

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

IPR2024-00109
U.S. Patent No. 8,474,016

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
I. INTRODUCTION	1
A. Background and Qualification	1
B. Information Considered	7
II. LEGAL STANDARDS	7
A. Legal Standards for Prior Art.....	7
B. Legal Standards for Obviousness.....	8
III. OVERVIEW OF THE ‘016 PATENT.....	13
A. Summary of the ‘016 Patent	13
B. The ‘016 Patent Prosecution History	14
C. Priority Date of the 016 Patent.....	16
D. Person of Ordinary Skill in the Art	16
E. Claim Construction Under 37 C.F.R. § 42.104(b)(3)	17
1. “the processor” (as used in the term “controlling, by the processor, one or more functions of the network device according to the management re-quests”) (claim 12)	17
IV. PRIOR ART REFERENCES.....	18
B. Patents	18
C. Patent Publications.....	18
D. Non-Patent Publications.....	18
V. GROUND 1: NEUFELD RENDERS OBVIOUS CLAIMS 1-3, 6, 9, 12 AND 17	21
A. Claim 1.....	24
1. [1.pre] 1. An apparatus, comprising:	24
2. [1.a] a processor configured to control one or more functions of a network device having a network interface, ...	25
3. [1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, ...	26
4. [1.c] wherein the management requests are received from a remote administrator;	30
5. [1.d] a first bus; and	30

6.	[1.e] a bus controller coupled to the processor via the first bus;	31
7.	[1.f] wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus	32
8.	[1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, ...	33
9.	[1.h] and to convey the encrypted form of the management requests to the processor via the first bus;	34
10.	[1.i] wherein the processor is configured to decrypt the encrypted form of the management requests	35
11.	[1.j] wherein the network device includes a processor configured to facilitate operation of the network device, and	36
12.	[i.k] wherein the processor of the apparatus is distinct from the processor included in the network device.	36
B.	Claim 2. The apparatus of claim 1, wherein the apparatus is configured to provide a command line interface to the remote administrator, and wherein the apparatus is configured to receive one or more commands to control the one or more functions of the network device.	37
C.	Claim 3. The apparatus of claim 1, wherein the bus controller is a peripheral component interconnect (PCI) controller.	38
D.	Claim 6. The apparatus of claim 1, wherein the processor is configured to establish a first virtual private network connection with the remote administrator, and wherein the processor is configured to receive the management requests via the first established connection.	39
E.	Claim 9. The apparatus of claim 1, wherein the apparatus is a component within the network device.	40
F.	Claim 12.....	40
1.	[12.pre] A method, comprising:.....	40
2.	[12.a] receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface	41
3.	[12.b] wherein the network device received the encrypted form of the management requests and data requests via the network interface,.....	41
4.	[12.c] wherein the management requests are from a remote administrator;	41
5.	[12.d] conveying the encrypted form of management requests from the bus controller to a processor of management device via a second bus of the management device,.....	41

6.	[12.e] wherein the network device includes a processor con-figured to facilitate operation of the network device, and.....	41
7.	[12.f] wherein the processor of the management device is distinct from the processor included in the network device;	42
8.	[12.g] decrypting, by the processor, the encrypted form of the management requests; and	42
9.	[12.h] controlling, by the processor, one or more functions of the network device according to the management re-quests.	42
G.	Claim 17. The method of claim 12, further comprising: receiving, by the management device, additional management requests from the remote administrator via a network interface of the management device, and wherein the additional management requests are not received via the first bus of the network device.	43
VI.	GROUND 2: NEUFELD IN COMBINATION WITH FRANTZ AND HUCKINS AND/OR PCI BRIDGE SPEC RENDERS OBVIOUS CLAIMS 1-3, 6, 9, 12 AND 17	43
A.	Introduction.....	43
B.	Claim 1.....	47
1.	[1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, ...	47
2.	[1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, ...	49
3.	[1.h] and to convey the encrypted form of the management requests to the processor via the first bus;	50
4.	[1.i] wherein the processor is configured to decrypt the encrypted form of the management requests	50
C.	Claim 12.....	52
VII.	GROUND 3: NEUFELD IN COMBINATION WITH MARTENSON AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC AND MARTENSON RENDERS OBVIOUS CLAIM 2.....	52
VIII.	GROUND 4: NEUFELD IN COMBINATION WITH MACWILLIAMS AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC AND MACWILLIAMS RENDERS OBVIOUS CLAIM 3.....	53
IX.	GROUND 5: NEUFELD, ROSSMAN AND RFC1492, OR NEUFELD, FRANTZ, PCI BRIDGE SPEC, ROSSMAN AND RFC1492, RENDER OBVIOUS CLAIMS 7 AND 16.....	55

A.	Claim 7. The apparatus of claim 6, wherein the processor is configured to establish a second virtual private network connection with an access control server configured to authenticate the remote administrator, and wherein the processor is configured to receive, via the second established connection, an indication of whether the remote administrator is authorized to administer the network device.	55
B.	Claim 16. The method of claim 12, further comprising: establishing, by the management device, a virtual private network connection with an access control server configured to authenticate the remote administrator	55
X.	GROUND 6: NEUFELD IN COMBINATION WITH SYVANNE AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC, AND SYVANNE RENDER OBVIOUS CLAIM 8.....	56
A.	Claim 8. The apparatus of claim 1, wherein the apparatus is configured to implement a firewall that restricts traffic received from the second bus.	56
XI.	GROUND 7: NEUFELD IN COMBINATION WITH NTP AAPA HRASTAR AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC, NTP AAPA AND HRASTAR RENDER OBVIOUS CLAIM 14	58
A.	Claim 14. The method of claim 12, wherein the one or more functions are associated with a network time protocol.....	58
XII.	GROUND 8: NEUFELD IN COMBINATION WITH RFC1157 AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC AND RFC1157 RENDER OBVIOUS CLAIM 15	60
A.	Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.	60
XIII.	GROUND 9: IPMI IN COMBINATION WITH FRANTZ AND HUCKINS RENDERS OBVIOUS CLAIMS 1-3, 9, 12, 15 AND 17	61
A.	Claim 1.....	63
1.	[1.pre] An apparatus, comprising:	63
2.	[1.a] a processor configured to control one or more functions of a network device having a network interface, ...	63
3.	[1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, ...	65
4.	[1.c] wherein the management requests are received from a remote administrator;	69
5.	[1.d] a first bus; and	69
6.	[1.e] a bus controller coupled to the processor via the first bus;	70
7.	[1.f] wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus	74

8.	[1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, ...	74
9.	[1.h] and to convey the encrypted form of the management requests to the processor via the first bus;	75
10.	[1.i] wherein the processor is configured to decrypt the encrypted form of the management requests	75
11.	[1.j] wherein the network device includes a processor configured to facilitate operation of the network device, and	76
12.	[1.k] wherein the processor of the apparatus is distinct from the processor included in the network device.	76
B.	Claim 2. The apparatus of claim 1, wherein the apparatus is configured to provide a command line interface to the remote administrator, and wherein the apparatus is configured to receive one or more commands to control the one or more functions of the network device.	76
C.	Claim 3. The apparatus of claim 1, wherein the bus controller is a peripheral component interconnect (PCI) controller.	78
D.	Claim 9. The apparatus of claim 1, wherein the apparatus is a component within the network device.	79
E.	Claim 12.....	81
1.	[12.pre] A method, comprising:.....	81
2.	[12.a] receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface	81
3.	[12.b] wherein the network device received the encrypted form of the management requests and data requests via the network interface,.....	81
4.	[12.c] wherein the management requests are from a remote administrator;	81
5.	[12.d] conveying the encrypted form of management requests from the bus controller to a processor of management device via a second bus of the management device,.....	81
6.	[12.e] wherein the network device includes a processor configured to facilitate operation of the network device, and	82
7.	[12.f] wherein the processor of the management device is distinct from the processor included in the network device;	82
8.	[12.g] decrypting, by the processor, the encrypted form of the management requests; and	82
9.	[12.h] controlling, by the processor, one or more functions of the network device according to the management re-quests.	82

F.	Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.	83
G.	Claim 17. The method of claim 12, further comprising: receiving, by the management device, additional management requests from the remote administrator via a network interface of the management device, and wherein the additional management requests are not received via the first bus of the network device.	84
XIV.	GROUND 10: IPMI IN COMBINATION WITH IPMIV2.0 AND HUCKINS RENDERS OBVIOUS CLAIMS 1-3, 9, 12, 15 AND 17	86
A.	Introduction.....	86
B.	Claim 1.....	87
1.	Limitations [1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface, [1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus, [1.h] and to convey the encrypted form of the management requests to the processor via the first bus;.....	87
2.	Limitation [1.i] wherein the network device includes a processor configured to facilitate operation of the network device	88
C.	Claim 12 A method, comprising: [12.a] receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface [12.b] wherein the network device received the encrypted form of the management requests and data requests via the network interface, [12.c] wherein the management requests are from a remote administrator; [12.d] conveying the encrypted form of management requests from the bus controller to a processor of management device via a second bus of the management device, [12.e] wherein the network device includes a processor configured to facilitate operation of the network device, and [12.f] wherein the processor of the management device is distinct from the processor included in the network device; [12.g] decrypting, by the processor, the encrypted form of the management requests; and [12.h] controlling, by the processor, one or more functions of the network device according to the management re-quests.....	88
D.	Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.	89
E.	Claim 17. The method of claim 12, further comprising: receiving, by the management device, additional management requests from the remote administrator via a network interface of the management device, and wherein the additional management requests are not received via the first bus of the network device.	89

XV.	GROUND 11: IPMI IN COMBINATION WITH FRANTZ, HUCKINS, AND VPN AAPA OR ROSSMAN AND/OR IPMI IN COMBINATION WITH IPMIV2.0, HUCKINS, AND VPN AAPA OR ROSSMAN RENDER OBVIOUS CLAIM 6.....	89
A.	Claim 6. The apparatus of claim 1, wherein the processor is configured to establish a first virtual private network connection with the remote administrator, and wherein the processor is configured to receive the management requests via the first established connection.	90
XVI.	GROUND 12: CLAIMS 7 AND 16.....	91
XVII.	GROUND 13: IPMI IN COMBINATION WITH FRANTZ, HUCKINS, AND SYVANNE AND/OR IPMI IN COMBINATION WITH IPMIV2.0, HUCKINS AND SYVANNE.....	92
A.	Claim 8. The apparatus of claim 1, wherein the apparatus is configured to implement a firewall that restricts traffic received from the second bus.	92
XVIII.	GROUND 14: IPMI IN COMBINATION WITH FRANTZ, HUCKINS, NTP AAPA AND HRASTAR AND/OR IPMI IN COMBINATION WITH IPMIV2.0, HUCKINS, NTP AAPA AND HRASTAR RENDER OBVIOUS CLAIM 14	92
A.	Claim 14. The method of claim 12, wherein the one or more functions are associated with a network time protocol.....	93
XIX.	GROUND 15: IMPI IN COMBINATION WITH FRANTZ, HUCKINS, AND RFC1157 OR RFC3414 AND/OR IMPI IN COMBINATION WITH IPMIV2.0, HUCKINS, AND RFC1157 RENDER OBVIOUS CLAIM 15.....	94
A.	Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.	94

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
1004	File History for U.S. Pat. App. No. 11/946,976
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 I ² C-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 (5 th 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	Reserved
1026	Reserved
1027	U.S. Patent No. 6,286,074

Exhibit No.	Description
1028	U.S. Patent No. 6,973,517
1029	U.S. Patent No. 6,189,096
1030	U.S. Patent No. 7,469,298
1031	U.S. Patent No. 6,272,537
1032	IETF Bibtex listing for RFC 3414
1033	IETF Bibtex listing for RFC 1157
1034	IETF Bibtex listing for RFC 2865
1035	IETF Bibtex listing for RFC 1492
1036	U.S. Patent No. 7,496,950
1037	“DSP0114 Alert Standard Format (ASF) Specification (“DSP0114”)
1038	U.S. Patent No. 7,263,716
1039	Declaration of Nathaniel E. Frank-White
1040	Reserved
1041	Reserved
1042	District Court Claim Construction Order Dated 5/28/24

CLAIMS
[1pre] An apparatus, comprising:
[1.a] a processor configured to control one or more functions of a network device having a network interface,
[1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface,
[1.c] wherein the management requests are from a remote administrator;
[1.d] a first bus; and
[1.e] a bus controller coupled to the processor via the first bus,
[1.f] wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus,
[1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus,
[1.h] and to convey the encrypted form of the management requests to the processor via the first bus;
[1.i] wherein the processor is configured to decrypt the encrypted form of the management requests,
[1.j] wherein the network device includes a processor configured to facilitate operation of the network device, and
[1.k] wherein the processor of the apparatus is distinct from the processor included in the network device.
[2.] The apparatus of claim 1, wherein the apparatus is configured to provide a command line interface to the remote administrator, and wherein the apparatus is configured to receive one or more commands to control the one or more functions of the network device.
[3.] The apparatus of claim 1, wherein the bus controller is a peripheral component interconnect (PCI) controller.
[4.] The apparatus of claim 1, wherein the apparatus is configured to receive power via a first power circuit, wherein the network device is configured to receive power via a second power circuit, and wherein the apparatus is configured to cycle the power received by the network device via the second power circuit.

CLAIMS
[5pre] The apparatus of claim 4, wherein the apparatus is configured to:
[5.a] determine whether the network device is receiving power via the second power circuit; and
[5.b] provide an indication, to the remote administrator, when the network device is not receiving power via the second power circuit.
[6.] The apparatus of claim 1, wherein the processor is configured to establish a first virtual private network connection with the remote administrator, and wherein the processor is configured to receive the management requests via the first established connection.
[7.] The apparatus of claim 6, wherein the processor is configured to establish a second virtual private network connection with an access control server configured to authenticate the remote administrator, and wherein the processor is configured to receive, via the second established connection, an indication of whether the remote administrator is authorized to administer the network device.
[8.] The apparatus of claim 1, wherein the apparatus is configured to implement a firewall that restricts traffic received from the second bus.
[9.] The apparatus of claim 1, wherein the apparatus is a component within the network device.
[10.] The apparatus of claim 1, wherein the apparatus is a card configured to be inserted into the network device via a card interface.
[11.] The apparatus of claim 1, wherein the network device is a network router that includes a plurality of network interfaces, and wherein the processor is dedicated to controlling one or more functions of the network router.
[12pre] A method, comprising:
[12.a] receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface,
[12.b] wherein the network device received the encrypted form of the management requests and data requests via the network interface,
[12.c] wherein the management requests are from a remote administrator;
[12.d] conveying the encrypted form of management requests from the bus controller to a processor of management device via a second bus of the management device,

CLAIMS
[12.e] wherein the network device includes a processor configured to facilitate operation of the network device, and
[12.f] wherein the processor of the management device is distinct from the processor included in the network device;
[12.g] decrypting, by the processor, the encrypted form of the management requests; and
[12.h] controlling, by the processor, one or more functions of the network device according to the management requests.
[13] The method of claim 12, wherein the one or more functions are associated with a domain name service protocol.
[14] The method of claim 12, wherein the one or more functions are associated with a network time protocol.
[15] The method of claim 12, wherein the one or more functions are associated with a network management protocol.
[16pre] The method of claim 12, further comprising:
[16.a] establishing, by the management device, a virtual private network connection with an access control server configured to authenticate the remote administrator.
[17] The method of claim 12, further comprising: receiving, by the management device, additional management requests from the remote administrator via a network interface of the management device, and wherein the additional management requests are not received via the first bus of the network device.
[18] The method of claim 17, wherein the network interface of the management device is a telephone-line interface.
[19pre] The method of claim 12, further comprising:
[19.a] receiving, by the management device, power via a first power circuit separate from a second power circuit of the network device; and
[19.b] cycling, by the management device, power from the second power circuit to reset the network device.
[20] The method of claim 12, wherein the management device is a card including the processor and the bus controller, wherein the card is configured to be inserted into the network device via a card interface.

CLAIMS

[21] The method of claim 12, wherein the network device is a network router that includes a plurality of network interfaces, and wherein the processor is dedicated to controlling one or more functions of the network router.

I. INTRODUCTION

1. I have been retained by counsel for Lenovo (United States) Inc. (“LUS”) 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 Nos. 8,474,016 (“the ’016 patent”), and claims of U.S. Patent No. 8,325,140 (“the ’140 patent”) (collectively, “the IV patents” or “asserted IV patents”).

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 Qualification

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 (“IV”). 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.

22. 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

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

24. I understand that a U.S. or foreign patent qualifies as prior art to an asserted patent if the date of issuance of the patent is prior to the invention of the asserted patent.

25. 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.

26. 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.

27. 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.

28. I also 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. Legal Standards for Obviousness

29. I understand that a patent claim is unpatentable 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.

30. 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.

31. 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.

32. I understand that an obviousness evaluation can be based on a combination of multiple prior art references.

33. I also 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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 propose combination, not necessarily something that suggests that the proposed combination is the most desirable combination available.

41. 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.

42. 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.

43. 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.

44. 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.

45. 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.

46. 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.

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

III. OVERVIEW OF THE ‘016 PATENT

A. Summary of the ‘016 Patent

48. The 016 patent relates to remote management of network devices in a secure manner. EX1001, 1:25-31. This remote management is accomplished by a “remote management access controller,” which is referred to as a “SMACC” (“Secure Management Access Control for Computer Chipset”) in some embodiments. EX1001, 5:46-67. The SMACC manages the network device in accordance with management requests received from a remote administrator. *Id.*

49. The ‘016 patent discloses that the remote administrator can communicate with the SMACC in band using the same network as the user data for the managed device, or out-of-band using a means other than the network used by users of the managed device. EX1001, 1:53-60; 5:67-6:31. Although the independent claims do not expressly recite in-band or out-of-band communication of management requests, they do recite a “network interface” configured to receive both data requests and management requests, which is an in-band communication of management requests. EX1001, 22:25-45 and 23:23-13:2.

50. In some embodiments of the ‘016 patent, the in-band management requests are received by the SMACC via a VPN (virtual private network) to logically separate them from the user data. *Id.*

B. The ‘016 Patent Prosecution History

51. Prior to the start of substantive examination, the Applicant amended the claims to recite a single “system bus” and a “bus controller” connected to that system bus. EX1004, 277 (2/30/11 Response at 2). The examiner rejected those claims over prior art referred to as Schelling. EX1004, 289 (3/13/12 Rejection at 3).

52. In response, the Applicant amended the claims to recite two distinct buses, a first bus and a second bus, and require that the “bus controller . . . convey

the encrypted form of the management requests to the processor” from one bus to the other. EX1004, 334 (4/30/12 Response at 2).

53. The Applicant then argued that Schelling’s bus controller 118 did not satisfy this limitation because that bus controller did not convey the encrypted management requests from one bus another. EX1004, 341 (4/30/12 Response at 9). Support for this two bus and controller arrangement was identified by the Applicant as Figs. 28 and 29 of the 016 Patent:

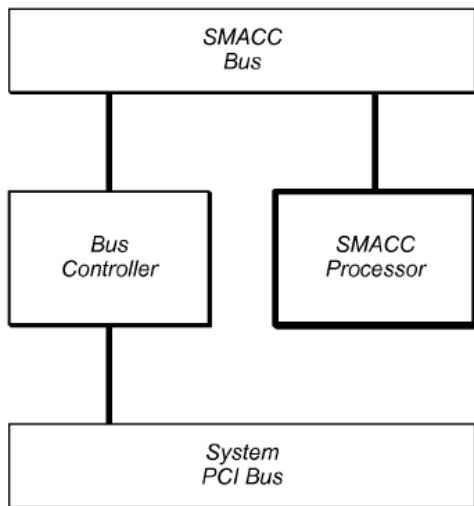


Fig. 28

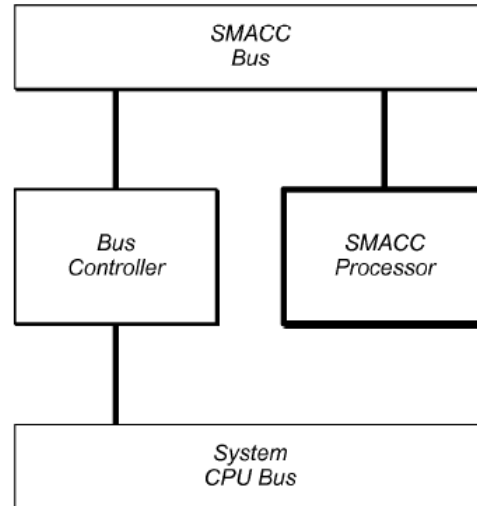


Fig. 29

EX1004, 393 (10/19/12 Response at 8). The two buses were recited as the first bus and the second bus in the allowed version of the claims. EX1004, 388 (10/19/12 Response at 3).

54. The independent claims were allowed after PO further amended them to require a processor of the network device distinct from the SMACC processor. EX1004, 428 (1/23/13 Response at 2) and 441 (2/25/13 Notice of Allowance at 2).

C. Priority Date of the 016 Patent

55. I have been instructed by counsel for Petitioner that the 016 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

56. A person of ordinary skill in the art (“POSITA”) at the time of the alleged invention of the 016 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.

57. In this regard, all of the technologies, techniques, methods, and components disclosed in Neufeld, Frantz, Huckins, Martenson, 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)

58. I understand from counsel for LUS 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.

59. In this declaration, I apply the claim language's ordinary and customary meaning, unless indicated otherwise. Except as indicated below, I do not believe that any express construction is necessary for the issues on which I opine in this declaration.

1. “the processor” (as used in the term “controlling, by *the processor*, one or more functions of the network device according to the management re-quests”) (claim 12)

60. For the purposes of this IPR, I have been asked to address unpatentability of this term as meaning “a processor of the management device” as recited in claim 12 as well as “a processor configured to facilitate operation of the network device” as recited in claim 12. 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 016 patent.

IV. PRIOR ART REFERENCES

61. 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:

B. Patents

62. 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	Frantz	1/4/2002	12/4/2003	102(e)
1011	Martenson	5/30/1996	4/17/2001	102(b), 102(e)
1012	MacWilliams	4/12/1995	7/22/1997	102(b), 102(e)
1015	Rossman	2/12/2002	8/21/2007	102(e)
1017	Hrastar	6/3/2002	6/3/2008	102(e)

C. Patent Publications

63. 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)
1007	Huckins	5/19/2001	5/22/03	102(a), 102(e)
1016	Syvanne	11/19/2001	5/22/2003	102(a), 102(e)

D. Non-Patent Publications

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

65. EX1008 (PCI Bridge Spec) is prior art under §102(b) because it was published on 12/18/98 as evidenced by EX1027 at 1.

66. EX1009 (PCF8584) is prior art under §102(b) because it was published on October 27, 1997 as evidenced by EX1009 itself at 40 (“Date of release: 1997 Oct 21”; FRE §803(16)) and by its citation in EX1028, 46:9-12.

67. 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), by its IETF “bibtex” listing (EX1035, 1). The citation to RFC1492 in WO99/57846 at 25 is further evidence that this document was published at least by the publication date of that document on November 11, 1999.

68. EX1014 (RFC2865) is prior art under §102(b) because it was published In June 2000 as evidenced by EX1014 at 1 (“Distribution of this memo is unlimited”;),by its citation in EX1030, 12:13-15), and by its IETF “bibtex” listing (EX1034, 1). I am also personally aware that RFC documents such as this are published and available to those of skill in the art as of the dates listed in the IETF bibtex listing.

69. EX1018 (RFC1157) is prior art under §102(b) because it was published in May 1990 as evidenced by EX1018 at 12 (“Distribution of this memo is unlimited”; FRE §803(16)), by its citation in EX1031, 2:10-11), and by its IETF

“bibtex” listing (EX1033, 1). The citations to RFC1157 in U.S. Patent No. 6,067,585 at 27:7-14 and Table 4 is further evidence that RFC1157 was published at least by the issue date of that patent on May 23, 2000.

70. 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.

71. EX1021 (RFC3414) is prior art under §102(a) because it was published in December 2002 as evidenced by EX1021, 1 (listing December 2002 and stating “Distribution of this memo is unlimited”) and by its IETF “bibtex” listing (EX1032, 1). I am also personally aware that RFC documents such as this are published and available to those of skill in the art as of the dates listed in the IETF bibtex listing.

72. EX1023 (IPMIv2.0) is prior art under §102(a) because it was published on 9/15/03. EX1023, 1; EX1039, 5 and 23.

73. EX1037 (DSP0114) is prior art under §102(b) because it was published on 6/20/2001 as evidenced by EX1037, 1 (listing June 20, 2001 and stating that “DTMF specifications and documents may be reproduced for uses consistent with this purpose by members and non-members, if attribution is given”), and by its citation in EX1038, 8:17-19.

V. GROUND 1: NEUFELD RENDERS OBVIOUS CLAIMS 1-3, 6, 9, 12 AND 17

74. 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].

75. 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].

76. 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:

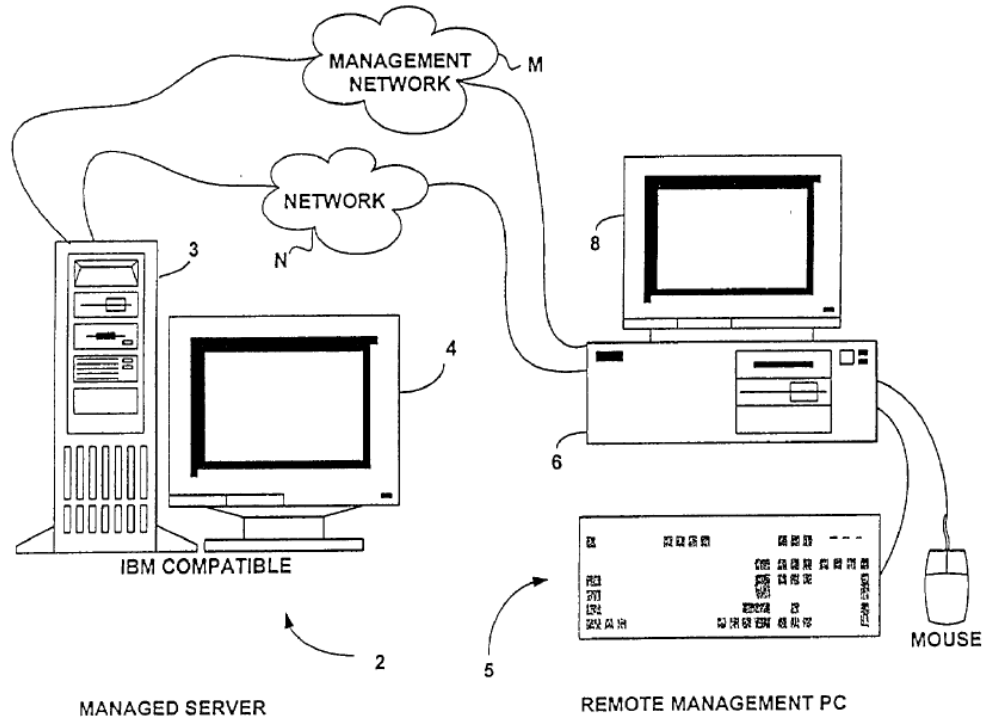


FIG. 1

77. 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:

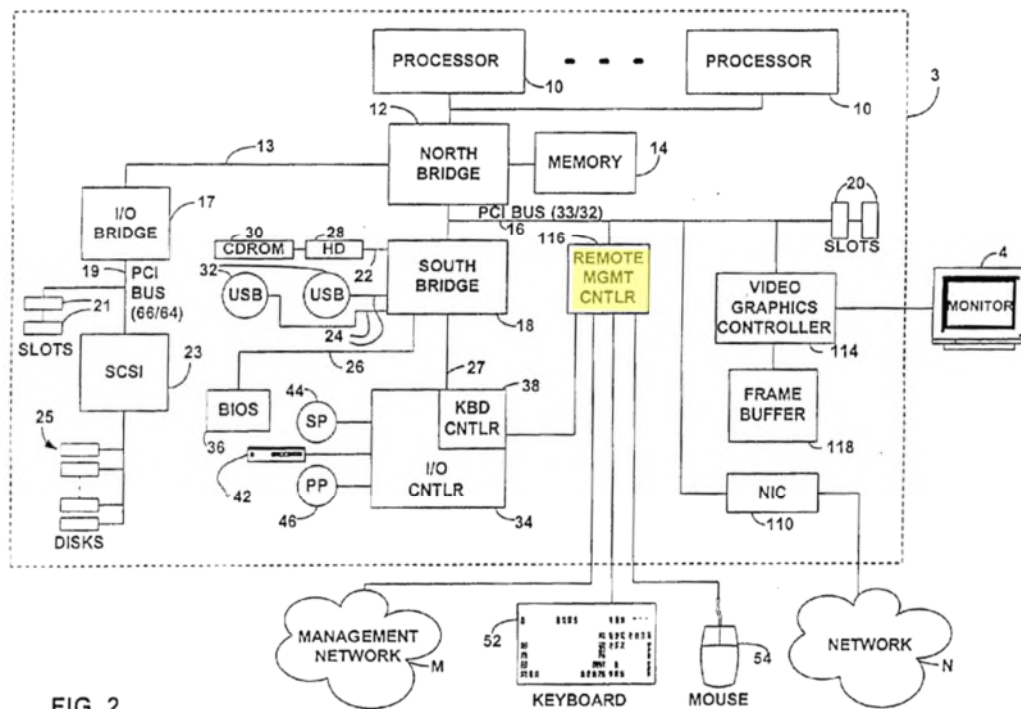
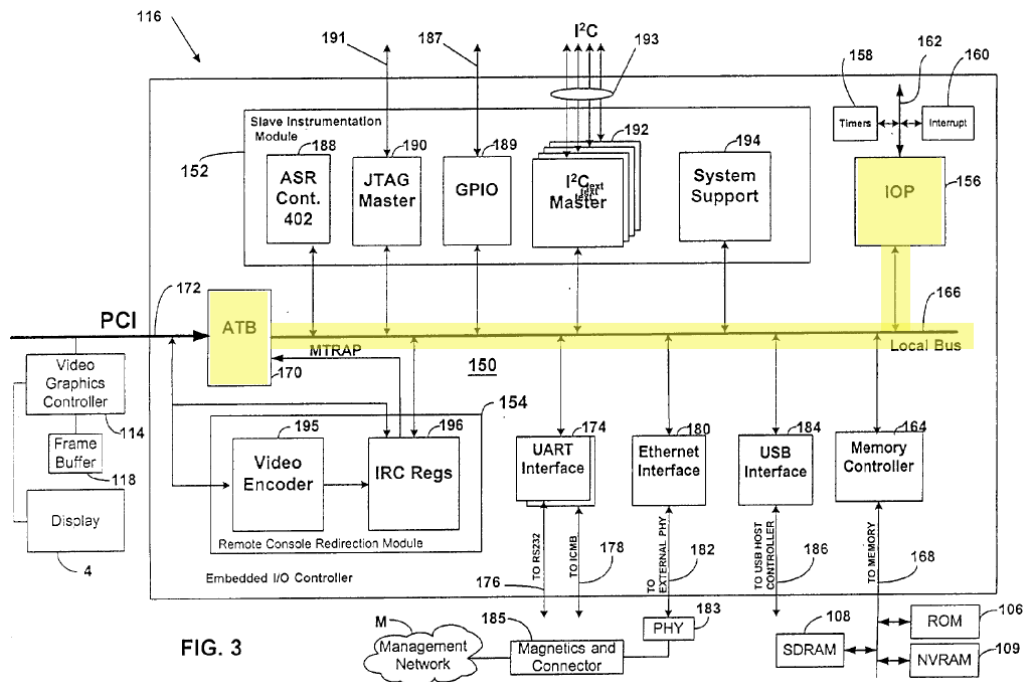


FIG. 2

78. 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 highlighted Fig. 3 below. The server's Network Interface Controller ("NIC") 110 is also connected to the PCI bus 1721 as shown above.



79. 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] 1. An apparatus, comprising:

80. To the extent the preamble is limiting, Neufeld discloses an apparatus. See, e.g., Neufeld’s title: “Method **and Apparatus** for Configuring Security Options in a Computer System.” EX1001, 1. Neufeld’s remote management controller 116, shown in Fig. 2 below, is the claimed “apparatus.” EX1005, ¶[0043].

2. [1.a] a processor configured to control one or more functions of a network device having a network interface,

81. Neufeld discloses this limitation. Neufeld's IOP 156 is the claimed "processor," Neufeld's managed server 2 is the claimed "network device," and the NIC 110 is a "network interface" of the managed server 2. Neufeld discloses that the remote management controller 116 "includes an Input/Output processor ('IOP') 156, which provides general control and functions as a management processor for the remote server management controller 116." EX1005, ¶[0054]; *see also* EX1005, Figures. 2 and 3 (highlighting added):

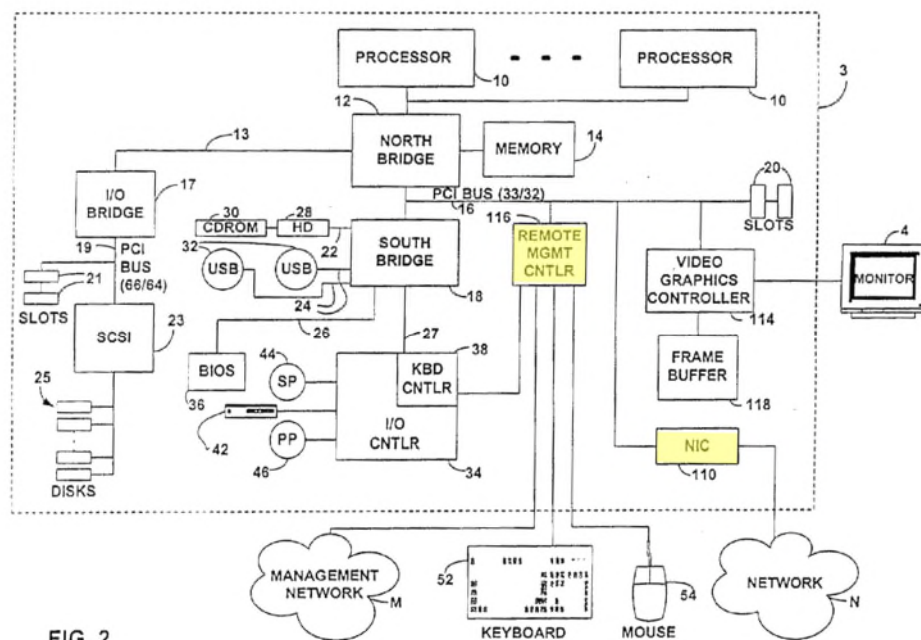
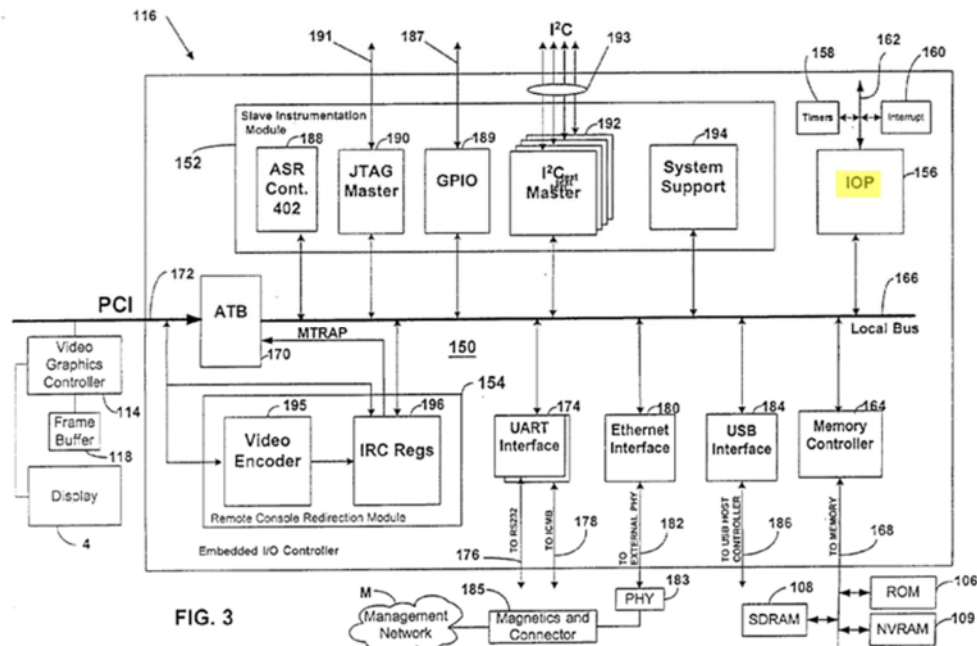


FIG. 2



82. The IOP 156 controls functions of Neufeld's managed server 2, such as rebooting, modifying BIOS and/or communicating with server operating system features such as the Emergency Management Services facility of the Windows XP, via the slave instrumentation module 152. Neufeld, ¶¶ [0066]-[0074].

83. The CPU 3 of Neufeld's managed server 2 has a network interface in the form of a NIC (network interface controller) 110 that interfaces to Network N as shown in Fig. 2 above. EX1005, ¶[0045].

3. [1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface,

84. Neufeld discloses and renders obvious this limitation. Neufeld's managed server 2 is configured to receive both data requests and in-band

management requests over a Network N from a remote management PC 5 (a “remote administrator”) as shown in Figure 1:

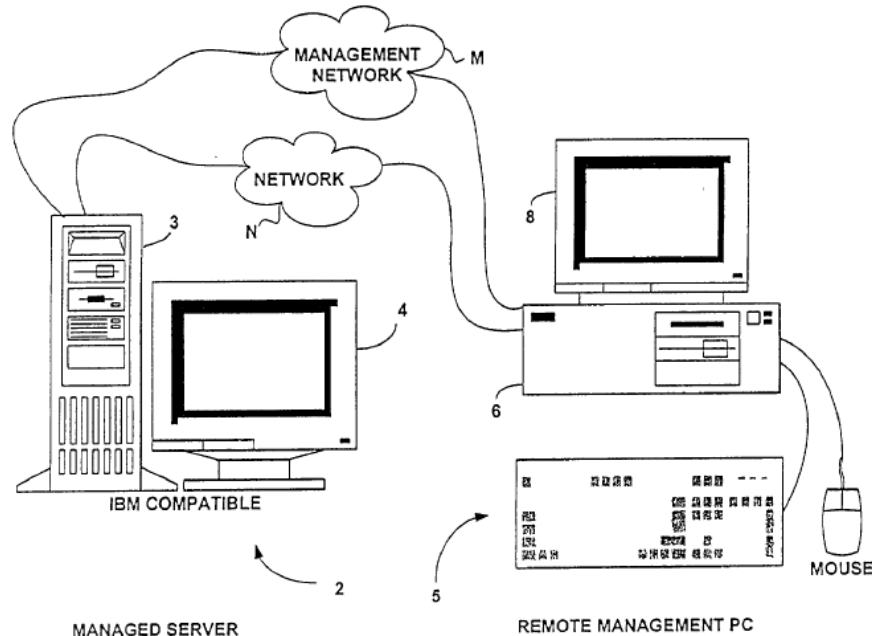


FIG. 1

EX1005, Fig. 1; *see also* ¶[0011] (referring to in-band, on-line communications).

85. Neufeld defines “in-band” communications as communications with the server “over a standard network connection, such as the managed server’s normal Ethernet connection.” EX1005, ¶[0011]. A POSITA would have understood the “server’s normal Ethernet connection” to be the Ethernet connection over which normal user (non-administrator) data requests are received, or at least would have found it to be obvious.

86. Neufeld further discloses the desirability of providing in-band as well as out-of-band communications for monitoring and control of the managed server

2. EX1005, ¶[0015] (explaining that an “important goal” is to increase the number of server problems that can be analyzed and repaired remotely, and that it is “highly desirable” to provide in-band communications to capture the maximum amount of information from, and allow control of, the managed server).

87. Neufeld also discloses that “[t]he remote management controller 116 connects . . . **the network N** and/or a management network M . . . to provide functionality for accessing, interacting, and monitoring the managed server 2 from the remote console 5 as will be more fully described below” and (“[t]he remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 from either the local keyboard 52 or from the remote console 5 via the modem **or NIC 110** which may be coupled to the network M [sic, N].” EX1005, ¶¶[0043], [0047] (emphases added). *See also* EX1005, ¶[0045] and Figs. 2-3 (showing connection between Network N and remote management controller 116).

88. Neufeld further discloses and therwise renders obvious the encryption of remote management requests sent to the remote management controller 116 via Network N. Neufeld notes that security may be an important issue when remotely communicating management requests to the managed server. EX1005, ¶[0018]. Consistent with this teaching, Neufeld discloses that “**any** type of remote access would typically utilize encryption techniques” and includes a Table 2 for “Network

Administrators” that lists the “security setting” for a “Net-admin 1” user as “encryption”. EX1005, ¶[0085] (emphasis added) and Table 2.

89. A POSITA would have recognized or at least found it obvious that “any type of remote access” includes communication of management requests, and that the “Net-admin 1” user, who is a Network Administrator that would send management requests, would access the remote management controller 116 for communicating such management requests and would do so in encrypted form in light of this disclosure.

90. Neufeld also discloses that a “network administrator,” who a POSITA would understand is the person responsible for managing the server 2 using the remote management controller 116, accesses it to send management requests from home or while traveling using a virtual private network (“VPN”). EX1005, ¶[0022].

91. A POSITA would have understood or at least found obvious that accessing the remote management controller 116 while traveling or from home required transmitting the management requests via the public Internet through NIC 110 as no Management Network M would be available to the user when traveling or at home. See EX1005, ¶[0035] (network N can be an “Internet connection”). Moreover, a POSITA would have understood and found it obvious that a virtual private network would employ encryption because this was extremely well-known

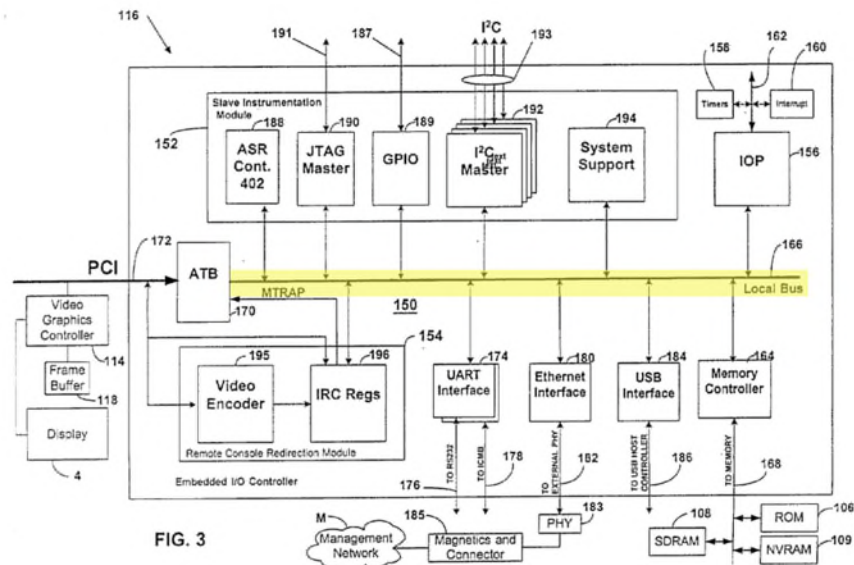
in the art and encryption is even in the definition of a VPN according to the Microsoft Computer Dictionary. EX1019, 3. In any event, Neufeld also discloses a user granted privileges for non-critical management functions when using a remote VPN connection that is encrypted. EX1005, ¶[0088] Table 4, User ID 7.

4. [1.c] wherein the management requests are received from a remote administrator;

92. Neufeld discloses this limitation. See limitation [1.b] (discussing receiving management requests from a “network administrator” at a remote management PC 5 of Neufeld’s Figure 1).

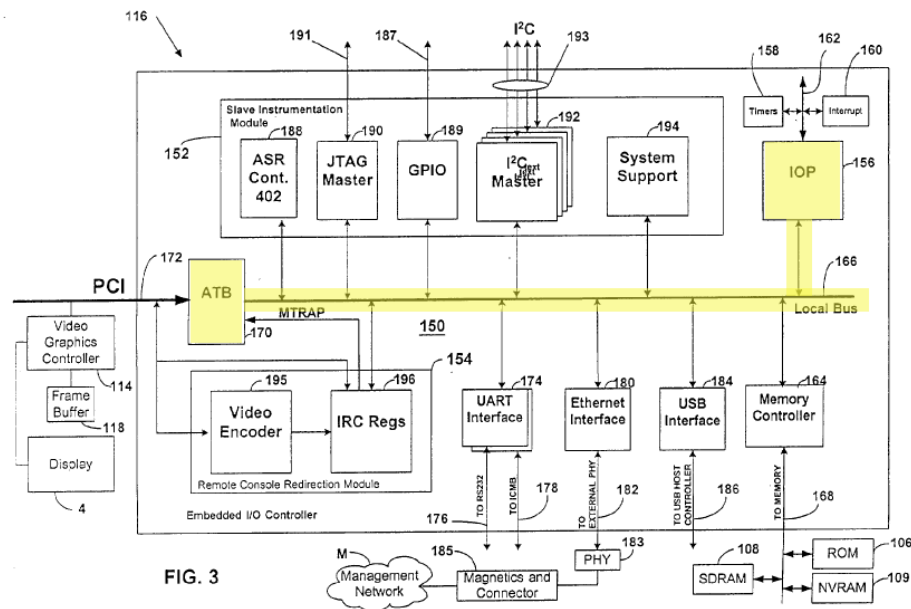
5. [1.d] a first bus; and

93. Neufeld discloses this limitation. Neufeld discloses an “internal local bus 166” that is part of the remote management controller 116. EX1005 ¶[0056] and Fig. 3 (emphasis added).



6. [1.e] a bus controller coupled to the processor via the first bus;

94. Neufeld discloses and renders obvious this limitation. Neufeld discloses an address translation and bridging (ATB) unit 170 coupled to IOP 156 via the local bus 166 as shown in annotated Fig. 3 below. EX1005, ¶¶ [0056]-[0057].



95. The ATB170, which Neufeld discloses resides on the compatibility segment of PCI bus 172, which itself is an extension PCI bus 16 of Fig. 2, is a bus controller. EX1005, ¶¶ [0057]-[0058]. Neufeld discloses that the ATB 170 “is constructed to allow the remote server management controller 116 to decode bus cycles on the PCI bus 172 and to communicate over the PCI bus 172 by initiating PCI bus cycles.” EX1005, ¶ [0057]. ATB 170 therefore includes a bus controller.

96. In the event that the Board determines that the ATB 170 does not include a bus controller, a POSITA would have found it obvious to include a bus controller in ATB 170. It was known in the art and customary for a bus bridge that links a primary bus to a secondary bus to include a bus controller to control the secondary bus. *See also* Ground 2 below.

7. [1.f] wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus

97. Neufeld discloses or render obvious this limitation. In addition to being coupled to the local bus 166, ATB 170 is coupled to a second distinct bus, the PCI bus 172 as shown in Fig. 3 below. EX1005, ¶[[0057] and Fig. 3 (highlighting added).

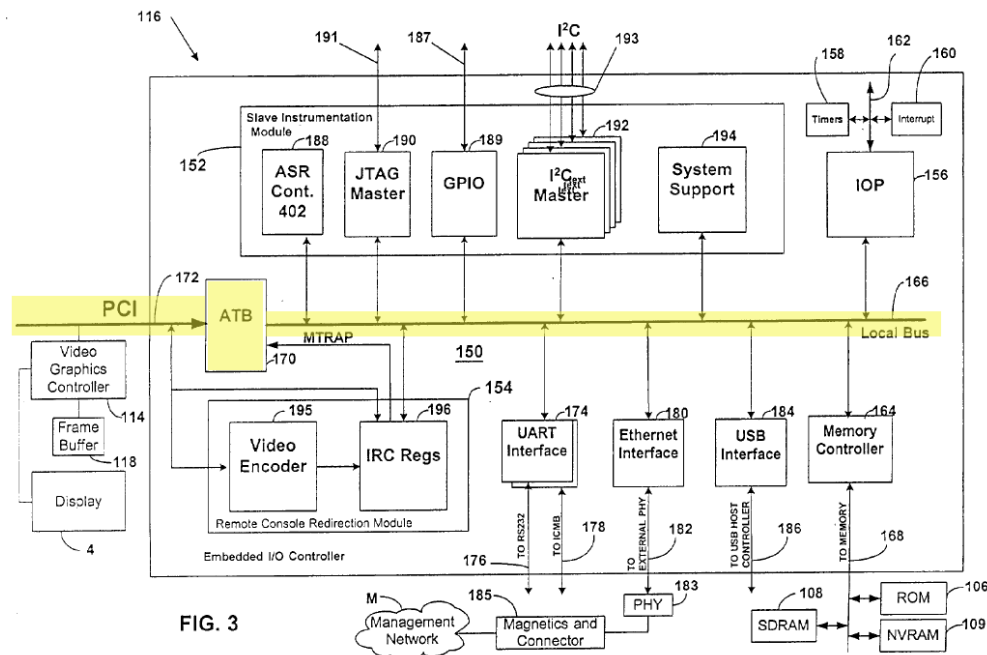


FIG. 3

8. [1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus,

98. As discussed above, Neufeld discloses and/or renders obvious to a POSITA that the remote management controller 116 receives in-band communications including management requests from the remote management PC 5 via the NIC 110. *see also* limitation [1.b] and EX1005, ¶[0043] (“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”), ¶[0047] (“[t]he remote management controller 116 also includes circuitry to route keystrokes to the keyboard controller 38 from either the local keyboard 52 or from the remote console 5 via the modem **or NIC 110** which may be coupled to the network M [sic, N]”) and Figs. 2-3 (showing connection between Network N and remote management controller 116).

99. As shown in Fig. 2, the NIC 110 is connected to the PCI bus 16 in the server CPU 3. As discussed above for limitation [1.f], the PCI bus 172 of Fig. 3 is an extension of the PCI bus 16 of Fig. 2. Thus, the ATB 170 receives the encrypted management requests from the remote management PC 5 through the NIC 110 via the PCI bus 172.

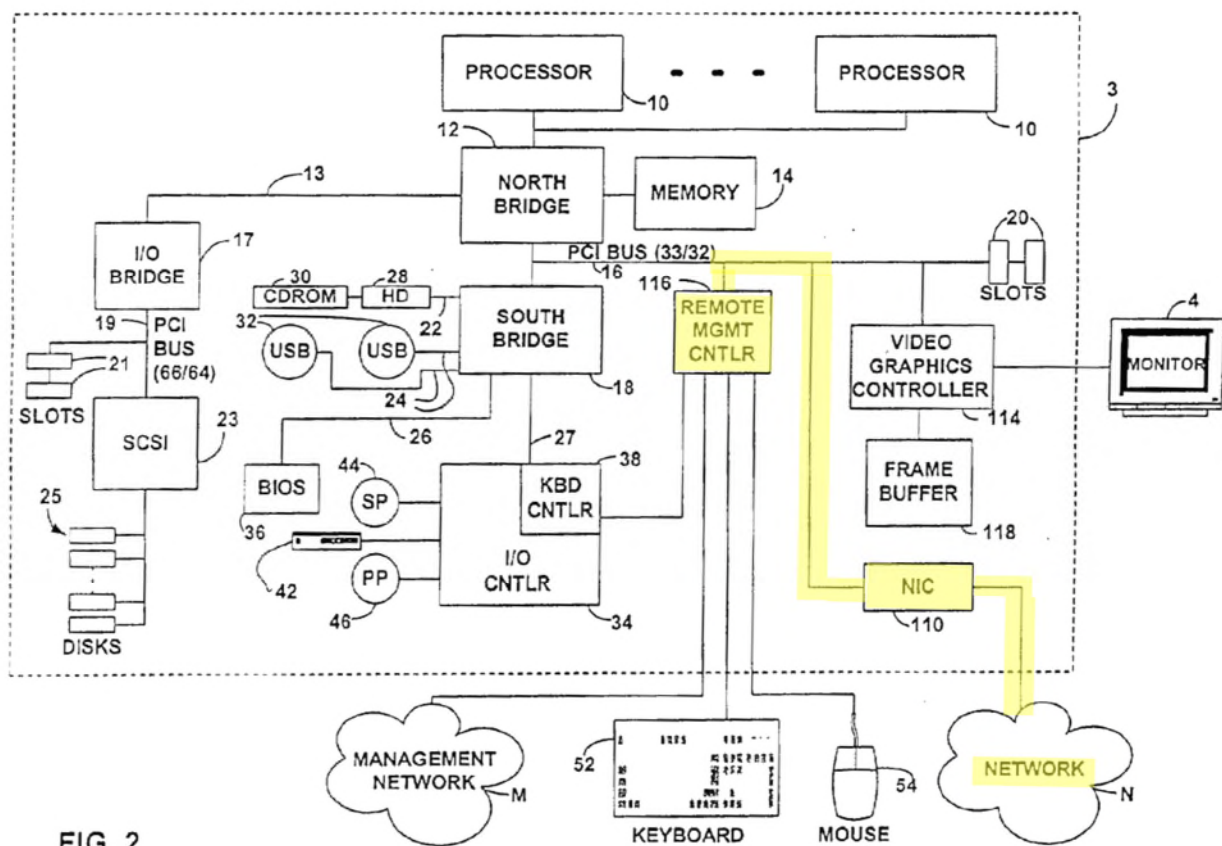


FIG. 2

9. [1.h] and to convey the encrypted form of the management requests to the processor via the first bus;

100. Neufeld discloses and/or renders this limitation obvious to a POSITA. See limitation [1.g] establishing that management requests are received by the ATB 170. Neufeld further discloses that the ATB 170 is connected to IOP 156 via the first bus 166. See limitation [1.e]; see also EX1005, Fig. 3.

101. Neufeld further discloses that IOP 156 provides general control and functions as the management processor for the remote management controller 156, and that the IOP 156 dictates the control and monitoring functions performed via

the slave instrumentation module 152. EX1005, ¶¶[0054], [0066]. A POSITA therefore would have understood and found it obvious that IOP 156 would be configured to receive the encrypted form of the management requests and to decrypt and act on them, because IOP 156 is a processor and therefore can be programmed to perform these functions, and because the other devices in the remote management controller 110 are directed toward specific functions that do not include decrypting or acting on remote management requests.

102. To the extent that Neufeld does not disclose this limitation, it would have been obvious to a POSITA to provide for in-band communication of management requests from the remote management PC 5 to the IOP 156 of the remote management controller 116 in light of Neufeld's disclosure of the desirability of providing for in-band communication to control the managed server at ¶[0015] and the need to decrypt management requests in order to act on them.

10. [1.i] wherein the processor is configured to decrypt the encrypted form of the management requests

103. Neufeld discloses or renders obvious this limitation. As discussed above, Neufeld discloses or renders obvious that remote management requests are received at the IOP 156 in encrypted form. See limitations [1.b], [1.e], and [1.h]. Neufeld at least implies that the IOP 156 will decrypt the encrypted management requests because without decryption the IOP would be unable to act on them. To the extent that Neufeld does not disclose that the IOP 156 decrypts encrypted

management messages, configuring it to do so would have been obvious to a POSITA for the reasons discussed above for limitation [1.h].

11. [1.j] wherein the network device includes a processor configured to facilitate operation of the network device, and

104. Neufeld discloses this limitation. Neufeld's managed server 2 includes a CPU with multiple processors 10 that facilitate operation of the managed server 2. EX1005, ¶[0038] and Fig. 2 (highlighting added).

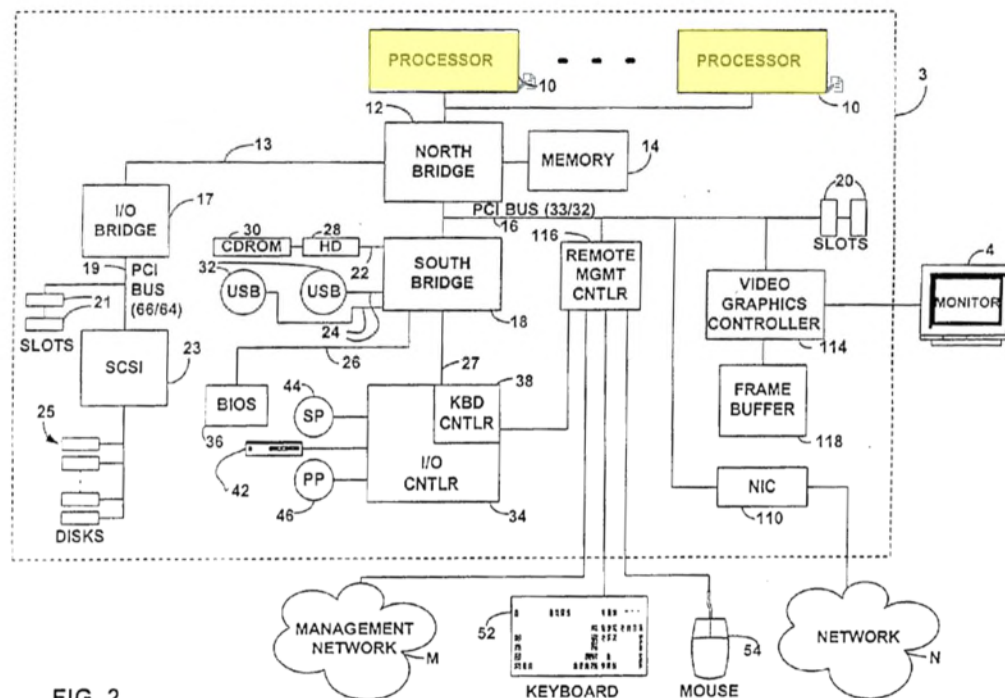


FIG. 2

12. [i.k] wherein the processor of the apparatus is distinct from the processor included in the network device.

105. Neufeld discloses this limitation. The IOP 156 in the remote management controller 116 is distinct from the processors 10 of the managed server CPU 3.

B. Claim 2. The apparatus of claim 1, wherein the apparatus is configured to provide a command line interface to the remote administrator, and wherein the apparatus is configured to receive one or more commands to control the one or more functions of the network device.

106. Neufeld renders claim 1 obvious and therefore also renders claim 2 obvious because Neufeld discloses the limitations of claim 2 and/or renders them obvious. Neufeld incorporates by reference U.S. Pat. App. No. 09/438,253 (“Emerson,” EX1010). EX1005, ¶¶ [0028], [0032]. Emerson discloses 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.

107. A POSITA would have understood, or at least found it obvious, that a telnet session utilizes a command line interface. Implementing a command line interface for a remote administration would have been obvious to a POSITA because command line interfaces via Telnet or SSH (secure shell) were very well-known and the use of a command line interface via Telnet or SSH was one of the most commonly-used ways to remotely administer devices at the time of the 016 patent. Indeed, the ’016 patent admits that both Telnet and SSH are “protocols that are typically utilized for management of a device.” EX1001, 12:28-33. Emerson discloses this connection being established over a modem, which a POSITA would understand corresponds to out-of-band communications with the remote

management controller 116 via a modem as discussed in Neufeld at ¶¶[0045] and [0060].

108. Neufeld further discloses that the remote management controller 116 controls one of more functions of the managed server 2 as discussed above in connection with limitation [1.a].

C. Claim 3. The apparatus of claim 1, wherein the bus controller is a peripheral component interconnect (PCI) controller.

109. Neufeld renders claim 1 obvious and therefore also renders claim 3 obvious because Neufeld renders the limitations of claim 3 obvious. Neufeld discloses that bus 172/16 to which local bus 166 is connected is a PCI bus. EX1005, ¶¶[0039], [0057]. Neufeld discloses that the purpose of the local bus 166 is to allow communication between the logical components of the embedded I/O controller 150 and the remote management controller 116, and does not specify how to implement the local bus 166 but instead characterizes the implementation as a design choice that is not crucial to Neufeld's invention. EX11005, ¶[0056].

110. It would have been obvious to a POSITA in light of the above to implement Neufeld's internal local bus 166 as a PCI bus like the PCI bus 172/16,, and to configure Neufeld's ATB 170 as a PCI-PCI bus controller/bridge.

111. A POSITA would have been motivated to implement Neufeld's local bus 166 as a PCI bus because Neufeld's Fig. 3 discloses multiple peripheral I/O devices (e.g., UARTs 174, Ethernet interface 180, USB interface 184) connected to

the local bus 166, and a POSITA would have recognized that many existing I/O devices at the time were configured for connection to a PCI bus as shown for example in Fig. 2 of Neufeld with the NIC 110 (which a POSITA would have recognized as commonly being implemented as an Ethernet NIC) connected to PCI bus 16, and therefore selection of a PCI bus implementation for the local bus 166 would have allowed use of such existing components.

112. A POSITA would have been motivated to choose a PCI bus implementation for local bus 166 as there were a finite number of identified predictable choices for implementing a bus at the time, and the PCI bus standard was very well-known in the art.

113. A POSITA would further have recognized that a PCI bus implementation would have been sufficient to meet the bandwidth requirements for the Neufeld's local bus 166 and the remote management functions supported by that bus. A POSITA would have had a reasonable expectation of success as implementing a PCI bus involved no more than routine skill in the art.

D. Claim 6. The apparatus of claim 1, wherein the processor is configured to establish a first virtual private network connection with the remote administrator, and wherein the processor is configured to receive the management requests via the first established connection.

114. Neufeld renders claim 1 obvious and therefore also renders claim 6 obvious because Neufeld discloses or renders obvious the limitations of this claim.

See discussion of receiving management requests at the remote management controller 116 from the remote management PC 5 over Network N via a VPN in Section IV.A and limitations [1.a], [1.b], [1.c] and [1.g].

115. A POSITA would have understood and found it obvious that Neufeld's IOP 156 would establish a VPN connection with the remote management PC 5 to ensure that any security breach of other portions of the managed sever 2 does not result in a security breach of remote management controller 116 or compromise its ability to react to such security breaches of the other portions of the managed server 2.

E. Claim 9. The apparatus of claim 1, wherein the apparatus is a component within the network device.

116. Neufeld renders claim 1 obvious and therefore also renders claim 9 obvious because Neufeld discloses the limitations of this claim. The remote management controller 116 is a device within the CPU 3 of the managed server 2. EX1005, ¶[0043] ("Further attached to the PCI bus 16 is a remote management controller 116.") and Fig. 2.

F. Claim 12

1. [12.pre] A method, comprising:

117. To the extent that the preamble is a limitation, Neufeld discloses it. See, e.g., EX1005 at title ("Method and Apparatus for Configuring Security Options in a Computer System") (emphasis added).

2. **[12.a] receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface**

118. Neufeld discloses or renders obvious this limitation. *See* limitations [1.a], [1.b], [1.e] and [1.g] (note: the first bus of claim 12 corresponds to the second bus of claim 1).

3. **[12.b] wherein the network device received the encrypted form of the management requests and data requests via the network interface,**

119. Neufeld discloses this limitation. *See* limitation [1.b] (note: the first bus of claim 12 corresponds to the second bus of claim 1).

4. **[12.c] wherein the management requests are from a remote administrator;**

120. Neufeld discloses this limitation. *See* limitation [1.c].

5. **[12.d] conveying the encrypted form of management requests from the bus controller to a processor of management device via a second bus of the management device,**

121. Neufeld discloses and renders obvious this limitation. *See* limitations [1.c] and [1.h] (note: the second bus of claim 12 corresponds to the first bus of claim 1).

6. **[12.e] wherein the network device includes a processor configured to facilitate operation of the network device, and**

122. Neufeld discloses this limitation. *See* limitation [1.j].

7. **[12.f] wherein the processor of the management device is distinct from the processor included in the network device;**

123. Neufeld discloses this limitation. *See* limitation [1.k].

8. **[12.g] decrypting, by the processor, the encrypted form of the management requests; and**

124. Neufeld discloses or renders obvious this limitation. *See* limitation [1.i].

9. **[12.h] controlling, by the processor, one or more functions of the network device according to the management requests.**

125. To the extent that “the processor” in this limitation refers to “a processor of management device” as recited in claim 12, Neufeld discloses it. *See* limitation [1.a] (discussing IOP 156 controlling aspects of CPU 3 of managed server 2).

126. To the extent that “the processor” in this limitation refers to “a processor configured to facilitate operation of the network device” as recited in claim 12, Neufeld discloses it and renders it obvious. *See* limitation [1.j] (discussing processor 10 that facilitates operation of the managed server 2) and the discussion in Neufeld at ¶[0074] of the remote management controller 116 communicating with the Emergency Management Services (“EMS”) facility of the Windows XP operating system.

127. A POSITA would have understood and found it obvious that the EMS facility of the operating system would be executed by one of the processors 10 in

the CPU 3 of the managed server 2 because Neufeld discloses that the operating system is separate from the remote management controller 116. EX1005, ¶[0014].

G. Claim 17. The method of claim 12, further comprising: receiving, by the management device, additional management requests from the remote administrator via a network interface of the management device, and wherein the additional management requests are not received via the first bus of the network device.

128. Neufeld renders this claim obvious because Neufeld render obvious claim 12 and discloses the limitations of this claim. As discussed above, Neufeld discloses out-of-band communications between the remote management PC 5 and the remote management controller 116 of the managed server 2. *E.g.*, EX1005, ¶[0014]; *see also* limitation [1.b]. Examples of out-of-band communications include, with reference to Figs. 2 and 3, communications sent to the remote management controller 116 over the Management Network M via the Ethernet interface 180, standard modems attached to the UART interface 174, and via the keyboard 52 and/or mouse 54. EX1005, ¶¶ [0060]-[0064]. These out-of-band communications are all received other than via the PCI bus 16 and/or the PCI bus 172, which correspond to the first bus of claim 12.

VI. GROUND 2: NEUFELD IN COMBINATION WITH FRANTZ AND HUCKINS AND/OR PCI BRIDGE SPEC RENDERS OBVIOUS CLAIMS 1-3, 6, 9, 12 AND 17

A. Introduction

129. To the extent not disclosed or rendered obvious by Neufeld, Neufeld in combination with Frantz would have rendered obvious to a POSITA the

requirements in claims 1 and 12 for encryption and decryption of in-band management requests from the remote management PC 5 to the remote management controller 116.

130. It would have been obvious to a POSITA to encrypt such management requests in view of the disclosure in Neufeld at, *e.g.*, ¶[0022] of the need for security, particularly when a network administrator uses a remote management PC 5 from the administrator's home or while the administrator is traveling, which a POSITA would have understood as requiring the administrator to communicate with the remote management controller 116 over the public Internet.

131. A POSITA would have been motivated to do so in order to provide for better security. A POSITA also would have been motivated to do so in light of the facts that Neufeld and Frantz have a common assignee, a common inventor, and that Neufeld's Figure 3 is nearly identical to Frantz's Figure 2. EX1001, 1, and Fig. 3; EX1006, 1 and Fig. 2.

132. A POSITA would still further have been motivated to do by the teaching in Frantz of the desirability of making such in-band communication of management requests secure due to the sensitive nature of such management information and that a hacker's chances of gaining access to secure data on the managed server 2 would be improved if the hacker had access to such management information. EX1006, 3:19-41 and 10:50-63.

133. A POSITA would have had a reasonable expectation of success in so doing because encryption was well-known to a POSITA at the time of the 016 patent and involved no more than routine skill.

134. To the extent not disclosed or rendered obvious by Neufeld alone or in combination with Frantz,, Neufeld and Frantz in combination with PCI Bridge Spec would have rendered obvious to a POSITA to include a bus controller in Neufeld's ATB 170. A POSITA would have recognized that the local bus 166 could have been implemented as a PCI bus because Neufeld states that the implementation of local bus 166 is a design choice that is not critical, and a POSITA would have understood that a PCI bus would have been acceptable for the relatively (with respect to, *e.g.*, the front side bus for Neufeld's CPU 3) low bandwidth that would be necessary for Neufeld's remote management controller 116. EX1005, ¶[0056].

135. PCI Bridge Spec discloses including in a PCI-to-PCI bridge device as shown in Figure 1-1 below a PCI bus controller for the secondary interface/local bus 166. EX1008, 11 (defining primary and secondary interfaces), 13 and Figure 1-1 (illustrating bridge as including secondary master interface)(annotations added), 109 (disclosing bridge device providing arbiter for secondary bus), and 119 (discussing secondary bus reset signal and secondary bus parking during reset). Bus arbitration is often performed by a bus controller.

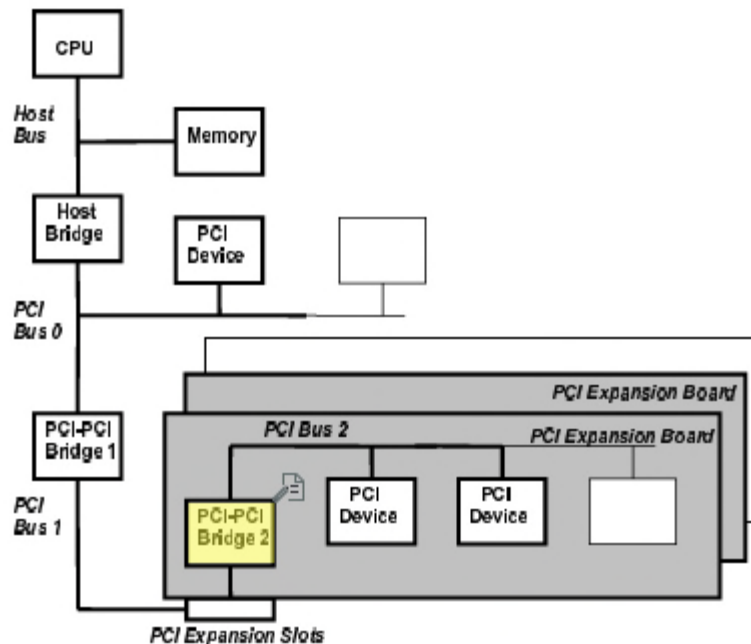


Figure 1-1: Typical Bridge Applications

136. Other bus bridging devices known in the art similarly include bus controllers for a secondary bus. See, e.g., Huckins (disclosing a PCI-to-non-PCI bus controller that “can also be referred to as a bridge”) and PCF8584 (disclosing a parallel bus-to-I²C bridging device that controls the I²C bus). EX1007, ¶[0026] and Fig. 1; EX1009, 3. A POSITA would have had a reasonable expectation of success in including bus controller functionality in ATB 170 because implementing bus controllers in bus bridges was well-known to a POSITA at the time of the 016 patent and involved no more than routine skill.

137. Addressed below are the specific limitations of claims 1 and 12 to which Frantz and PCI Bridge Spec are relevant for this Ground 2, which again is based on the combination of Neufeld with Frantz and PCI Bridge Spec. The

analysis for all other limitations and claims is the same for Ground 1 above and is incorporated here by reference.

138. The reference numbers used for the limitations of claims 1 and 12 apply equally to Ground 2 and all further grounds in this petition, and the claim language corresponding to those reference numbers will not be repeated below.

B. Claim 1

- 1. [1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface,**

139. In the Neufeld-Frantz-PCI Bridge Spec combination, Frantz discloses the encryption of in-band management requests as covered by this limitation for the reasons discussed in the Introduction to Ground 2.

140. Frantz discloses a remote console applet 606 in a client computer 72 that corresponds to Neufeld's remote management PC 5, and a managed server 20 with a remote server management controller 200 that corresponds to Neufeld's managed server 2 and remote management controller 116. EX1006, 5:4-40 and Figs. 2-3 (highlighting added).

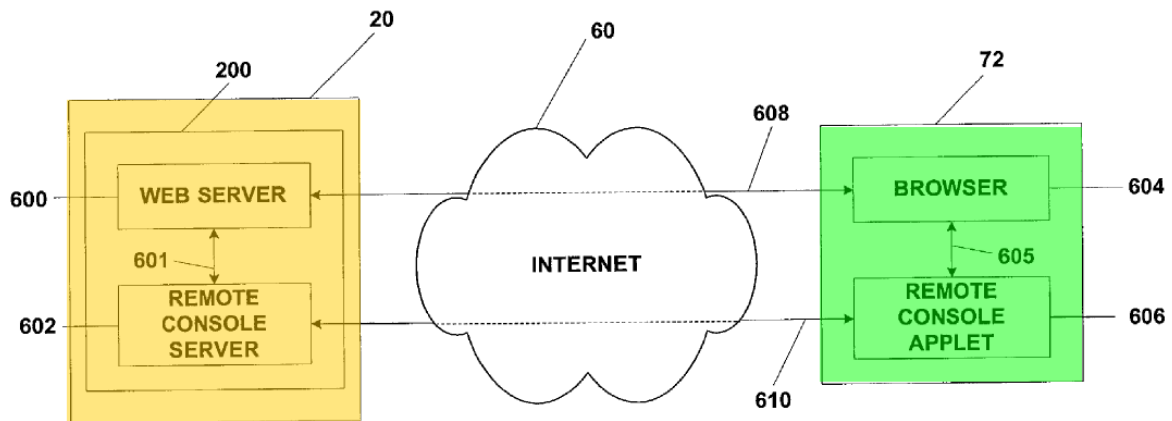


FIG. 3

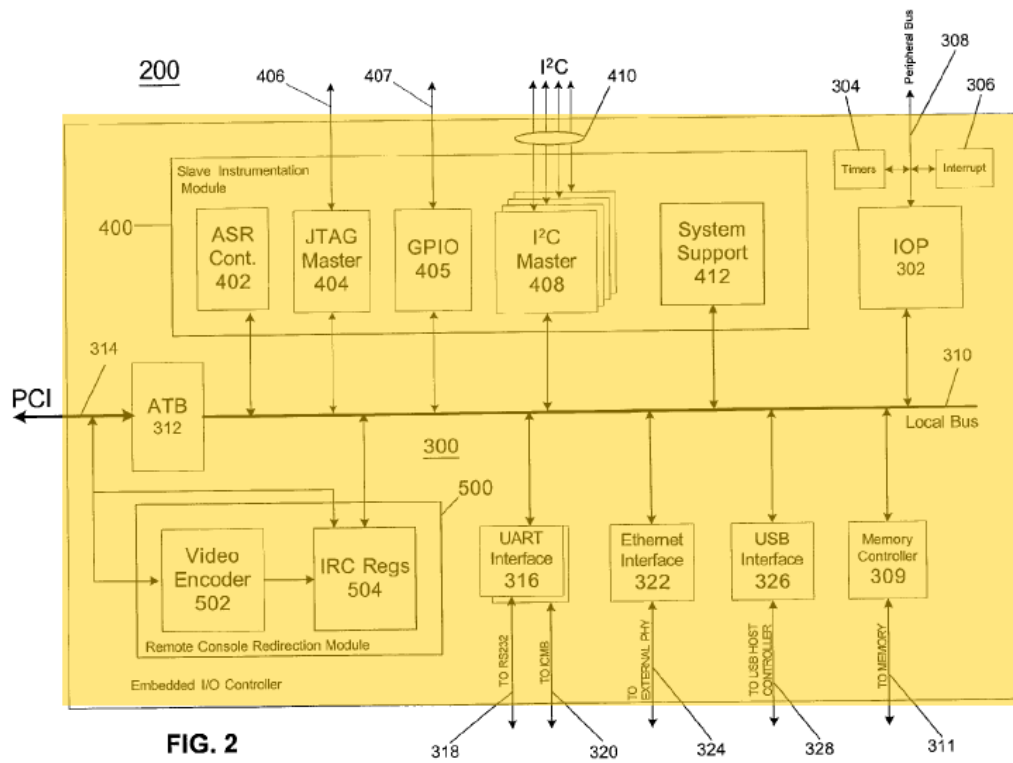


FIG. 2

141. The remote console applet 606 on the client computer 72 is used to communicate control (management) information to the remote management server controller 200 on the managed server 20. EX1006, 9:8-44.

142. For example, Frantz discloses that management requests may be sent in encrypted form using a Secure Sockets Layer protocol by an administrator using remote console applet 606 via link 605 to a web browser 604 at a client device 72, which communicates over link 608 with remote console server 602 via web browser 600 and link 601 as shown in Fig. 3. EX1006, 9:8-10:39.

143. A POSITA would have found it obvious to encrypt communications Neufeld's management messages in light of these disclosures for the reasons discussed above in the Introduction to Ground 2. *See, e.g.*, EX1006, 3:19-41 and 10:50-63.

2. [1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus,

144. The encryption requirement of this limitation would have been obvious to a POSITA over Frantz for the same reasons discussed above in connection with limitation [1.b].

3. [1.h] and to convey the encrypted form of the management requests to the processor via the first bus;

145. The encryption requirement of this limitation would have been obvious to a POSITA over Frantz for the same reasons discussed above in connection with limitation [1.b].

146. To the extent not disclosed or rendered obvious by Neufeld alone, the requirement for the bus controller to convey management requests from the second bus to the processor via the first bus would have been obvious to a POSITA in view of PCI Bridge Spec for the reasons discussed above in the Introduction to Ground 2. All of these references disclose devices that act as a combination of bridge between two busses and a controller for at least one of those busses.

4. [1.i] wherein the processor is configured to decrypt the encrypted form of the management requests

147. Neufeld in combination with Frantz renders obvious the decryption of in-band management requests as required by this limitation. Encrypting in-band management requests would have been obvious as discussed above in connection with limitation [1.b], and decrypting them would have been obvious to a POSITA because a POSITA would have understood that encrypted requests must be decrypted in order for them to be processed.

148. Frantz discloses or at least renders obvious that Frantz's IOP 302 receives and decrypts encrypted in-band management requests. For example,

Frantz discloses that management requests may be sent in encrypted form using a Secure Sockets Layer protocol by an administrator using remote console applet 606 via link 605 to a web browser 604 at a client device 72, which communicates over link 608 with remote console server 602 via web browser 600 and link 601 as shown in Fig. 3. EX1006, 9:8-10:39.

149. Frantz further discloses that the “web server 600 may be a functional block of the firmware stack that is executing on the IOP 302,” and the web “server decrypts” data. EX1006, 8:63-66, 10:17-21. Thus, a POSITA would have understood or at least found obvious that IOP 302 receives and decrypts in-band management requests.

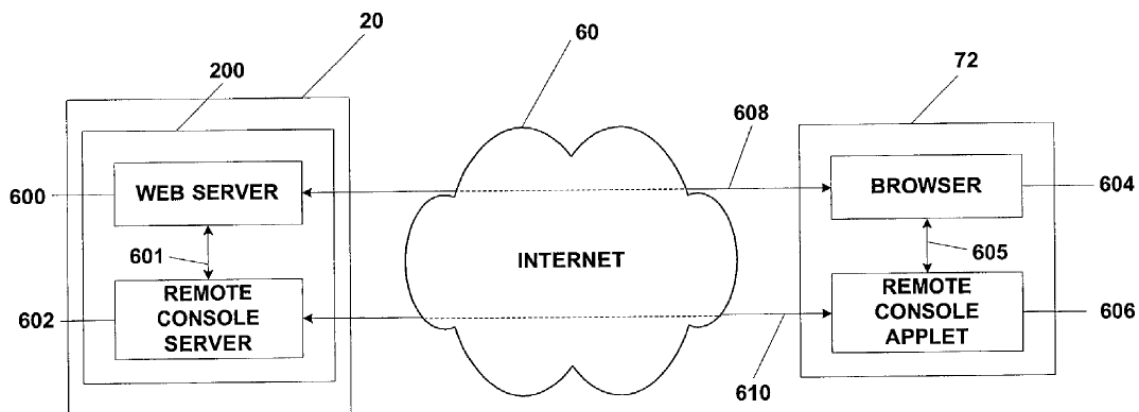


FIG. 3

150. For example, Frantz discloses that the remote console server 602 of Frantz’s remote management controller 200 employs an encryption/decryption algorithm such as RC4 for management request communications with the remote

console applet 606. EX1006, 11:8-26. Accordingly, a POSITA would have found it obvious to configure Neufeld's IOP 156 to decrypt encrypted management requests from the remote management PC 5.

C. Claim 12

151. Neufeld in combination with Frantz and PCI Bridge Spec renders obvious the portions of limitations [12.a], [12.b], [12.d] and [12.g] of claim 12 directed toward encryption and decryption for reasons substantially similar to those discussed in Ground 2 for limitations [1.b], [1.g], [1.h], and [1.i]. All other limitations of claim 12 are obvious for the reasons discussed in Ground 1.

VII. GROUND 3: NEUFELD IN COMBINATION WITH MARTENSON AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC AND MARTENSON RENDERS OBVIOUS CLAIM 2.

152. Claim 1 is obvious over Neufeld alone for the reasons discussed above for Ground 1, and is obvious over Neufeld in combination with Frantz and PCI Bridge Spec for the reasons discussed above for Ground 2.

153. To the extent that claim 2 is also not obvious over these references as applied in Grounds 1 and 2, claim 2 would have been obvious to a POSITA in view of the references in either Ground 1 or 2 in combination with Martenson (EX1011).

154. Martenson, which is directed toward a "System for Network Resource Management," discloses performing remote management of a managed network

device “via a command line interface initiated over a Telnet session to perform management operations [on the managed network device].” EX1011, title and 5:42-52. The use of a command line interface for performing management functions and for other uses was well-known to POSITAs at the time of the 016 patent.

155. A POSITA would therefore have found it an obvious choice to implement Martenson’s command line interface for both in-band and out-of-band management requests in Neufeld’s system to facilitate the use of Neufeld’s system by network administrators. A POSITA would have had a reasonable expectation of success in doing so as this involved nothing more than routine skill.

**VIII. GROUND 4: NEUFELD IN COMBINATION WITH
MACWILLIAMS AND/OR NEUFELD IN COMBINATION WITH
FRANTZ, PCI BRIDGE SPEC AND MACWILLIAMS RENDERS
OBVIOUS CLAIM 3.**

156. Claim 1 is obvious over Neufeld alone for the reasons discussed above for Ground 1, and is obvious over Neufeld in combination with Frantz and Huckins, PCI Bridge Spec and PCF8584 for the reasons discussed above for Ground 2. To the extent that claim 3 is also not obvious over those references as applied in Grounds 1 and 2, claim 3 would have been obvious to a POSITA in view of the references in either Ground 1 or 2 in combination with MacWilliams (EX1012).

157. Neufeld teaches that the implementation details of local bus 166 are a matter of design choice, and MacWilliams teaches that the PCI bus has adequate bandwidth to be used as a main memory bus for low end or entry level systems rather than the type of high performance local bus necessary for maximum processor-cache-memory performance. EX1012, 3:23-44.

158. A POSITA would have recognized that Neufeld's remote management controller 116 is the kind of low-end system that could employ a PCI bus implementation for the local bus 166 and would have found it obvious to do so and to configure Neufeld's ATB 170 as a PCI-PCI bus controller/bridge to allow the PCI implementation of Neufeld's local bus 166 to communicate with Neufeld's PCI bus 172.

159. A POSITA would have been motivated to do so (i) given the implementation of bus 172 as a PCI bus, which indicates that a PCI bus had the bandwidth necessary to support the video graphics controller 114/frame buffer 118/display 4 of Figs. 2 and 3; and (2) because Neufeld's Fig. 3 discloses multiple peripheral I/O devices (e.g., UARTs 174, Ethernet interface 180, USB interface 184) connected to the local bus 166, and a POSITA would have recognized that many existing I/O devices at the time were configured for connection to a PCI bus as shown for example in Fig. 2 of Neufeld with the NIC 110 (which a POSITA would have recognized as commonly being implemented as an Ethernet NIC)

connected to PCI bus 16, and therefore selecting a PCI bus implementation for the local bus 166 would have allowed use of such existing components.

160. A POSITA would have had a reasonable expectation of success as such an implementation was within the skill level of a POSITA and involve using known elements according to their established functions to yield predictable results.

IX. GROUND 5: NEUFELD, ROSSMAN AND RFC1492, OR NEUFELD, FRANTZ, PCI BRIDGE SPEC, ROSSMAN AND RFC1492, RENDER OBVIOUS CLAIMS 7 AND 16

- A. Claim 7. The apparatus of claim 6, wherein the processor is configured to establish a second virtual private network connection with an access control server configured to authenticate the remote administrator, and wherein the processor is configured to receive, via the second established connection, an indication of whether the remote administrator is authorized to administer the network device.**
- B. Claim 16. The method of claim 12, further comprising: establishing, by the management device, a virtual private network connection with an access control server configured to authenticate the remote administrator**

161. Claims 1 and 6 (from which claim 7 depends) and claim 12 (from which claim 16 depends) are obvious over the references discussed above in Grounds 1 and 2. Claims 7 and 16 are obvious over those references as applied in Grounds 1 or 2 in further combination with Rossmann and RFC1492 (EX1013).

162. The use of access servers such as RADIUS servers was very well-known in the art at the time of the '016 patent, and a POSITA would have been

found it obvious and been motivated to configure Neufeld's remote management controller 116/IOP 156 to establish a connection to such an access server in order to use such an access sever in order to simplify management and authentication of multiple remote administrator users and access profiles such as disclosed in Neufeld at Tables 2-4. EX1014, 1-8; EX1013, 1-2.

163. A POSITA would further have found it obvious employ a virtual private network (VPN) connection when connecting to such a RADIUS server as taught by Rossman (EX1015) at 20:35-37 and would have been motivated to do so in order to enhance security. A POSITA would have had a reasonable expectation of success in so doing because access control servers such as RADIUS as well as VPNs were well-known in the art, and their implementations were well within the skill level of a POSITA and involved no more than ordinary skill.

X. GROUND 6: NEUFELD IN COMBINATION WITH SYVANNE AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC, AND SYVANNE RENDER OBVIOUS CLAIM 8

A. Claim 8. The apparatus of claim 1, wherein the apparatus is configured to implement a firewall that restricts traffic received from the second bus.

164. Claim 1 (from which claim 8 depends) is obvious over the references cited above in Grounds 1 and 2 for the reasons stated therein. Claim 8 is obvious over those references as applied in either Grounds 1 or 2 in further combination with Syvanne.

165. 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, ¶¶[0003], [0010], [0029]. Such locally executing software firewalls were well-known to a POSITA and 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.

166. Syvanne discloses the use of a personal firewall on a laptop that will be exposed to a foreign network such as the Internet. EX1016, ¶[0003]. A POSITA would have understood that Neufeld’s remote management controller 116, particularly given that it can be reached in-band via the Network N (i.e., the public Internet), would similarly be exposed to such a foreign network and therefore would have been motivated to implement such a firewall on the IOP 156 of Neufeld’s remote management controller 116 in view of Syvanne’s teaching.

167. 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.

**XI. GROUND 7: NEUFELD IN COMBINATION WITH NTP AAPA
HRASTAR AND/OR NEUFELD IN COMBINATION WITH
FRANTZ, PCI BRIDGE SPEC, NTP AAPA AND HRASTAR
RENDER OBVIOUS CLAIM 14**

**A. Claim 14. The method of claim 12, wherein the one or more
functions are associated with a network time protocol.**

168. Claim 12 (from which claim 14 depends) is obvious over the references cited above in Grounds 1 and 2 for the reasons stated therein. Claim 14 is obvious over those references as applied to claim 12 in either Grounds 1 or 2 in further combination with applicant admitted prior art and Hrastar.

169. Keeping accurate track of time is important to any management and security function in a networked system. The use of the Network Time Protocol (NTP) for maintaining accurate and synchronized clocks on network devices on a network for those purposes was well-known to a POSITA at the time of the '016 patent and it admits as much in the background section:

Maintenance and troubleshooting of network element problems can often be facilitated by having the element maintain an accurate time clock. One way of keeping the clock accurate on an element is to allow the network to set the clock utilizing a protocol such as Network Time Protocol (NTP). If an attacker were able to alter or interfere with NTP, the smooth operation of the network could be interfered with.

EX1001, 3:30-36 ("NTP AAPA"). NTP allows one to answer the very basic question: Did an event, such as the sending of a message, happen before or after an event on another device, and what is the time between two events? NTP is a tool to ensure that there is no perception of time jumping forwards and backwards - all

devices engaged in a particular process agree on what the time is. The protocol has been in ubiquitous use since its introduction in 1985, e.g., in such domains as systems management and security of networked devices, instances being the detection of “man in the middle” attacks, anomaly detection and event reconstruction, the reliable implementation of financial transactions, and for reliable backup processes when a system recovery is necessary.

170. It was also known in the art to allow configuration of network devices to enable or disable the use of an NTP server to synchronize the time on the network device. E.g., Hrastar at 18:32-39 and 20:1-8 (describing configuring NTP using a command line interface). It would have been obvious to a POSITA in view of these disclosures to configure Neufeld’s remote management controller 116 with the ability to configure (e.g., enable and disable) the use of NTP by Neufeld’s managed server, which is a function of the managed server.

171. A POSITA would have been motivated to do so by Neufeld’s disclosure of the desirability of allowing remote management of network device. EX1005, ¶[0015]. A POSITA would have had a reasonable expectation of success as doing so involved no more than routine skill.

XII. GROUND 8: NEUFELD IN COMBINATION WITH RFC1157 AND/OR NEUFELD IN COMBINATION WITH FRANTZ, PCI BRIDGE SPEC AND RFC1157 RENDER OBVIOUS CLAIM 15

A. Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.

172. Claim 12 (from which claim 15 depends) is obvious over the references cited above in Grounds 1 and 2 for the reasons stated therein. Claim 15 is obvious over those references as applied to claim 12 in either Grounds 1 or 2, in further combination with RFC1157 and/or RFC3414.

173. RFC1157 describes the “Simple Network Management Protocol,” or “SNMP” (a.k.a. “SNMPv1”). SNMP is a “simple protocol by which management information for a network element may be inspected or altered by logically remote users.” EX1018, 2. A subsequent version of SNMP, referred to as SNMPv3, was updated to include message level security. EX1021, 1.

174. It would have been obvious to a POSITA to configure Neufeld’s remote management controller 116 to utilize a network management protocol such as SNMP or SNMPv3 as described in RFC1157 and RFC3414 for management requests sent by Neufeld’s remote management PC 5. Such management requests could include requests such as setting a parameter indicating a time until a reboot of the network device as discussed in RFC1157. EX1018, 7. A POSITA would have been motivated to use SNMP or SNMPv3 as they were well-known protocols.

175. A POSITA would have had a reasonable expectation of success as doing so involved nothing more than the use of known components according to their established functions and involved no more than routine skill.

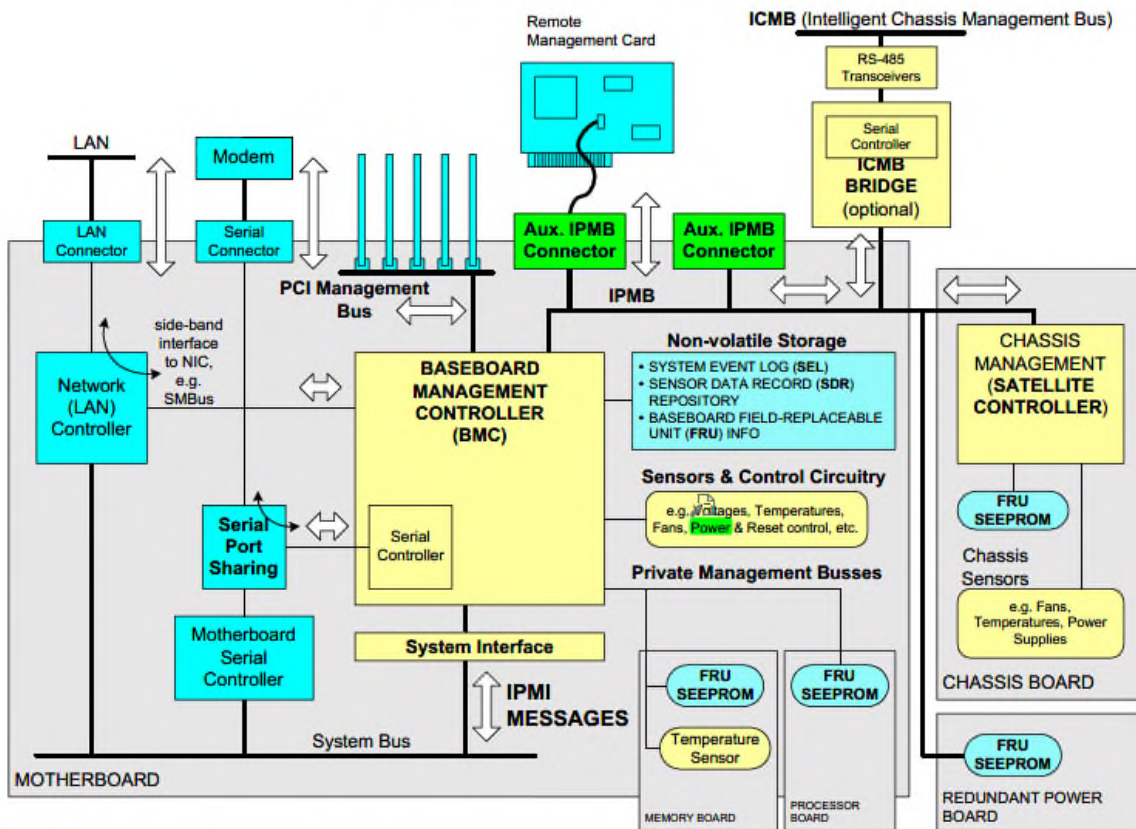
XIII. GROUND 9: IPMI IN COMBINATION WITH FRANTZ AND HUCKINS RENDERS OBVIOUS CLAIMS 1-3, 9, 12, 15 AND 17

176. As discussed in more detail below, IPMI discloses a Baseboard Management Controller, or BMC, that provides remote “Intelligent Platform Management” for a network device. EX1020, 9. Although IPMI does not disclose encryption for in-band management messages received via a LAN at the BMC, it would have been obvious to modify IPMI to encrypt these management messages as taught by Frantz to improve security for the IPMI system for the same reasons discussed above in Ground 2 and explained in further detail below. IPMI also discloses that the BMC receives the in-band management messages sent over the LAN via a sideband interface, but does not include implementation details for this sideband interface. A POSITA would therefore look to prior art references such as Huckins for such implementation details as explained in further detail below.

177. IPMI is a specification that “define[s] standardized, abstracted interfaces to the platform management subsystem.” EX1020, 1. “Platform management” refers to “the monitoring and control functions that are built in to the platform hardware and primarily used for the purposes of monitoring of health of

the system hardware.” *Id.* Fig. 1-2 below is a block diagram showing the main elements of an IPMI implementation:

Figure 1-2, IPMI Block Diagram



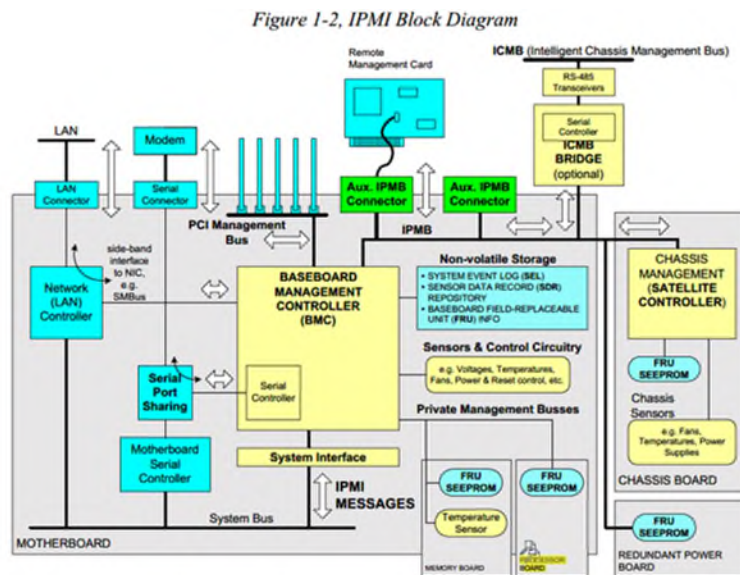
178. The heart of the system is the Baseboard Management Controller, or BMC. The “BMC provides the intelligence behind the intelligent platform management” and (i) manages the interface between the system management software and the platform management hardware, (ii) provides autonomous monitoring, event logging, and recovery control, and (iii) serves as the gateway between system management software and the Intelligent Chassis Management Bus (“ICMB”) and Intelligent Peripheral Management Bus (“ICPB”). EX1020, 9.

179. IPMI provides multiple different interfaces to the platform management system including, as shown above, a modem connected to a serial port a remote management card, the ICMB, ICPB (all corresponding to out-of-band connections), and via the system's LAN connector (an in-band connection). IPMI, 10. Additional prior art I rely on for this ground is discussed below.

A. Claim 1

1. [1.pre] An apparatus, comprising:

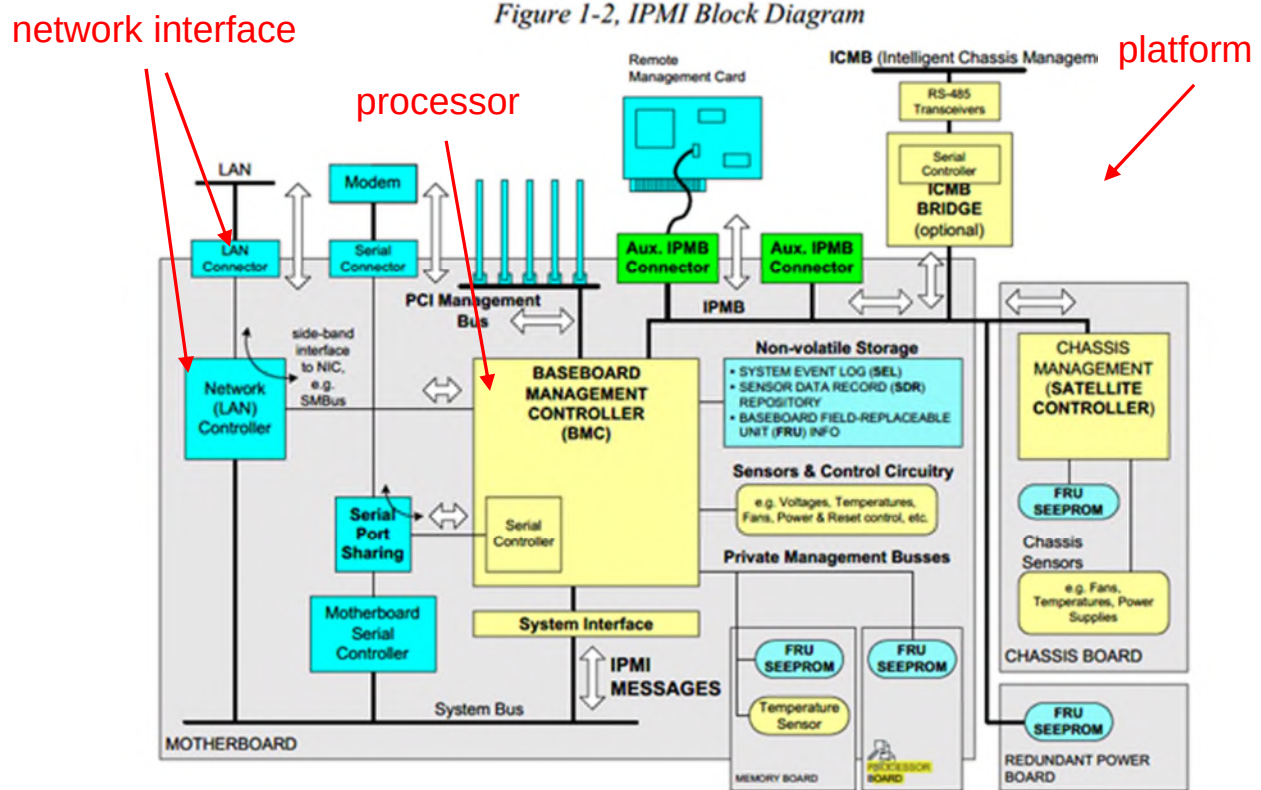
180. To the extent the preamble is limiting, IPMI discloses an apparatus as shown in Figure 1-2 below.



2. [1.a] a processor configured to control one or more functions of a network device having a network interface,

181. IPMI discloses this limitation. IPMI's BMC is the claimed "processor," IPMI's platform is the claimed "network device," and the LAN

Connector and/or the Network (LAN) Controller is the claimed “network interface” as show below in the annotated version of Figure 1-2.



182. IPMI discloses that the BMC is a microcontroller that provides the intelligence behind Intelligent Platform Management. EX1020, 9. A microcontroller is a type of processor. IPMI further discloses that the “BMC manages the interface between system management software and the platform management hardware, provides autonomous monitoring, event logging, and recovery control, and serves as the gateway between system management software and the IPMB and ICMB.” EX1020, 9.

183. With respect to controlling platform functions, IPMI discloses that in an entry-level system, all management functions can be integrated into the BMC.

Id. The BMC can, for example, in response to receipt of an IPMI management message, cause a power off or system reset via manipulation of a watchdog timer.

IPMI, 267 and 274 (chassis control command with value 3h for “hard reset”).

These management functions are examples of control of platform functions.

3. [1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface,

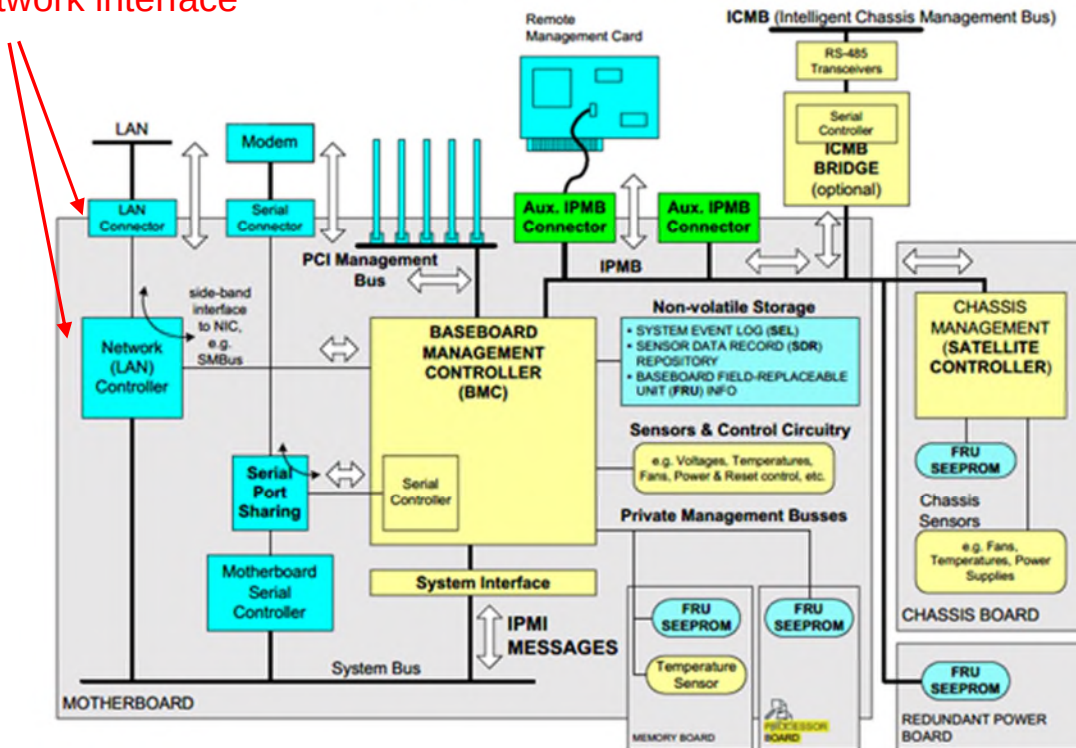
184. IPMI in combination with Frantz renders this limitation obvious.

IPMI’s platform is configured to receive both data requests from normal users and in-band management requests from a remote management system via the LAN

Connector/Network (LAN) Controller of annotate Fig. 1-2:

Figure 1-2, IPMI Block Diagram

network interface



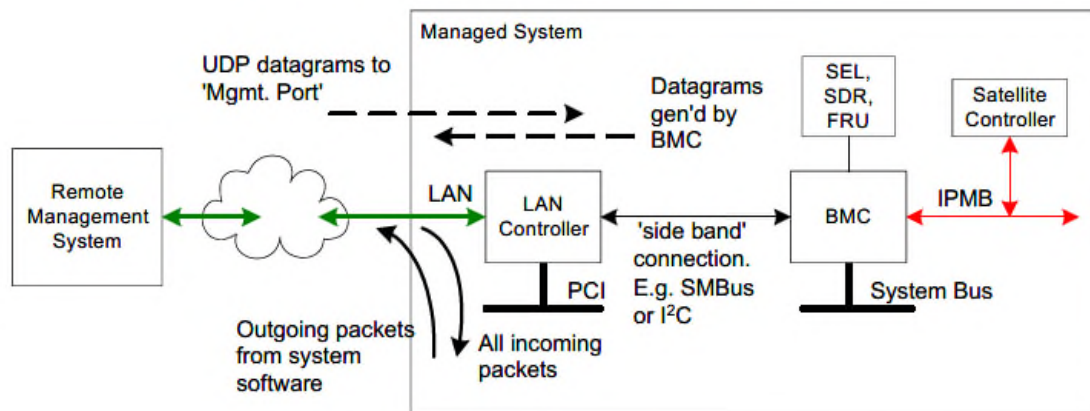
EX1020, 106.

185. IPMI discloses that the IPMI LAN interface will usually be accomplished using a LAN Controller that can be shared for both BMC and system use. *Id.* A POSITA would have recognized or at least have found obvious that the LAN Controller involves receiving and transmitting user data messages to the parts of the platform other than the BMC that handle typical platform tasks for normal users in addition to receiving and transmitting IPMI messages with the BMC.

186. IPMI discloses that the LAN Controller detects UDP (user data protocol) datagrams that include management messages sent to the BMC from a remote management system console over an Ethernet LAN connection and

transfers those UDP datagrams to the BMC via a “sideband interface” as shown in Figure 12-1 below, which illustrates an embedded LAN Controller Implementation. EX1020, 106.

Figure 12-1, Embedded LAN Controller Implementation



187. IPMI discloses that the IPMI management messages sent from the remote management system in the UDP datagrams via the LAN interface conform to an RMCP (Remote Management Control Protocol). EX1020, 107.

188. IPMI further states that the common IPMI messaging protocols do not use encrypted packets, but does not state why encrypted packets are not used, and does not state not to encrypt packets containing IPMI management messages.

IPMI thus does not teach away from encryption for such messages. EX1020, 108 (noting that “Ping/Pong” packets do not include IPMI management messages, and statement that “IPMI messaging does not need to use the secondary port” because IPMI messaging protocols and authentication mechanisms do not use encrypted packets is not a statement that encryption cannot or should not be used).

189. Moreover, IPMI discusses a secure secondary RMCP port (port 298h), which suggests to a POSITA sending encrypted IPMI management message packets. EX1020, 108, 119, 232 and 252. A POSITA would have recognized that encrypting the payloads of packets would improve security, particularly in view of the teaching in Frantz of the desirability of making such in-band communication of management requests secure due to the sensitive nature of such management information and that a hacker's chances of gaining access to secure data on the managed server 2 would be improved if the hacker had access to such management information, and the use of encryption in order to do so. EX1006, 3:19-41; 10:50-63.

190. Additionally, the "Alert Standard Format" ("ASF") specification DSP0114, which defines the interface between a management console and a managed device using RMCP communications, discloses the possibility of designing-in security mechanisms within the RMCP packet structure, which a POSITA would recognize as including encryption in Section 2.4. EX1037, 7.

191. DSP0114 also allows for customization of the data block based on the IANA Enterprise Number in the RMCP packet. EX1037, 19. A POSITA would recognize this as a mechanism that would allow the use of encrypted packet payloads with IPMI messages.

192. The desirability of using encryption further have been apparent to a POSITA in view of the ability to perform highly sensitive operations such as setting user passwords using IPMI commands. EX1020, 227. Accordingly, a POSITA would have found it obvious, and would have been motivated, to encrypt the IPMI message portions (the payload of the RCMP packets, not any headers encapsulating such messages) of at least some of IPMI UDP datagrams.

193. A POSITA would have had a reasonable expectation of success in doing so as encryption technology was well-known to a POSITA and would have involved the application of only routine skill.

4. [1.c] wherein the management requests are received from a remote administrator;

194. IPMI discloses this limitation as IPMI disclose that IPMI management messages are received from an administrator at a remote management system. *See* limitation [1.b] of this Ground 9.

5. [1.d] a first bus; and

195. IPMI discloses this limitation. IPMI discloses a sideband interface between the Network (LAN) Controller and the BMC that is implemented over an I²C bus. EX1020, 9, 106, and annotated versions of Figures 1-2 and 12-1:

Figure 1-2, IPMI Block Diagram

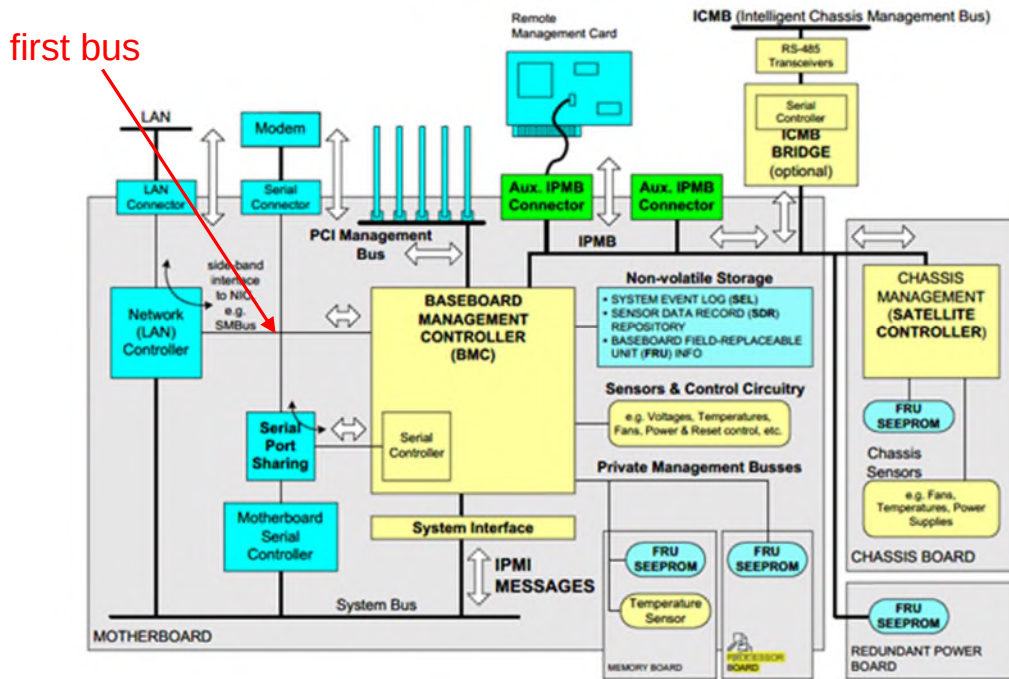
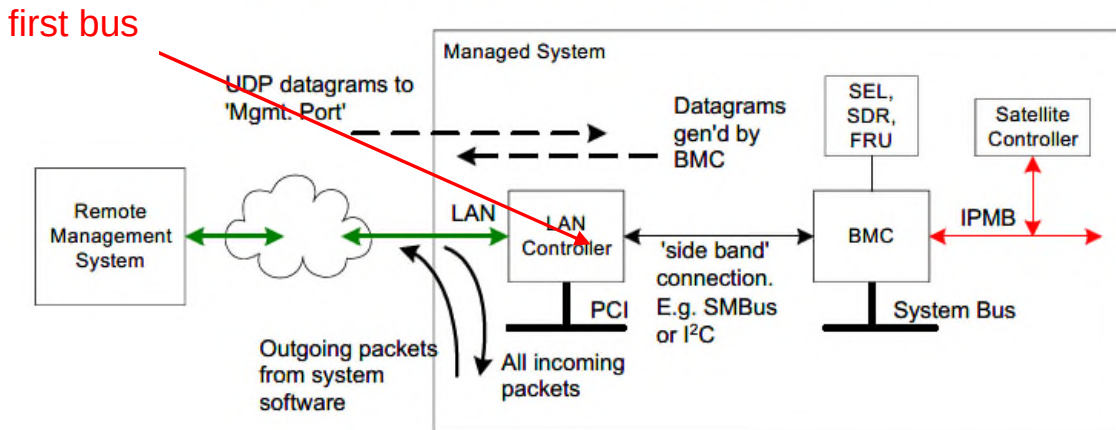


Figure 12-1, Embedded LAN Controller Implementation



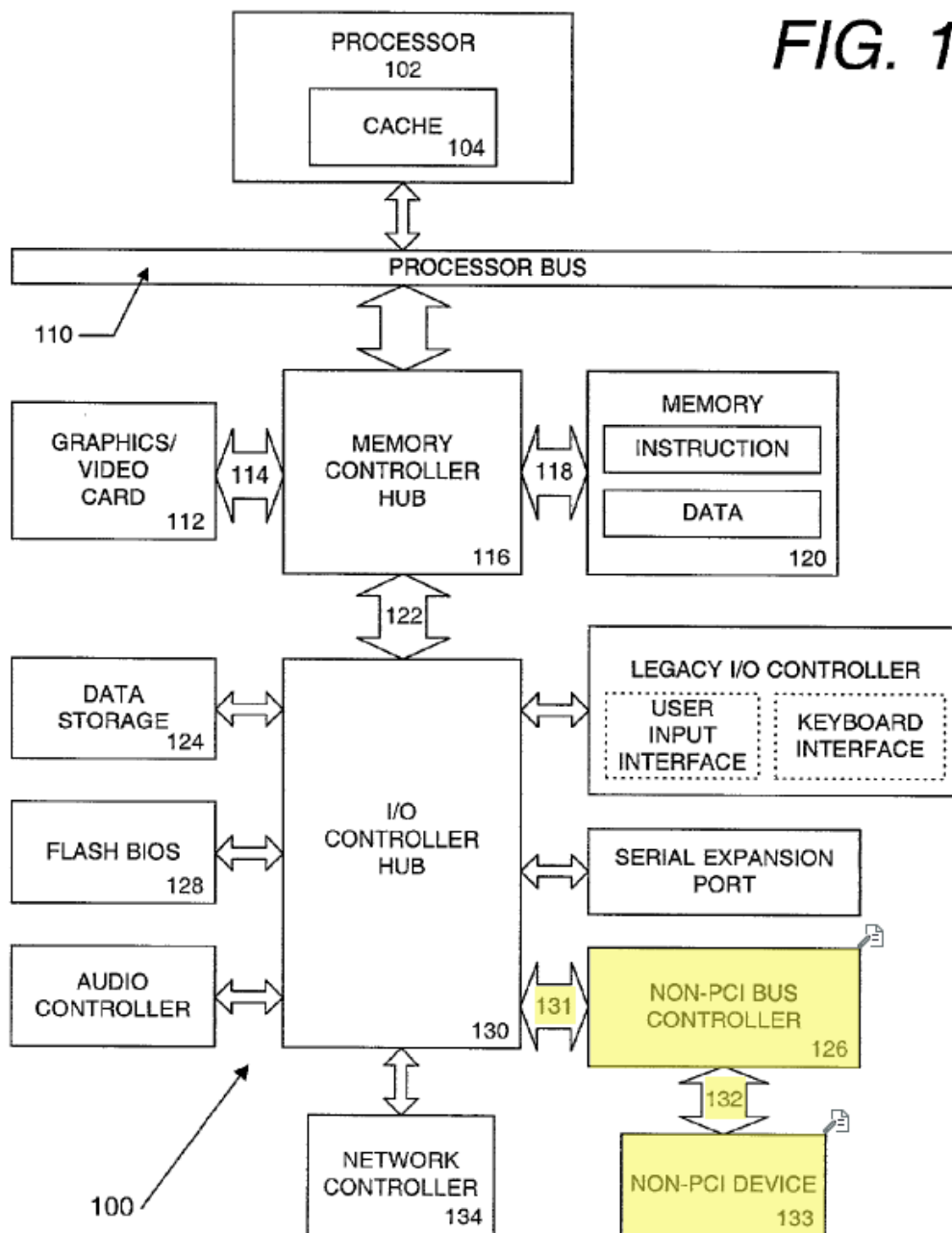
6. [1.e] a bus controller coupled to the processor via the first bus;

196. IPMI in combination with Huckins renders obvious this limitation.

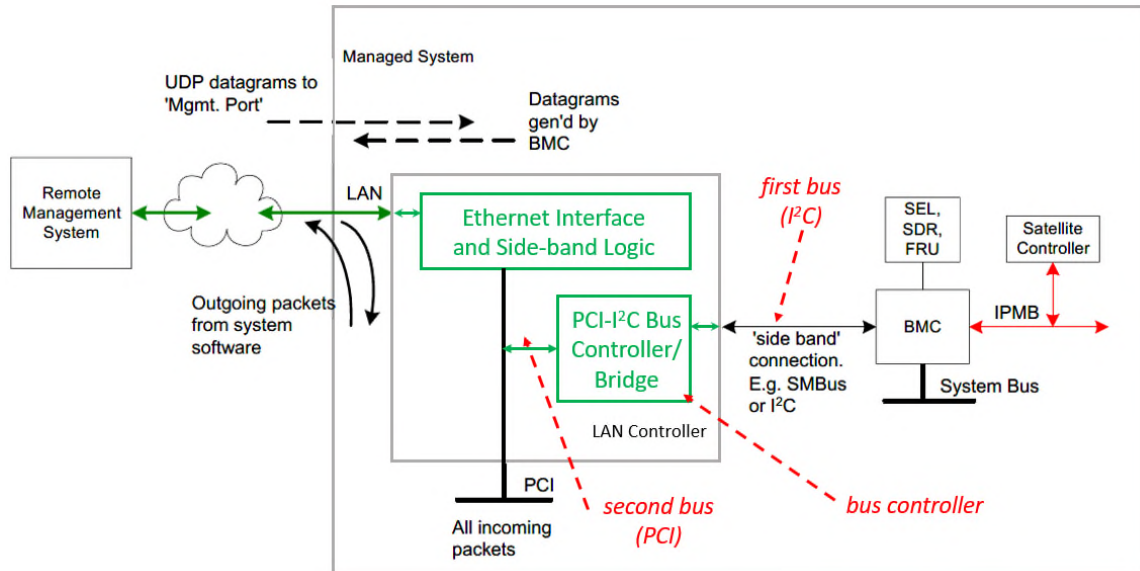
As discussed above, IPMI discloses in Fig. 12-1 a “Network (LAN) Controller” that connects to a PCI bus on the managed platform and that includes a side-band

interface to an I²C bus or SMBus on which in-band IPMI management messages received from a remote management system are sent to the BMC, but does not explain how to implement such a network controller with such a side-band interface. In IPMI Figure 12-1 above, the Network (LAN) Controller must interface to a PCI bus. A POSITA would have recognized that one way to implement a side-band connection using a Network (LAN) Controller that interfaces with a PCI bus is by (1) adding a bridge between the PCI bus to which the Network (LAN) Controller interfaces and the side-band bus, which IPMI identified in Fig. 12-1 as an I²C bus or an SMBus, and (2) configuring the Network (LAN) controller to direct packets addressed to the BMC to the bridge. A POSITA would therefore look to known implementations of a bridge between a PCI bus and an I²C bus or an SMBus.

197. Huckins discloses a “non-PCI bus controller 126” that “can also be referred to as a bus bridge.” EX1007, ¶[0026]. This bus controller-bridge can connect a non-PCI device 133 connected to a non-PCI bus 132 to a system 100 over a PCI bus 131 as illustrated in Figure 1 below (highlighting added). EX1007, ¶[0026]. Huckins discloses that the non-PCI bus may be “one of many types of bus protocols available,” and I²C was a well-known bus type available at the time of the 016 patent. EX1007, ¶[0040].



198. A POSITA would have found it obvious to implement a network controller/side-band interface as described in IPMI by combining Ethernet LAN controller logic with a PCI-I²C bus controller and bridging device of the type described in Huckins as shown in the modified version of Fig. 12-1 below.



199. In this modified version of Figure 12-1, the Network (LAN) Controller is implemented using known Ethernet Interface logic with additional Sideband logic that recognizes UDP datagram packets directed toward the management port which carry IPMI management messages. These packets can be differentiated from packets carrying normal user data based on IP addresses and/or or UDP port numbers. Those packets are transmitted over the PCI bus (the claimed second bus of limitation [1.f]) to a PCI-I²C bus controller-bridge of the type described in Huckins. EX1007, ¶[0026]. The packets are then transmitted from the PCI-I²C bus controller-bridge over the I²C/first bus to the BMC (the claimed processor). EX1007, ¶[0026]. The normal user data packets are transmitted from the Ethernet Logic to the system PCI bus for normal processing by the managed platform.

200. This is a straightforward implementation of a Network (LAN) controller with side-band logic as described in IPMI that would have been obvious to, and well within the skill level of, a POSITA at the time of the 016 patent. A POSITA would have had a reasonable expectation of success in implementing the IPMI Network (LAN) Network (LAN) Controller in this manner.

7. [1.f] wherein the bus controller is also coupled to a second bus of the network device that is distinct from the first bus

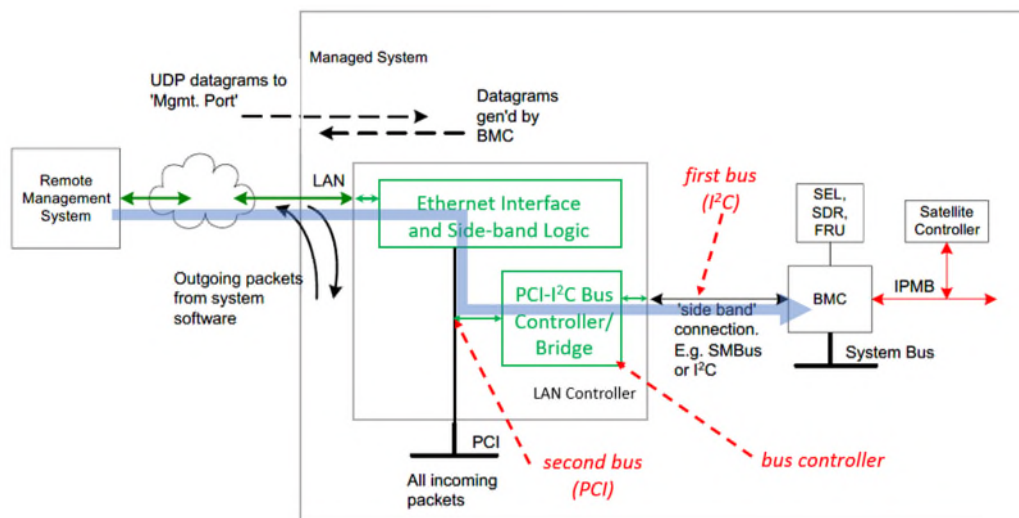
201. IPMI in combination with Huckins renders obvious this limitation. As discussed for limitation [1.e] and illustrated in the modified version of Figure 12-1 above, the PCI-I²C bus controller-bridge in this exemplary implementation is also coupled to a second bus, the PCI bus, which is distinct from the I²C/first bus.

8. [1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus,

202. IPMI in combination with Frantz and Huckins renders obvious this limitation. As discussed above for limitation [1.b] of this Ground 9, IPMI in combination with Frantz renders obvious that encrypted IPMI management messages would be sent from the Remote Management System over the network to the LAN Controller.

203. Additionally, IPMI in combination with Huckins renders obvious that the encrypted IPMI management messages destined for the BMC would be sent from the Ethernet Logic and Side-band Logic to the PCI-I²C bus controller-bridge

via the PCI/second bus as discussed above in connection with limitation [1.e]. The PCI-I²C bus controller-bridge would be configured for receipt of such messages over the PCI bus as discussed in EX1007, ¶[0026]. The path of these management messages from the remote management system to the BMC is illustrated by the blue arrow in the annotated modified version of Fig. 12-1 below.



9. [1.h] and to convey the encrypted form of the management requests to the processor via the first bus;

204. IPMI combined with Frantz and Huckins renders this limitation obvious to a POSITA for the reasons discussed above in connection with limitations [1.b] and [1.e] of this Ground 9.

10. [1.i] wherein the processor is configured to decrypt the encrypted form of the management requests

205. IPMI combined with Frantz and Huckins renders this limitation obvious. As discussed above in connection with limitations [1.b], [1.e] and [1.h]

of this Ground 9, the IPMI-Frantz-Huckins system renders obvious the receipt of in-band encrypted IPMI management messages by the BMC. Frantz discloses, or at least renders obvious to a POSITA, to configure the BMC to decrypt these encrypted messages because without decryption the BMC would not be able to act on them. *See* EX1006, 10:27-39 (discussing decrypting encrypted communications).

11. [1.j] wherein the network device includes a processor configured to facilitate operation of the network device, and

206. IPMI discloses this limitation. IPMI's managed platform includes at least one "main processor" that executes an operating system to facilitate operation of the platform. EX1020, 8 and 9.

12. [1.k] wherein the processor of the apparatus is distinct from the processor included in the network device.

207. IPMI discloses this limitation. The main processor is distinct from the BMC and the BMC can operate when the main processor becomes unavailable. *See* limitations [1.g], [1.h] and [1.j].

B. Claim 2. The apparatus of claim 1, wherein the apparatus is configured to provide a command line interface to the remote administrator, and wherein the apparatus is configured to receive one or more commands to control the one or more functions of the network device.

208. Claim 1 is obvious for the reasons discussed above in this Ground 9. Claim 2 is obvious for the same reasons and because IPMI further discloses the limitations of claim 2. IPMI provides a terminal mode in which ASCII text

commands may be entered in a command line interface at a dumb terminal.

EX1020, 148-149. Examples of ASCII text commands are shown in the excerpt of Table 13-13 below. EX1020, 153.

209. The modified IPMI system discussed above in this ground 9 therefore includes the limitations of claim 2. In any event, including a command line interface in the modified IPMI system would have been obvious to a POSITA because such the provision of such interfaces for creating management messages well-known to a POSITA. .

13.7.8 Terminal Mode ASCII Text Commands

A small number of ASCII-text commands can be delivered while in terminal mode. The following table lists these commands. Commands are CASE SENSITIVE. *Appendix E - Terminal Mode Grammar*, lists the rules for the format of terminal mode input and output for both IPMI messages and text commands. Refer to *Table 13-13, Terminal Mode Examples* for some examples of Terminal Mode text command and IPMI messages.

Table 13-13, Terminal Mode Text Commands

Command Text	Description
SYS PWD -U USERNAME <password>	Used to activate a terminal mode session. USERNAME corresponds to the ASCII text for the username. <password> represents a printable password (up to 16 characters). If <password> is not provided, then a Null password (all binary 0's) is submitted. Passwords are case sensitive. Either the SYS PWD command (or <i>Activate Session</i> IPMI message) must be successfully executed before any command or IPMI messages will be accepted. Note that a modem connection may be automatically dropped if multiple bad passwords are entered.
SYS PWD -N <password>	-N represents a Null username. <password> represents a printable password (up to 16 characters). If <password> is not provided, then a Null password (all binary 0's) is submitted. Passwords are case sensitive. Either the SYS PWD command (or <i>Activate Session</i> IPMI message) must be successfully executed before any command or IPMI messages will be accepted. Note that a modem connection may be automatically dropped if multiple bad passwords are entered.
SYS PWD -X	-X immediately 'logs out' any presently active session. Entering an invalid password with -U or -N will also have the same effect.
SYS TMODE	Used as a 'no-op' confirm that Terminal Mode is active. BMC returns an OK response followed by "TMODE".
SYS SET BOOT XX YY ZZ AA BB	Sets the boot flags to direct a boot to the specified device following the next IPMI command or action initiated reset or power-on. XX...BB are five hex-ASCII bytes for the boot flags parameter in the Boot Options Parameters. See <i>Table 22-12, Boot Option Parameters</i> . Upon receiving this command, the BMC will also set the 'valid bit' in the boot options, and will set all the Boot Initiator Acknowledge data bits to 1b.

C. Claim 3. The apparatus of claim 1, wherein the bus controller is a peripheral component interconnect (PCI) controller.

210. Claim 1 is obvious for the reasons discussed above in this Ground 9.

Claim 3 is obvious for the same reasons and because IPMI combined with Huckins renders obvious the limitations of claim 3. *See* limitation [1.e] in this Ground 9.

See also EX1007, ¶[0026] (“The non-PCI bus controller 126 is capable of receiving and transmitting signals to and from the system 100 on the PCI bus 131.”).

211. A POSITA would recognize the “hardware controller” as being a PCI controller (on its PCI bus connection) and a controller for the non-PCI bus (on its other, non-PCI bus connection), since the hardware controller presents itself to the PCI bus as a PCI controller, thereby allowing non-PCI devices to be accessible on a PCI bus as if they were PCI compliant. “A PCI to non-PCI translator 302 is included in the hardware controller 301. This translator 302 is to translate data, commands, interrupts, and other information between the PCI and non-PCI bus protocols.” EX1007, ¶[0032]; *see also* Huckins at ¶[0030] (“...the PCI system views the hardware controller 201 as a P2P bridge on the PCI bus 212.”). For instance, the hardware controller handles PCI controller functions such as memory mapping, including direct memory mapping (DMA), serving as a PCI memory controller. EX1007, ¶¶[0029][0033]. Additional evidence is found in Huckins at ¶[0018] (discussing functionality of device); ¶[0019] (“Similarly, a hardware

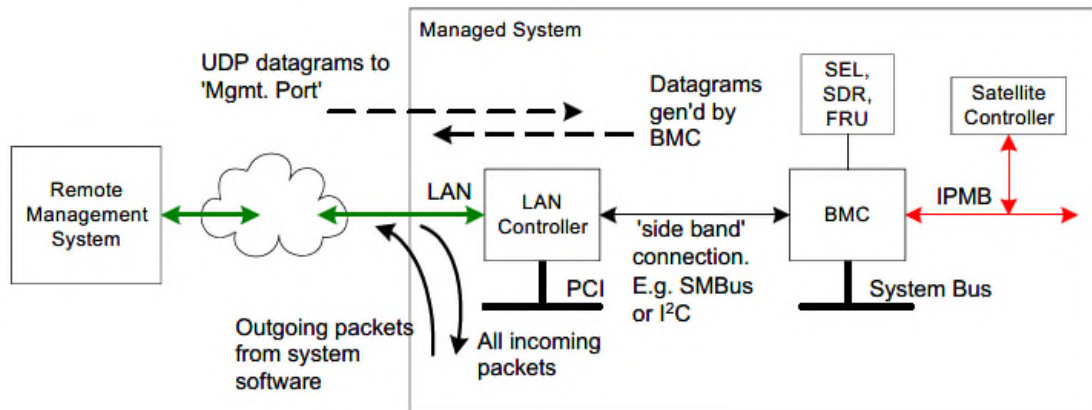
controller has to translate the upstream non-PCI commands into PCI commands to the host. As a result, embodiments of the present invention also manage a mapping between the PCI device identification (ID) and the non-PCI device ID in order to properly route communication traffic to and from the PCI bus”); ¶[0027] (“The hardware controller 201 may also be referred to as a bus bridge as the hardware controller 201 functions as a bridge to communications between a first bus 212 compatible with the PCI protocol and a second bus 213 having a non-PCI compatible protocol.”); ¶[0029] (“The hardware controller 201 of this embodiment also includes a direct memory access (DMA) controller for each I/O device to handle the accesses to the associated memory Space.”) and Fig. 2. Such functionality indicates that Huckins’ device serves as a controller for both the PCI bus and non-PCI bus because its hardware controller 201 engages with the PCI bus as a regular PCI bus controller (see discussion of memory mapping earlier in this paragraph) that mediates PCI protocol access with the devices on the non-PCI bus.

D. Claim 9. The apparatus of claim 1, wherein the apparatus is a component within the network device.

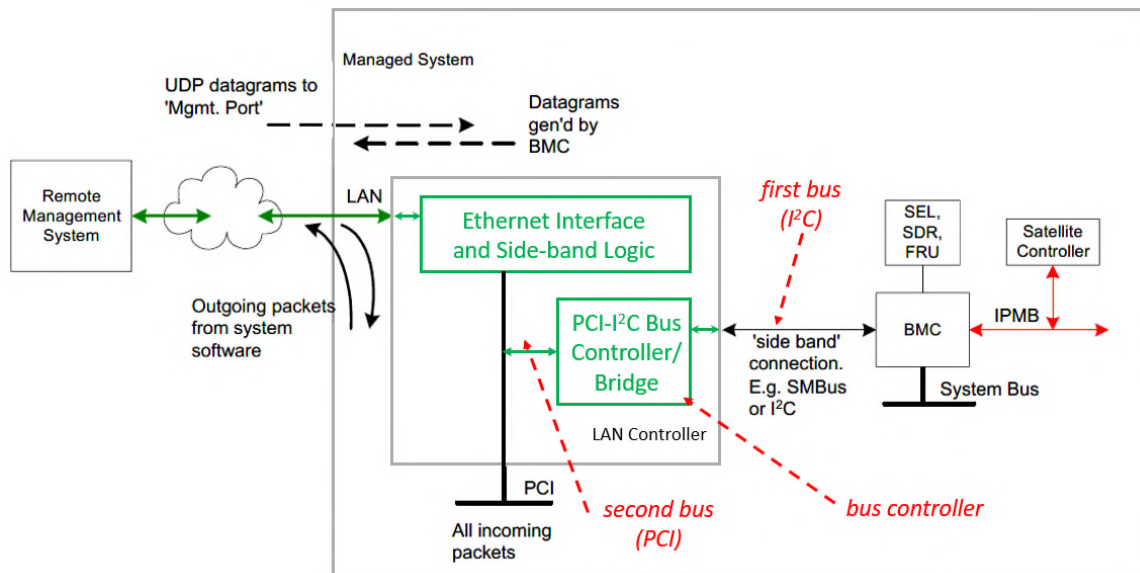
212. IPMI combined with Huckins renders obvious the limitations of claim 1 for the reasons discussed above in this Ground 9, and further renders obvious the limitations of claim 9. The claimed apparatus includes a processor, a first bus, and a bus controller. EX1001, 22:25-45.

213. As discussed above for limitation [1.e], IPMI discloses an embodiment with an *embedded* LAN Controller in Figure 12-1:

Figure 12-1, Embedded LAN Controller Implementation



214. As further discussed above for limitation [1.e], a potential implementation of the apparatus of claim 1 is illustrated below:



215. Because IPMI discloses that the LAN Controller is “embedded” in this implementation, a POSITA would have understood or at least found it obvious

that this LAN Controller along with PCI-I²C bus controller and the I²C bus is embedded in a device with the BMC that is a component of the managed platform device. EX1020, 106.

E. Claim 12

1. [12.pre] A method, comprising:

216. To the extent that the preamble is a limitation, IPMI discloses it. IPMI discloses methods of operation for the BMC on the managed platform. EX1020, 106.

2. [12.a] receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface

217. IPMI discloses this limitation. *See* limitations [1.a], [1.b], [1.e] and [1.g] of Ground 9 (note: the first bus of claim 12 corresponds to the second bus of claim 1).

3. [12.b] wherein the network device received the encrypted form of the management requests and data requests via the network interface,

218. IPMI discloses this limitation. *See* limitation [1.b] of Ground 9 (note: the first bus of claim 12 corresponds to the second bus of claim 1).

4. [12.c] wherein the management requests are from a remote administrator;

219. IPMI discloses this limitation. *See* limitation [1.c] of Ground 9.

5. [12.d] conveying the encrypted form of management requests from the bus controller to a processor of

management device via a second bus of the management device,

220. IPMI discloses this limitation. *See* limitation [1.h] of Ground 9 (note: the second bus of claim 12 corresponds to the first bus of claim 1).

6. [12.e] wherein the network device includes a processor configured to facilitate operation of the network device, and

221. IPMI discloses this limitation. *See* limitation [1.j] of Ground 9.

7. [12.f] wherein the processor of the management device is distinct from the processor included in the network device;

222. IPMI discloses this limitation. *See* limitation [1.k] of Ground 9.

8. [12.g] decrypting, by the processor, the encrypted form of the management requests; and

223. IPMI discloses this limitation. *See* limitation [1.i] of Ground 9.

9. [12.h] controlling, by the processor, one or more functions of the network device according to the management requests.

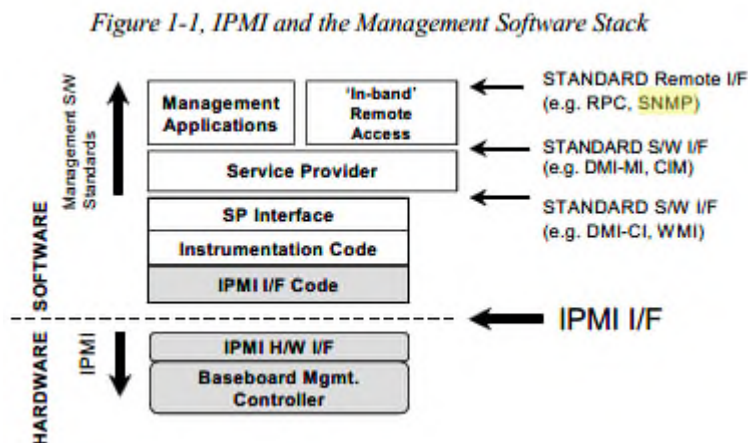
224. To the extent that “the processor” in this limitation refers to “a processor of management device” as recited in claim 12, IPMI discloses it. *See* limitation [1.a] of Ground 9 (discussing BMC controlling functions of managed platform according to IPMI management requests).

225. To the extent that “the processor” in this limitation refers to “a processor configured to facilitate operation of the network device” as recited in claim 12, IPMI discloses it and/or renders it obvious. *See* limitation [1.j] of

Ground 9 (discussing main processor that facilitates operation of the managed platform).

F. Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.

226. Claim 12 (from which claim 15 depends) is obvious for the reasons discussed above in this Ground 9. Claim 15 is obvious for the same reasons and because IPMI discloses or at least renders obvious the limitations of claim 15. IPMI discloses that it is “used best in conjunction with system management software running under the operating system” and that it is “management software neutral” and provides “monitoring and control functions that can be exposed through standard management software interfaces such as DMI, WMI, CIM, **SNMP**, etc.” EX1020, 8 (emphasis added) and Fig. 1-1 (highlighting added):



227. IPMI specifically discloses using SNMP for LAN alerting. EX1020, 16 and 116. In light of these disclosures, it would have at least been obvious to a POSITA to use SNMP (which a POSITA would have recognized as referring to

system network management protocol) in an IPMI system. A POSITA would have been motivated to do so at least because software implementing SNMP was widely available and a POSITA would have been familiar with its implementation.

- G. Claim 17. The method of claim 12, further comprising: receiving, by the management device, additional management requests from the remote administrator via a network interface of the management device, and wherein the additional management requests are not received via the first bus of the network device.**

228. Claim 12 (from which claim 17 depends) is obvious for the reasons discussed above in this Ground 9. Claim 17 is obvious for the same reasons and because IPMI discloses or renders obvious the limitations of claim 17. IPMI discloses out-of-band communications of IPMI management requests via, *e.g.*, a terminal mode connection over a serial interface as discussed above for claim 2 of Ground 9; *see also* EX1020, 15; 122-123 and 148-150.

229. IPMI management request messages received via the serial interface are not received via the first bus or the second bus discussed above for limitations [1.e] and [12.a] because the serial interface is connected to the BMC via a different path represented by the wide blue arrow through the “Serial Port Sharing” box connected to the “Serial Connector” as shown in the of Fig. 1-2 below (annotation added).

Figure 1-2, IPMI Block Diagram

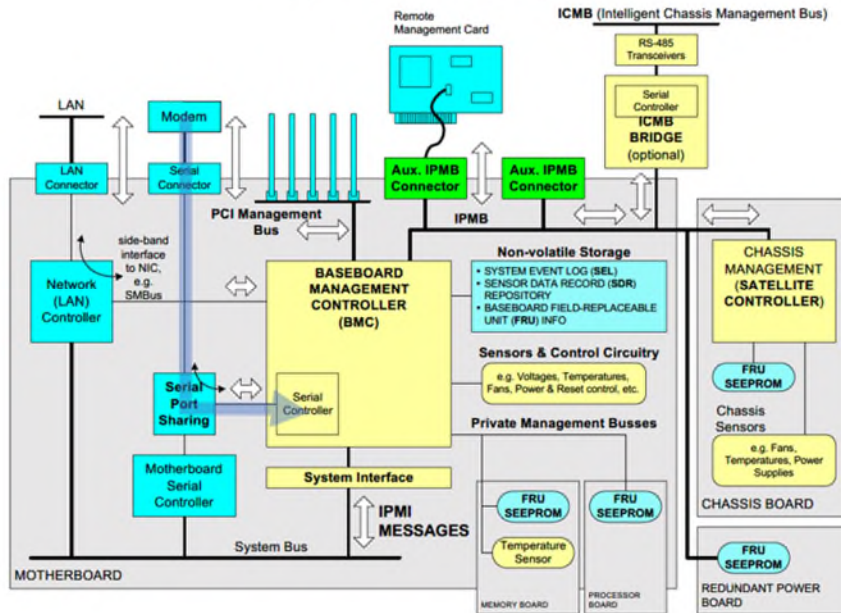
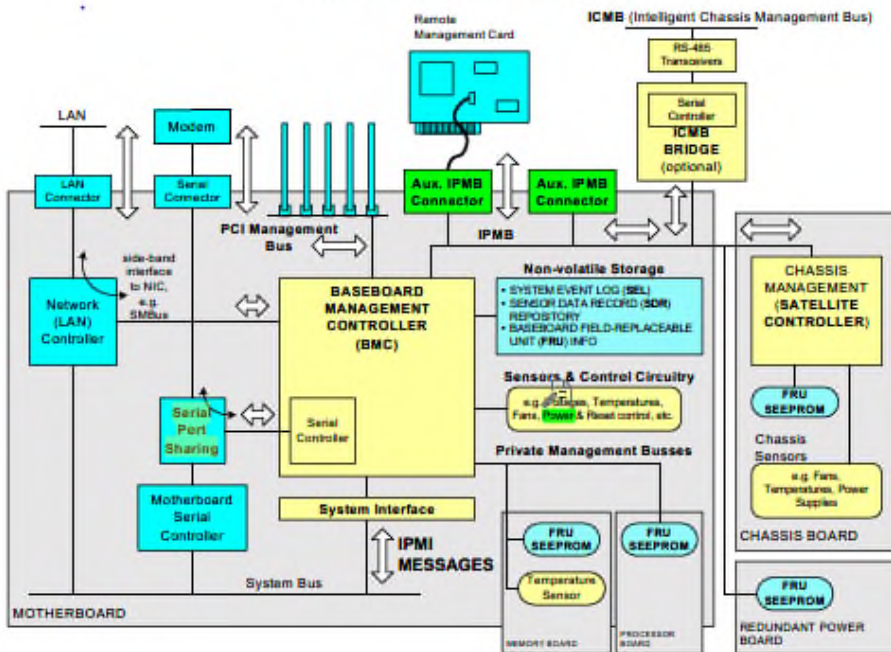


Figure 1-2, IPMI Block Diagram



XIV. GROUND 10: IPMI IN COMBINATION WITH IPMIV2.0 AND HUCKINS RENDERS OBVIOUS CLAIMS 1-3, 9, 12, 15 AND 17

A. Introduction

230. Ground 9 above relies on Frantz in combination with IPMI and Huckins to render obvious claims 1-3, 8, 12 and 17. In that combination, Frantz discloses the limitations in claims 1 and 12 that relate to encryption and decryption of in-band IPMI management messages sent to IPMI's BMC. As an alternative to Ground 9, this Ground 10 relies on IPMIv2.0 rather than Frantz for the limitations of claims 1 and 12 relating to encryption and decryption of in-band IPMI management messages sent to IPMI's BMC. The analysis in this Ground 10 for all other limitations and claims is the same for Ground 9 above and is incorporated here by reference.

231. IPMIv2.0 presented proposed additions to the then-existing IPMI specification, version 1.5 (EX1020), in primarily two areas: an enhanced version of RMCP from IPMI, referred to in IPMIv2.0 as "RMCP+", and SOL ("Serial Over LAN"). EX1023, 6. RMCP+ "is an enhanced protocol for transferring IPMI messages and other type of payloads to an IPMI-based BMC over IP." *Id.* Particularly relevant to Ground 10 is that RMCP+ includes support for encrypting IPMI messages and other payloads using AES-128 (Advanced Encryption Standard, 128 bit) in a CBC (cipher block chaining) mode. EX1023, 6 and 21-22.

232. It would have been obvious to a POSITA to modify IPMI to include the encryption enhancements in IPMIv2.0 in order to improve security for IPMI management messages, including at least IPMI management messages setting user passwords as disclosed in IPMIv2.0. EX1023, 7. A POSITA would have been motivated to do so in order to enhance security of the IPMI BMC and associated managed platform.

233. A POSITA would have had a reasonable expectation of success as doing so involved the exercise of only routine skill and encryption and decryption were well-known to a POSITA.

234. Specific limitations involving encryption are discussed below.

B. Claim 1

1. Limitations [1.b] wherein the network device is configured to receive data requests and an encrypted form of management requests via the network interface,

[1.g] wherein the bus controller is configured to receive the encrypted form of the management requests from the second bus,

[1.h] and to convey the encrypted form of the management requests to the processor via the first bus;

235. IPMIv2.0 in combination with IPMI renders obvious the encryption requirements of these limitations as pertains to in-band IPMI management requests for the reasons discussed in the Introduction to Ground 10.

2. Limitation [1.i] wherein the network device includes a processor configured to facilitate operation of the network device

236. IPMIv2.0 in combination with IPMI renders obvious the decryption of in-band management requests. IPMIv2.0 discloses the decryption of encrypted payload data at 22 and 36. IPMIv2.0, 22, 36. In any event, a POSITA would have found it obvious to configure the BMC to decrypt encrypted IPMI management messages in order for the BMC to be capable of acting on them.

C. Claim 12 A method, comprising:

[12.a] receiving, by a bus controller of a management device, an encrypted form of management requests via a first bus of a network device having a network interface

[12.b] wherein the network device received the encrypted form of the management requests and data requests via the network interface,

[12.c] wherein the management requests are from a remote administrator;

[12.d] conveying the encrypted form of management requests from the bus controller to a processor of management device via a second bus of the management device,

[12.e] wherein the network device includes a processor configured to facilitate operation of the network device, and

[12.f] wherein the processor of the management device is distinct from the processor included in the network device;

[12.g] decrypting, by the processor, the encrypted form of the management requests; and

[12.h] controlling, by the processor, one or more functions of the network device according to the management re-quests.

237. IPMIv2.0 in combination with IPMI renders obvious the portions of limitations [12.a], [12.b], [12.d] and [12.g] of claim 12 directed toward encryption and decryption for reasons substantially similar to those discussed in Ground 10 for limitations [1.b], [1.g], [1.h], and [1.i]. All other limitations of claim 12 are obvious for the reasons discussed in Ground 9.

D. Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.

238. Claim 12 (from which claim 15 depends) is obvious over IPMIv2.0 in combination with IPMI and Huckins for the reasons discussed above in this Ground 10. Claim 15 is obvious for the same reasons discussed above in connections with claim 15 of Ground 9.

E. Claim 17. The method of claim 12, further comprising: receiving, by the management device, additional management requests from the remote administrator via a network interface of the management device, and wherein the additional management requests are not received via the first bus of the network device.

239. Claim 12 (from which claim 17 depends) is obvious over IPMIv2.0 in combination with IPMI and Huckins for the reasons discussed above in this Ground 10. Claim 17 is obvious for the same reasons discussed above in connections with claim 17 of Ground 9.

XV. GROUND 11: IPMI IN COMBINATION WITH FRANTZ, HUCKINS, AND VPN AAPA OR ROSSMAN AND/OR IPMI IN COMBINATION

**WITH IPMIV2.0, HUCKINS, AND VPN AAPA OR ROSSMAN
RENDER OBVIOUS CLAIM 6**

- A. Claim 6. The apparatus of claim 1, wherein the processor is configured to establish a first virtual private network connection with the remote administrator, and wherein the processor is configured to receive the management requests via the first established connection.**

240. Claim 1 from which claim 6 depends is obvious over the references discussed above in Grounds 9 and 10. Those references as applied to claim 1 in combination with VPN AAPA (as defined below) and/or Rossman render obvious claim 6. Virtual Private Networks (VPNs) were well-known in the art at the time of the 016 patent. Indeed, the 016 patent's "Background of the Invention" section admits that firewall/VPN appliances were existing technology which could be used to protect in-band management traffic between a user interface on the managed device and a central location from which the device is managed. EX1001, 3:53-59 ("VPN AAPA").

241. Rossman similarly discloses VPNs as known technology. EX1015, 2:24-28. For all of the reasons discussed in Grounds 9 and 10 for limitation [1.b], it would have been obvious to a POSITA to encrypt in-band IPMI management messages. It would further have been obvious to a POSITA to utilize existing VPN technology as discussed in AAPA and Rossman for such in-band management messages because VPNs provide such encryption and further enhances security for such in-band messages.

XVI. GROUND 12: CLAIMS 7 AND 16

Claim 7. The apparatus of claim 6, wherein the processor is configured to establish a second virtual private network connection with an access control server configured to authenticate the remote administrator, and wherein the processor is configured to receive, via the second established connection, an indication of whether the remote administrator is authorized to administer the network device.

Claim 16. The method of claim 12, further comprising: establishing, by the management device, a virtual private network connection with an access control server configured to authenticate the remote administrator.

242. Claims 1, 6 and 12 are obvious over the references discussed above in Grounds 9-11. Claims 7 and 16 are obvious over those references as applied in Grounds 9-11 in combination with the RFC1492 and/or Rossman cited in Ground 5 above, for similar reasons stated therein.

243. In particular, a POSITA would have been motivated to use a RADIUS access server in order to simplify management and authentication of multiple users and access profiles as described in RFC1492, and would further have been motivated to employ VPN technology to communications with such an access sever in order to ensure security of such communications as taught by Rossman for the reason discussed above in Ground 5.

XVII. GROUND 13: IPMI IN COMBINATION WITH FRANTZ, HUCKINS, AND SYVANNE AND/OR IPMI IN COMBINATION WITH IPMIV2.0, HUCKINS AND SYVANNE

- A. Claim 8. The apparatus of claim 1, wherein the apparatus is configured to implement a firewall that restricts traffic received from the second bus.**

244. Claim 1 (from which claim 8 depends) is obvious over the references discussed above in Grounds 9-10. Claim 8 is obvious over those references as applied in Grounds 9-10 in combination with Syvanne for reasons similar to those discussed in Ground 6. As discussed in Ground 6, IPMI's BMC can be reached in-band via a public network such as the Internet, in the same way as Neufeld's remote management controller 116. A POSITA would therefore have found it obvious to add a locally executing firewall to IPMI's BMC, as taught by Syvanne, "*in addition to or instead of a firewall on an internal network.*" EX1016, ¶¶[0003], [0010], [0029]. A POSITA would have been motivated to do so to improve security of the BMC.

245. 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.

XVIII. GROUND 14: IPMI IN COMBINATION WITH FRANTZ, HUCKINS, NTP AAPA AND HRSTAR AND/OR IPMI IN

**COMBINATION WITH IPMIV2.0, HUCKINS, NTP AAPA AND
HRASTAR RENDER OBVIOUS CLAIM 14**

**A. Claim 14. The method of claim 12, wherein the one or more
functions are associated with a network time protocol.**

246. Claim 12 (from which claim 14 depends) is obvious over the references discussed above in Grounds 9-10. Claim 14 is obvious over those references in combination with NTP AAPA and Hrastar for reasons similar to those discussed in Ground 7 as a POSITA would have recognized that keeping accurate track of time is important for IPMI's managed device as it is for Neufeld's managed server. The use of Network Time Protocol (NTP) for maintaining an accurate clock on network devices on a network for those purposes was well-known to a POSITA at the time of the 016 patent as discussed in the "Background of the Invention" section of the 016 patent. EX1001, 3:30-36. It was also known in the art to allow configuration of network devices to enable or disable the use of an NTP server to synchronize the time on the network device. *E.g.*, EX1017 (Hrastar) at 18:32-39 and 20:1-8 (describing configuring NTP using a command line interface). It would have been obvious to a POSITA in view of these disclosures to configure IPMI's remote management system with the ability to configure (e.g., enable and disable) the use of NTP by IPMI's managed device (which is a function of the managed device) via the BMC. A POSITA would have been motivated to do so in view of the desirability of allowing remote management of network

device. A POSITA would have had a reasonable expectation of success as doing so involved no more than routine skill.

XIX. GROUND 15: IMPI IN COMBINATION WITH FRANTZ, HUCKINS, AND RFC1157 OR RFC3414 AND/OR IMPI IN COMBINATION WITH IPMIV2.0, HUCKINS, AND RFC1157 RENDER OBVIOUS CLAIM 15

A. Claim 15. The method of claim 12, wherein the one or more functions are associated with a network management protocol.

247. Claim 12 (from which claim 15 depends) is obvious over the references discussed above in Grounds 9-10. Claim 15 is obvious over those references in combination with RFC1157 for reasons similar to those discussed in Ground 8. RFC1157 describes the “Simple Network Management Protocol,” or “SNMP” (a.k.a. “SNMPv1”). SNMP is a “simple protocol by which management information for a network element may be inspected or altered by logically remote users.” EX1018, 2. A subsequent version of SNMP, referred to as SNMPv3, was updated to include message level security. EX1021, 1. It would have been obvious to a POSITA to configure IPMI’s BMC to utilize a network management protocol such as SNMP or SNMPv3 as described in RFC1157 and RFC3414 for management requests sent by Neufeld’s remote management PC 5. Such management requests could include requests such as setting a parameter indicating a time until a reboot of the network device as discussed in RFC1157. EX1018, 7. A POSITA would have been motivated to use SNMP or SNMPv3 as they were

well-known and widely-used protocols for which software implementations were available. A POSITA would have had a reasonable expectation of success as doing so involved nothing more than the use of known components according to their established functions and involved no more than routine 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 og numeriske metoder, \$370,000. 1991 – 1993

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 3rd 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 2nd 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 36th 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 13th 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 ω -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 ω ." 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 3rd 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 10th 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 11th 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 18th 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 3rd Workshop on Large Grain Parallelism*, October 1989.
- Sigurd Meldal. "An Abstract Axiomatization of Pointer Types." In *Proceedings of the 22nd 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 21st 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.