSF), Information Assurance Capacity Building Program (IACBP), \$356,000. 2006 – 2009
- Intel, Software Security Laboratory (co-PI), \$40,000. 2005
- Samsung Electronics, Software Engineering Internationalization, \$60,000. 2005
- GREEN Foundation, Fund for Excellence in Computer Software Engineering, \$500,000. 2000–2004
- CalPoly Plan, Retaining Females in Computer Science Education, \$15,000. 2000 – 2002
- CalPoly Plan, High Demand Courses - Computer Science, \$30,000. 2000 – 2002
- Private Donation, The Bonderson Advanced Software Design Studio, \$1,000,000. 2001
- Compaq, Computer Software Engineering Laboratory, \$35,000. 2001
- Compaq, Static Analysis Tools (requirements phase), \$20,000. 2000 – 2001
- Raytheon Systems, User Interface Frameworks for Command & Control, \$45,000. 1999 – 2000
- Raytheon Systems, JavaBeans, \$75,000. 2000
- Norges Forskningsråd (The Research Council of Norway), Architecture Independence in Software Design and Development, \$175,000. 1997 – 2000
- US Department of Education, Supporting Effective Educator Development (SEED) Grant Program, \$2,500,000. 1999
- Metrowerks, Integrated Development Environment, \$157,398. 1998

- Norges Forskningsråd, Biocomputing, \$150,000. 1996 – 1998
- Norges Forskningsråd, Internationalization, \$75,000. 1994 – 1997
- US Department of Defense/Office of Naval Research, Rapid Construction of Software Prototypes (with Stanford University Program Analysis and Verification Group), senior personnel, \$545,367. 1989 – 1996
- US Advanced Research Projects Agency (ARPA), Computer Aided Educational Technology (with Stanford University Program Analysis and Verification Group), senior personnel. Approx. \$600,000. 1989 – 1996
- European Strategic Program on Research in Information Technology (ESPRIT), COMPASS-II (co-PI with Universität Bremen and other European partners), \$408,000. 1993 – 1996
- Norges Forskningsråd, Genetic Structures, \$150,000. 1994 – 1996
- Norges Forskningsråd, Architecture Abstraction, \$75,000. 1993 – 1995
- Norges Allmenvitenskapelige Forskningsråd, Parallellitet – algoritmer, pålitelighet 1991 – 1993 og numeriske metoder, \$370,000.

## DISSERTATIONS

- Sigurd Meldal. "On Hierarchical Abstraction and Partial Correctness of Concurrent Structures." Ph.D. dissertation, Institute of Informatics, University of Oslo, June 1986.
- Sigurd Meldal. "CHAP — Et Forslag til Syntaks og Semantikk for Parallelle Prosesser." Master's thesis, Institute of Informatics, University of Oslo, June 1982. (In Norwegian.)

## BOOKS

- J. Homb, T.M. Jonassen, Sigurd Meldal, T. Rekdal, A. Schjalm. "Overlevelsesguide for Realfagstudenten." Realistaksjonens forlag, 1982. (In Norwegian.)

## EDITED PROCEEDINGS

- Proceedings of Norsk Informatikkonferanse (NIK '94). Edited with Magne Haveraaen, Bjørn Jæger, Siri Bjorvand, Randi Karlsen, Stein Krogdahl, Arne Maus, and Syvert Nørsett. Tapir forlag, November 1994.
- Proceedings of the 3<sup>rd</sup> Nordic Workshop on Program Correctness (NWPC). Edited with Magne Haveraaen. University of Bergen, November 1992.

## JOURNAL ARTICLES AND BOOK CHAPTERS

- Michal A. Walicki, Magne Haveraaen, and Sigurd Meldal. "Computation Algebras." In *Mathematical Structures in Computer Science*, vol. 11, no. 5. Cambridge University Press, October 2001.

- David C. Luckham, James Vera, and Sigurd Meldal. "Key Concepts in Architecture Definition Languages." In *Foundations of Component Based Systems*, pp. 23–46. Cambridge University Press, 2000.
- Sigurd Meldal, Gene L. Fisher, Daniel J. Stearns, and Peter C. Ölveczky. "Software Prototyping." In *Wiley Encyclopedia of Electrical and Electronics Engineering*. Wiley Online Library, 1999.
- Sigurd Meldal and David C. Luckham. "NSA's MISSI Reference Architecture – From Prose to Precise Specification." In *Requirements Targeting Software and Systems Engineering*, Lecture Notes in Computer Science (LNCS) 1526, pp. 293–329. Springer-Verlag, 1998.
- Sigurd Meldal and M. A. Walicki. "Singular and Plural Non-deterministic Parameters." In *SIAM Journal of Computing*, vol. 26, no. 4. Society for Industrial and Applied Mathematics, August 1997.
- Michal Walicki and Sigurd Meldal. "Algebraic Approaches to Non-Determinism – an Overview." In *ACM Computing Surveys*, vol. 29, no. 1, pp. 30–81. Association for Computing Machinery, March 1997.
- Sigurd Meldal and A. I. Vermesan. "Verification Oriented Development of Knowledge Based Systems." In *New Review of Applied Expert Systems*, vol. 2, pp. 91–104. 1996.
- Michal Walicki and Sigurd Meldal. "Multialgebras, Power Algebras and Complete Calculi of Identities and Inclusions." In *Recent Trends in Data Type Specification*, Lecture Notes in Computer Science (LNCS) 906, pp. 453–468. Springer-Verlag, March 1995.
- Michal Walicki and Sigurd Meldal. "A Complete Calculus for the Multialgebraic and Functional Semantics of Non-determinism." In *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 17, no. 2, pp. 366–393. Association for Computing Machinery, March 1995.
- John Mitchell, Sigurd Meldal, and Neel Madhav. "An Extension of Standard ML Modules with Subtyping and Inheritance." In *Information and Control*, vol. 71, pp. 95–130. 1991.
- Sigurd Meldal. "A Complete Axiomatic Semantics of Spawning." In *Distributed Computing 5*, pp. 159–174. Springer-Verlag, May 1991.
- Sigurd Meldal. "Fra Spesifikasjon til Virkelighet." In *DATA*, vol. 17, no. 4, pp. 42–45. 1987. (In Norwegian.)
- Sigurd Meldal. "Partial Correctness of Exits from Concurrent Structures." In *BIT Numerical Mathematics*, vol. 26, iss. 3, pp. 295–302. BIT Computer Science and Numerical Mathematics, September 1986.
- Sigurd Meldal. "An Axiomatic Semantics for Nested Concurrency." In *BIT Numerical Mathematics*, vol. 26, iss. 2, pp. 164–174. BIT Computer Science and Numerical Mathematics, April 1986.
- Sigurd Meldal and E. Mellbye-Larsen. "Styring av Bus- of Lageraksess i en Multiprosessorarkitektur." In *Trip Report from the Joint Scandinavian Computer Conference (NordDATA '83)*. Den Norske Dataforening, June 1983. (In Norwegian.)

## CONFERENCE PAPERS

- Sigurd Meldal. "Some Thoughts on Cyber Risk and the Science(s) of Security." Keynote address, IEEE International Symposium on Signals, Circuits and Systems, July 2013.
- Sigurd Meldal. "Breadth, Depth...and Predictable Weather. Components of the Success of Silicon Valley." Invited talk, Third International Exhibition and Forum of Industry and Innovations (INNOPROM), July 2011.
- Sigurd Meldal. "Security – a Science?" Invited Valedictorian address, IEEE 2<sup>nd</sup> International Advance Computing Conference (IACC), February 2010.
- Sigurd Meldal. "It's a Dangerous World Out There – The Interplay of Security, Safety and Policy." Keynote address, IEEE International Advance Computing Conference (IACC), March 2009.

- Sigurd Meldal, Kristen Gates, Russell Smith, and Xiao Su. "Security, Safety and Privacy – Pervasive Themes for Engineering Education." In *Proceedings of the International Conference on Engineering Education (ICEE)*, March 2008.
- Daniel Manson, Sigurd Meldal, Carol Sledge, Stephen M. Maurer, John C. Mitchell, Erich Spengler, Janos Sztipanovits, and Javier Torner. "Learning Modules for Security, Privacy and Information Assurance in Undergraduate Engineering Education." In *Proceedings of the 36<sup>th</sup> Annual Frontiers in Education Conference (FIE)*, October 2006.
- Jerry Gao, Yumei Wu, Lee Chang, and Sigurd Meldal. "Measuring Component-Based Systems Using a Systematic Approach and Environment." In *Proceedings of the Second IEEE International Symposium on Service-Oriented System Engineering (SOSE)*, October 2006.
- Daniel J. Stearns, C. S. Turner, and Sigurd Meldal. "Ten Pounds in a Five-Pound Sack: Providing Software Engineering Students with Management Experience." In *Proceedings of the International Conference on Engineering Education (ICEE)*, August 2001.
- Michal Walicki and Sigurd Meldal. "Nondeterminism vs. Underspecification." In *Proceedings of The Fifth World Multi-Conference on Systemics, Cybernetics and Informatics (SCI/ISAS)*, July 2001.
- Michal Walicki, Adis Hodzic, and Sigurd Meldal. "Compositional Homomorphisms of Relational Structures." In *Proceedings of the 13<sup>th</sup> International Symposium on Fundamentals of Computation Theory*, August 2001.
- David C. Luckham and Sigurd Meldal. "Causal Event-Relations as a Basis for Analyzing Distributed Architectures." In *Proceedings of the 8th International Colloquium on Computer Science with Applications*, August 1999.
- Peter C. Ölveczky and Sigurd Meldal. "Specification and Prototyping of Network Protocols in Rewriting Logic." In *Proceedings of Norsk Informatikkonferanse (NIK '98)*, November 1998.
- Sigurd Meldal. "Reference Architectures and Conformance." In *Proceedings of the International Workshop on Requirements Targeting Software and Systems Engineering (RTSE)*, April 1998.
- Valentinas Kriauciukas, Michal A. Walicki, and Sigurd Meldal. "Nondeterministic Algebraic Specifications in a Relational Syntax." In *Proceedings of the Nordic Workshop on Programming Theory (NWPT)*, November 1995.
- Anca Vermesan and Sigurd Meldal. "An Algebraic Approach to Refinement of KBS Specifications." In *Proceedings of the European Symposium on the Validation and Verification of Knowledge-Based Systems (EUROVAV)*, June 1995.
- Michal A. Walicki and Sigurd Meldal. "Generated Models and the  $\omega$ -Rule: The Nondeterministic Case." In *Proceedings of the Sixth International Joint Conference on Theory and Practice of Software Development (TAPSOFT)*, May 1995.
- Aida Pliuskeviciene, Regimantas Pliuskevicius, Michal Walicki, and Sigurd Meldal. "On Specialization of Derivations in Axiomatic Equality Theories." In *Proceedings of the Symposium on Logical Foundations of Computer Science (LFCS)*, July 1994.
- Dinesh Katiyar, David Luckham, John Mitchell, and Sigurd Meldal. "Polymorphism and Subtyping in Interfaces." In *Proceedings of the Workshop on Interface Definition Languages*, January 1994.
- P.O. Tvette and Sigurd Meldal. "Causality Breakdown at  $\omega$ ." In *Proceedings of the Nordic Workshop on Programming Theory (NWPT)*, October 1994.
- Michal Walicki and Sigurd Meldal. "Initiality + Nondeterminism  $\Rightarrow$  Junk." In *Proceedings of Norsk Informatikkonferanse (NIK '93)*, November 1993.

- Michal Walicki and Sigurd Meldal. "Sets and Nondeterminism." In *Proceedings of the Tenth International Conference on Logic Programming (ICLP) Workshop on Logic Programming with Sets*, June 1993.
- Michal Walicki and Sigurd Meldal. "Computations: A Deterministic Semantics of Nondeterminism." In *Proceedings of the 3<sup>rd</sup> Nordic Workshop on Program Correctness (NWPC)*, November 1992.
- John Mitchell, Dinesh Katiyar, David C. Luckham, Neel Madhav, Sigurd Meldal, and Sriram Sankar. "Subtyping, Assignment and Cloning in a Concurrent Object-Oriented Language." In *Proceedings of the DARPA Software Technology Conference*, April 1992.
- Michal Walicki and Sigurd Meldal. "Towards an Equational Theory of Nondeterminism." In *Proceedings of Norsk Informatikkonferanse (NIK '91)*, November 1991.
- Sigurd Meldal, Sriram Sankar, and James Vera. "Exploiting Locality in Maintaining Potential Causality." In *Proceedings of the 10<sup>th</sup> ACM Symposium on the Principles of Distributed Computing (PODC)*, August 1991.
- Neel Madhav and Sigurd Meldal. "An Object-Oriented Approach to Formal Specification of Reactive Systems." In *Proceedings of the 11<sup>th</sup> International Conference on Distributed Computing Systems (ICDCS)*, May 1991.
- John C. Mitchell, Neel Madhav, and Sigurd Meldal. "An Extension of Standard ML Modules with Subtyping and Inheritance." In *Proceedings of the 18<sup>th</sup> ACM Symposium on the Principles of Programming Languages (POPL)*, January 1991.
- Sigurd Meldal. "Supporting Architecture Mappings in Concurrent Systems Design." In *Proceedings of the 1990 Australian Software Engineering Conference (ASWEC '90)*, May 1990.
- David C. Luckham and Sigurd Meldal. "Specifying and Observing Concurrent Programs." In *Proceedings of the 3<sup>rd</sup> Workshop on Large Grain Parallelism*, October 1989.
- Sigurd Meldal. "An Abstract Axiomatization of Pointer Types." In *Proceedings of the 22<sup>nd</sup> Annual Hawaii International Conference on System Sciences (HICSS)*, January 1989.
- Sigurd Meldal, David C. Luckham, and Michael A. Haberler. "Specifying Ada Tasking Using Patterns of Behavior." In *Proceedings of the 21<sup>st</sup> Annual Hawaii International Conference on System Sciences (HICSS)*, January 1988.
- Sigurd Meldal. "Redundancy in Software Design." In *Proceedings of Norsk Informatikkonferanse (NIK '88)*, November 1988.
- Sigurd Meldal. "Har Formelle Metoder Noen Plass i Programutvikling?" In *Trip Report from the Joint Scandinavian Computer Conference (NordDATA '87)*, June 1987. (In Norwegian.)
- David C. Luckham, David P. Helmbold, Sigurd Meldal, D.L. Bryan, and Michael A. Haberler. "Task Sequencing Language for Specifying Distributed Ada Systems." In *System Development and Ada, Proceedings of the CRAI Workshop on Software Factories and Ada*, 1987.