University of Technology, Sydney

Event Management of Large Distributed System and Network Management Environments

Antony Gavin James Parsons

Thesis in fulfilment of the degree of Ph.D. (Computing Sciences)

28th July 2006

CERTIFICATE OF AUTHORSHIP/ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any help that I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

Signature of Student

Production Note:
Signature removed prior to publication.

Acknowledgements

This thesis could not have been written without the support of others.

The first person to be "mentioned in dispatches" is my supervisor, Bruce Howarth. Without him this thesis would not have been possible. I would like to thank him for his ideas and suggestions throughout the development of this thesis. I would also like to thank him for all the hours of proof reading while I wrote this thesis, and for continuing to be my supervisor even as he entered retirement. It was Bruce that ruthlessly removed split infinitives, verbalised nouns and inappropriate apostrophes, as well as gently persuading me to shed the excess baggage of an overweight first draft.

I would like to thank the team of Reid Purvis, Jarra Voleynik and Tom Spudic who helped me make the first practical part of the thesis such a success, and I would like to thank Matt Fitzgerald and Nick Tamburro who greatly assisted in subsequent work in the implementation of the thesis.

Naomi Sweeney deserves a special mention for all the countless hours she saved me by helping on the formatting and editing of the thesis.

I would also like to thank my employer, Hewlett-Packard for providing me with the time and resources that I required for this thesis.

Finally, I wish to thank my wife, Alison, as well as my daughters Lizzie and Alex – who both came along during the thesis – for putting up with the inconvenience of having my study slowly grow through the house as the thesis approached completion!

Table of Contents

Acknowledgements iii

Table of Contents iv

List of Figures xi

List of Tables xv

Abstract xvi

1. Introduction 1-1

1.1. Genesis of event management 1-3
- 1.1.1. System Monitoring Focuses on the Network Layer 1-6
- 1.1.2. Network-Level Monitoring doesn't even solve network problems 1-7
- 1.1.3. Summary of what is needed from event management 1-8

1.2. Genesis of this thesis 1-8

1.3. Contribution of this thesis 1-9

1.4. Structure of this thesis 1-10

2. Architectures, Frameworks and Standards 2-1

2.1. Standards based architectures 2-2
- 2.1.1. OSI Management 2-2
- 2.1.2. Telecommunications Management Network 2-5
- 2.1.3. Review of standards 2-12

2.2. Standards 2-13
- 2.2.1. Internet management standards and tools 2-14
- 2.2.2. Simple Network Management Protocol 2-25
- 2.2.3. Simple Network Management Protocol Version 2 2-30
- 2.2.4. Simple Network Management Protocol version 3 2-39
- 2.2.5. Future of Internet management tools 2-44
- 2.2.6. Desktop Management Task Force (DMTF) 2-45

2.3. IT Infrastructure Library (ITIL) 2-46
- 2.3.1. Next generation of ITIL (V3) 2-50

2.4. Architectures 2-52
- 2.4.1. Event Management Architecture 2-52
- 2.4.2. Event Management Applications 2-61
- 2.4.3. Drivers for frameworks 2-62
- 2.4.4. Event Monitoring Framework 2-64
- 2.4.5. Basic Control Framework 2-69
- 2.4.6. Information Distribution Framework 2-74
- 2.4.7. Remote Access Framework 2-75
- 2.4.8. Principles in deploying frameworks 2-76

2.5. Commercial Architectures 2-77
- 2.5.1. Hewlett-Packard OpenView 2-78
- 2.5.2. Computer Associates Unicenter TNG 2-101
- 2.5.3. IBM, Tivoli and TME 10 2-115
- 2.5.4. BMC Patrol 2-132
- 2.5.5. Review of commercial architectures 2-142

3. Tools and Enabling Technologies **3-1**
3.1. Agents 3-2
3.1.1. Simple SNMP Agents 3-4
3.1.2. Autonomous Agents 3-9
3.1.3. Smart Agents 3-21
3.1.4. Pattern Recognition Agents 3-22
3.1.5. Mobile Agents 3-26
3.1.6. Scaling Agents 3-34
3.1.7. Issues with Agents 3-37
3.1.8. Agents in the Intranet Context 3-39
3.2. SQL Databases & Warehouses 3-42
3.2.1. Consolidating Management Databases 3-44
3.2.2. Replication 3-46
3.2.3. Open Database Connectivity (ODBC) 3-47
3.3. Object Orientation 3-49
3.3.1. Object-Orientation in a Management Context 3-50
3.3.2. Object Request Brokers 3-53
3.3.3. Knowledge Representation Using Objects 3-56
3.3.4. Searching and Developing Front-Ends 3-58
3.4. Security – Firewalls 3-59
3.4.1. Event management of firewalls 3-59
3.4.2. Event management through firewalls 3-60
3.4.3. Implementation considerations for event management with firewalls 3-61
3.5. High Availability – Clusters, Resilience, Redundancy 3-62

4. Design of an Event Management Architecture **4-1**
4.1. Terminology 4-2
4.1.1. Event 4-2
4.1.2. Event Management 4-2
4.1.3. Event Processing 4-3
4.1.4. Automation and automated actions 4-3
4.2. Concepts and Issues 4-4
4.2.1. Event flow 4-4
4.2.2. Filtering and forwarding 4-5
4.2.3. Duplication detection and throttling 4-6
4.2.4. Correlation 4-6
4.2.5. Event Synchronisation 4-17
4.2.6. Notification 4-18
4.2.7. Trouble Ticketing 4-18
4.2.8. Escalation 4-19
4.2.9. Maintenance Mode 4-21
4.2.10. Automation 4-22
4.2.11. Drivers for an Event Architecture 4-23
4.3. Overall Architecture 4-31
4.3.1. High Level Architecture 4-31
4.3.2. Data Warehouse Function 4-33
4.3.3. Reporting Function 4-33
4.3.4. Service Desk Function 4-34
4.3.5. Event Handling 4-34

4.4. Classification of Events 4-42
4.4.1. Developing the schema for event classification 4-43
4.4.2. Managing Event Classifications 4-45
4.5. Visualisation of Events 4-46
4.5.1. Common Visualisation Contexts 4-49
4.5.2. Visualisation Media 4-50
4.5.3. Architecture for Visualisation 4-51
4.5.4. Use of Maps for Visualisation 4-52
4.5.5. Synchronised System Views 4-53
4.6. Event Filtering 4-55
4.6.1. Why filter 4-55
4.6.2. How to filter 4-56
4.6.3. Where to filter 4-57
4.6.4. What to filter 4-58
4.6.5. Filtering best practices 4-60
4.7. Event Duplication Detection & Suppression 4-61
4.7.1. Suppressing duplicate events 4-62
4.7.2. Implications of duplicate detection and suppression 4-63
4.7.3. Duplicate detection and throttling best practices 4-66
4.8. Event Correlation 4-67
4.8.1. Correlation best practices 4-68
4.8.2. Implementation considerations 4-70
4.9. Event Notification 4-73
4.9.1. How to notify 4-73
4.9.2. Notification best practices 4-74
4.10. Event Escalation 4-76
4.10.1. Escalation best practices 4-76
4.10.2. Implementation considerations 4-82
4.11. Event Synchronisation 4-83
4.11.1. Event synchronisation best practices 4-85
4.12. Trouble Ticketing 4-86
4.12.1. Trouble ticketing best practices 4-86
4.13. Maintenance Mode 4-89
4.13.1. Maintenance status notification 4-91
4.13.2. Handling events from a system in maintenance mode 4-92
4.13.3. Prolonged maintenance mode 4-94
4.13.4. Network topology considerations 4-95
4.14. Automation 4-96
4.14.1. Automation best practices 4-97
4.14.2. Automation implementation considerations 4-99
4.15. Event Simulation 4-101
4.15.1. Key principles of discrete event simulation 4-101
4.15.2. Mechanisms for time advance 4-103
4.15.3. Mechanisms for describing logic 4-104
4.15.4. Detail of the event execution structure 4-105
4.15.5. Object-oriented simulation 4-106
4.15.6. Implementation Considerations 4-107
4.16. Event Integration 4-108
4.16.1. Levels of Integration 4-108
4.17. Event Management best practices flowchart 4-111

4.18. Detailed Event Management Architecture 4-113
4.19. Design Principles and Drivers 4-116
4.20. Technical Architecture - Details 4-118
4.20.1. Agents 4-118
4.20.2. Mid Level Manager 4-121
4.20.3. Element Managers 4-124
4.20.4. Event Handler 4-127
4.20.5. Event Correlator 4-131
4.20.6. Event Notification and Routing 4-134
4.20.7. Event CMDB 4-138
4.20.8. Event Database(s) 4-141
4.20.9. Portal 4-143
4.20.10. Security 4-145
4.21 Summary 4-147

5. Implementation of an Event Management Architecture 5-1
5.1. Development of Event Management 5-2
5.1.1. Implementation – First Generation 1996-2002 5-3
5.1.2. Implementation – Second Generation 2002-2005 5-10
5.1.3. Implementation – Third Generation 2005-2010 5-12
5.2. Delivery Architecture 5-14
5.2.1. Operations Bridges and ITIL/ITSM 5-15
5.3. Event Management Architecture 5-18
5.3.1. Event Management Architecture – Detailed Technical View 5-20
5.4. Event Message Format 5-21
5.4.1. Background 5-21
5.4.2. Details of event message format 5-22
5.4.3. Implementation of event message format 5-29
5.4.4. Results 5-30
5.5. Event Monitoring Utility (EMU) 5-31
5.5.1. EMU main features 5-32
5.5.2. System components 5-33
5.5.3. Results 5-36
5.6. DECADE 5-39
5.6.1. Event Routing/Correlation 5-41
5.6.2. Event Configuration Database (CMDB) 5-43
5.6.3. Centralised Monitoring Configuration (CMC) Instance 5-44
5.7. SMSPI 5-44
5.7.1. Functional View 5-46
5.7.2. Technical View 5-48
5.7.3. Implementation Views 5-49
5.7.4. Small to Medium Implementation 5-49
5.7.5. Large Implementation 5-50
5.7.6. Air Gapped Implementation 5-51
5.7.7. SMSPI Agent Components 5-51
5.8. Overall Results 5-53

6. The Future 6-1
6.1. What next for event management? 6-3
6.2. Autonomic Computing 6-9

6.3. Neural Computing and Neural Nets 6-10
6.4. Conclusion 6-12

Glossary **Glossary-1**

References **References-1**

A. Details on Standards **A-1**
A.1. OSI Management A-2
A.1.1. OSI Systems Management Overview A-2
A.1.2. Information Areas A-2
A.2. Telecommunications Management Network A-11
A.2.1. TMN Architecture A-11
A.2.2. TMN Functional Architecture A-12
A.2.3. TMN Physical Architecture A-17
A.2.4. Responsibility Model A-18
A.3. Desktop Management Task Force (DMTF) A-22
A.3.1. Architecture A-22
A.3.2. Future of DMTF A-25

B. Patents **B-1**

C. Awards **C-1**
C.1. Background C-2
C.1.1. Press Release 1 C-3
C.1.2. Press Release 2 C-5
C.2. Australian Newspaper article 13th July 1999 C-8
C.2.1. Same article from online archive C-9

D. Requirements for an Operations Management Centre **D-1**
D.1. Technology requirements of HP's Operations Management Centres (OMCs) D-2
D.1.1. Business Principles D-2
D.1.2. Technology Principles D-3
D.1.3. Change Management D-3
D.1.4. Integration External to MSDD D-3
D.1.5. Transition D-4
D.1.6. Abstract D-4
D.2. Industry Drivers D-5
D.3. Executive Summary D-5
D.3.1. IT Complexity Growth D-6
D.3.2. The New IT Environment D-6
D.3.3. Servicing the IT Environment D-8
D.3.4. Why Current Approaches Fail D-10
D.3.5. What's Needed For IT Visibility? D-12
D.4. IT Business Rules and Breakthrough Objectives – by Process D-14
D.4.1. Generic requirements on the framework environment D-14
D.5. Service Design & Management D-18
D.5.1. Service Level Management D-18
D.5.2. Security Management D-19
D.5.3. Availability Management D-20
D.5.4. Capacity Management D-21
D.5.5. Cost Management D-23

D.6. Operations Bridge D-23
D.6.1. Operations Management D-23
D.6.2. Incident Management D-25
D.6.3. Problem Management D-27
D.7. Service Delivery Assurance D-28
D.7.1. Change Management D-28

E. APJ OMCnet Version 2 Infrastructure and Services Design E-1
E.1.1. Background E-4
E.2. Requirements E-5
E.3. Design Overview E-5
E.3.1. Compartments E-5
E.3.2. Services E-10
E.4. Detailed Design E-14
E.4.1. MMI Detailed Design E-14
E.4.2. TCE Core Detailed Design E-16
E.4.3. TCE Shared Detailed Design E-20
E.4.4. Encryption E-21
E.5. Compartment Relationships E-23
E.5.1. MMI-TCE Core E-23
E.5.2. Intranet-TCE Core E-24
E.5.3. MMI-TCE Shared E-25
E.5.4. TCE Core-TCE Shared E-26
E.6. Implementation Considerations E-27
E.7. Radix Integration E-28

F. Practical Examples F-1
F.1. Solution Design Overview F-2
F.2. Mayne Monitoring Solution Detail F-2
F.2.1. Monitoring Server Configuration F-2
F.2.2. NT system monitoring F-3
F.2.3. NT Message Flow F-5
F.2.4. UNIX system monitoring F-5
F.2.5. UNIX Message Flow F-6
F.2.6. Network monitoring F-7
F.3. Unicenter TNG and HP/Compaq OMC F-7
F.4. Unicenter TNG and Optus F-8
F.5. Unicenter TNG Management Stations and OMC F-8
F.6. Unicenter TNG High Availability F-9
F.7. Monitoring Helpdesk (MHD) F-9

G. Details on commercial products used in practical implementation G-1
G.1. Event Management Architecture – Detailed Technical View G-2
G.1.1. Network G-3
G.1.2. NNM Event Correlation G-5
G.1.3. Network OV RAMS for Advanced Router Monitoring G-7
G.1.4. Network Syslog Server G-7
G.1.5. OVPI Reachability G-8
G.2. Server Monitoring G-9
G.2.1. OpenView Operations Server Monitoring G-9
G.2.2. OVO Agent Server Monitoring G-9

G.2.3. HP Systems Insight Manager (SIM) Server Monitoring G-9
G.3. ISEE Systems Hardware Monitoring G-9
G.3.1. HPUX-ITOX Server Monitoring G-9
G.3.2. SMSPI Monitoring and Data Collection G-10
G.3.3. OpenView Performance Agent Server Monitoring G-10
G.3.4. CODA Agent for Server Monitoring G-10
G.4. Application Monitoring G-11
G.4.1. WW_DBMON - database Monitoring G-11
G.4.2. WW_WINMON – Windows server monitoring G-11
G.4.3. Web Server Monitoring G-11
G.4.4. OpenView Internet Services G-11
G.4.5. OpenView Transaction Analyzer G-11
G.5. Correlation G-12
G.5.2. DECADE Event Routing / Reduction G-12
G.6. Ticketing G-12
G.6.1. OpenView Service Desk - Incident Management G-12
G.6.2. OpenView Service Desk - Configuration Management G-13
G.6.3. CMC CIs G-13
G.7. Event Notification G-13
G.7.1. JTOC notification services - Alert notification and workforce management G-13
G.8. Configuration Management G-13
G.8.1. Radia Tool configuration G-13
G.8.2. Centralized Management Configuration G-13

H. IBM Common Event Infrastructure H-1
H.1. Overview H-2
H.2. Architecture H-2
H.2.1. Event selector language H-4
H.3. Driver for Common Base Event Model H-5
H.4. Structure of the Common Base Event H-6
H.5. Drilling down H-7
H.5.1. Core data for a Common Base Event H-8
H.5.2. How components are defined in the Common Base Event model H-9
H.5.3. How situation data is defined in Common Base Events H-10
H.5.4. Remaining situation data in the Common Base Event model H-12
H.5.5. Application of the Common Base Event model H-16
H.6. Summary H-17

I. HP ITSM Operations Management Process I-1
I.1. Structure of ITSM Processes I-2
I.2. Management of IT Infrastructure Events I-3

List of Figures

Figure 1-1	The problem with event management today.	1-2
Figure 1-2	Where this thesis aspires to take event management.	1-3
Figure 2-1	Where TMN fits into a telecommunications network	2-7
Figure 2-2	TMN related recommendations.	2-9
Figure 2-3	The structure of the top of the MIB tree.	2-22
Figure 2-4	The structure of the mgmt (2) subtree.	2-23
Figure 2-5	SNMPv2 Management Hierarchy.	2-33
Figure 2-6	SNMPv3 Architecture.	2-40
Figure 2-7	The overall ITIL process standards framework.	2-47
Figure 2-8	Details of the ITIL Service Support processes.	2-48
Figure 2-9	Details of the ITIL Service Delivery processes.	2-49
Figure 2-10	HP extended version of ITIL called the IT Service Management Reference Model.	2-51
Figure 2-11	In a Centralised Architecture the single event management station is responsible for all management duties on all system & network devices.	2-55
Figure 2-12	In a Hierarchical Architecture the Event Management Station clients perform local management queries and use the Event Management Station server for database storage.	2-58
Figure 2-13	In a Distributed Architecture multiple peer event management systems have complete databases.	2-60
Figure 2-14	The relationship between a event management platform and applications.	2-61
Figure 2-15	Abstract components of an event monitoring framework.	2-65
Figure 2-16	Components of basic control framework.	2-71
Figure 2-17	OpenView Operational Model	2-79
Figure 2-18	HP OpenView distributed management platform services	2-82
Figure 2-19	HP OpenView distributed management infrastructure	2-83
Figure 2-20	Unicenter TNG.	2-103
Figure 2-21	Unicenter-TNG Real World Interface.	2-106
Figure 2-22	Unicenter-TNG Real World Interface.	2-107
Figure 2-23	Unicenter-TNG Real World Interface depicting software and management views of the enterprise.	2-108
Figure 2-24	Unicenter TNG Performance Neugent running on a production system (status is Green).	2-112
Figure 2-25	IBM and Tivoli's plans for TME 10.	2-116
Figure 2-26	TME Architecture.	2-123
Figure 2-27	TEC Architecture	2-128
Figure 2-28	Internal structure of NetView for AIX	2-131
Figure 2-29	Robust functions offer adaptive event management	2-140
Figure 3-1	Taxonomy of agents.	3-3
Figure 3-2	Proxy agent structure.	3-6
Figure 3-3	Functional components of a simply proxy agent	3-8
Figure 3-4	Life-cycle of distributed applications.	3-18
Figure 3-5	Information tree for client/server applications.	3-20
Figure 3-6	Model for pattern matching agents.	3-23

Figure 3-7	Delivery system for mobile agents.	3-27
Figure 3-8	Summary of object-oriented concepts (for class-based objects)	3-52
Figure 3-9	The object request broker model.	3-55
Figure 3-10	Example of knowledge representation of a LAN topology.	3-56
Figure 4-1	Problem and clearing correlation sequence.	4-7
Figure 4-2	Correlation of multiple events reporting the same problem.	4-9
Figure 4-3	Escalation sequence.	4-10
Figure 4-4	Correlation sequence in which secondary event does not require action.	4-13
Figure 4-5	Correlation sequence in which secondary event requires action.	4-14
Figure 4-6	Currently achievable manager-agent scaling models.	4-27
Figure 4-7	High Level Event Management Architecture - Summary View.	4-31
Figure 4-7a	High Level Event Management Architecture - Detailed View.	4-32
Figure 4-8	Event Handling Architecture - Summary View.	4-35
Figure 4-8a	Event Handling Architecture - Detailed View.	4-36
Figure 4-9	Criteria for classifying events.	4-44
Figure 4-10	Mapping events to different viewpoints.	4-47
Figure 4-11	Basic architecture of visualization solutions.	4-51
Figure 4-12	Static time window for peak events.	4-63
Figure 4-13	Multiple time windows for peak event.	4-64
Figure 4-14	Clearing event does not reset the time window.	4-65
Figure 4-15	Clearing event resets time window.	4-66
Figure 4-16	Types of notifications.	4-73
Figure 4-17	Upward and downward event synchronization.	4-84
Figure 4-18	Trouble ticketing process flow.	4-87
Figure 4-19	Mapping severities at the event processor.	4-90
Figure 4-20	Structure of a simulation system	4-102
Figure 4-21	Ways of describing model logic.	4-104
Figure 4-22	Detail of the event approach structure	4-105
Figure 4-23	Inheriting classes in OO software.	4-107
Figure 4-24	The six levels of integration. The higher up, the greater the degree of integration and the lower the frequency of use.	4-109
Figure 4-25	Example of integration between PNV and SMS.	4-110
Figure 4-26	Event processing flowchart.	4-112
Figure 4-27	Detailed event management event flow.	4-114
Figure 4-28	Event Infrastructure.	4-115
Figure 4-29	Event Configuration Database.	4-116
Figure 5-1	Operations Management Centre architecture.	5-4
Figure 5-2	Conceptual event management solution.	5-5
Figure 5-3	Event management solution with commercial and developed tools.	5-6
Figure 5-4	Compaq global OMC model.	5-7
Figure 5-5	Showing the Cisco routers on a typical Unicenter TNG map.	5-9
Figure 5-6	All UNIX systems at one customer on a Unicenter TNG status map.	5-10
Figure 5-7	HP ITSM Reference Model.	5-15
Figure 5-8	HP ITSM reference model with details of individual process areas.	5-16
Figure 5-9	Detailed view of Operations Bridge processes.	5-17
Figure 5-10	Operations Bridges from an event flow (left to right) viewpoint.	5-18
Figure 5-11	New HP event management functional architecture.	5-19
Figure 5-12	New event management technical view.	5-20

Figure 5-13	New extended event management architecture with ISEE and HP System Insight Manager added.	5-21
Figure 5-14	EMU Sample Screen	5-23
Figure 5-15	EMU Architecture.	5-34
Figure 5-16	EMU sample screen.	5-34
Figure 5-17	EMU/TNG Integration.	5-36
Figure 5-18	EMU event display with filters set to display all active events for one customer – OPT (Optus Communications).	5-38
Figure 5-19	Similar filter as previous figure, again with single customer view but this time using basic Internet Explorer browser style view.	5-39
Figure 5-20	DECADE high level architecture.	5-40
Figure 5-21	OpenView to DECADE integration.	5-41
Figure 5-22	DECADE event flow.	5-42
Figure 5-23	How events are handled within DECADE.	5-43
Figure 5-24	SMSPI Functional View.	5-47
Figure 5-25	SMSPI with Auto Recovery Technical View.	5-48
Figure 5-26	Small to Medium customer configuration.	5-50
Figure 5-27	Large customer implementation.	5-50
Figure 5-28	SMSPI agent components.	5-51
Figure 6-1	The future of event management.	6-2
Figure A-1	A managed object	A-3
Figure A-2	Manager-agent concept	A-4
Figure A-3	Functional areas and elementary management functions	A-5
Figure A-4	The CMIP protocols in the OSI Reference Model	A-7
Figure A-5	The flow of a CMIS service request between two CMISE-service-users	A-10
Figure A-6	Relationship between TMN concepts and OSI concepts	A-11
Figure A-7	Relationship between TMN architectures	A-12
Figure A-8	TMN Function Blocks	A-12
Figure A-9	Example of reference points between function blocks	A-13
Figure A-10	Relationship between OSF, NEF and q3	A-14
Figure A-11	Q Adapter Functions	A-15
Figure A-12	Function blocks, components, MCF and DCF	A-17
Figure A-13	Mapping reference points to interfaces	A-18
Figure A-14	TMN Functional hierarchy	A-19
Figure A-15	Example of Value Added Services	A-21
Figure A-16	DMI Architecture.	A-22
Figure A-17	Example of part of a MIF.	A-23
Figure D-1	Today's Complex IT Ecosystem	D-7
Figure D-2	IT Services Operating Against the IT Ecosystem	D-8
Figure D-3	Current Approaches for Gaining IT Visibility	D-10
Figure D-4	IT Resource Alignment Stack	D-12
Figure D-5	Desired approach for gaining IT visibility	D-13
Figure D-6	Representation of IT environment including services, technology and processes	D-14
Figure E-1	APJ Tools Reference Model	E-3
Figure E-2	User View	E-4

Figure E-3	Overall OMCNet 2.0 Compartment Design	E-7
Figure E-4	Authoritative (DNS Core) and Local Caching Name Servers	E-12
Figure E-5	OMCSVC relationship to OMCAPJ	E-13
Figure E-6	OMCNet MMI Options	E-15
Figure E-7	MMI Policy Domain Example	E-16
Figure E-8	TCE Core Detailed Design	E-18
Figure E-9	TCE Core Interior Detail	E-19
Figure E-10	TCE Shared connectivity via POP Router	E-20
Figure E-11	TCE Shared connectivity via MMI	E-21
Figure E-12	OMCNet Encryption over the HPQNet Backbone	E-22
Figure E-13	MMI-TCE Core Compartment Relationship	E-23
Figure E-14	Intranet-TCE Core Compartment Relationship	E-24
Figure E-15	MMI-TCE Shared Compartment Relationship	E-25
Figure E-16	TCE Core-TCE Shared Compartment Relationship	E-26
Figure E-17	OMCnet2 and the Radix network environment	E-28
Figure F-1	Mayne Monitoring infrastructure	F-3
Figure F-2	NT monitoring solution.	F-4
Figure F-3	Unix monitoring solution.	F-6
Figure F-4	Optus Unicenter TNG in the OMC	F-8
Figure F-5	TNG cluster configuration.	F-9
Figure F-6	Event process from TNG to Clarify	F-10
Figure F-7	Response process from Clarify back to TNG	F-11
Figure G-1	New extended event management architecture with ISEE and HP System Insight Manager added.	G-2
Figure H-1	CEI Architecture Overview	H-3
Figure H-2	Class diagram for Common Base Event schema – top level.	H-7
Figure H-3	Class diagram for component information in the Common Base Event schema.	H-9
Figure H-4	Class diagram for situation data in the Common Base Event schema	H-11
Figure H-5	Class diagram for remaining situation data in the Common Base Event schema	H-13
Figure H-6	Class diagram for the entire Common Base Event model	H-15
Figure H-7	How a situation created for a typical log message is translated to Common Base Event	H-17
Figure I-1	HP ITSM process definitions.	I-2
Figure I-2	Management of IT Infrastructure Events.	I-3

List of Tables

Table 2-1	Basis of OSI Management.	2-3
Table 2-2	Supporting client/server requirements for monitoring.	2-66
Table 5-1	EMU Label Summary	5-24
Table 5-2	Customer Examples	5-24
Table 5-3	Business designation.	5-25
Table 5-4	Product Category.	5-26
Table 5-5	Product Type examples for operating system.	5-26
Table 5-6	Product Type examples for hardware.	5-27
Table 5-7	Product type for networks.	5-27
Table 5-8	Product type for security.	5-27
Table 5-9	Managed Object type example.	5-28
Table 5-10	Agent example.	5-28
Table 5-11	Manager example.	5-29
Table 5-12	Scaling definitions.	5-49
Table 5-13	Measure of success of implementation of Event Management components	5-55
Table A-1	Structure of Management Information standards.	A-4
Table A-2	Managed objects standards.	A-4
Table A-3	Systems Management Functions.	A-6
Table A-4	The Management Operation Services.	A-8
Table A-5	CMIS Services and corresponding Data Units.	A-10
Table A-6	Relationship between function blocks	A-15
Table A-7	Relationship between function blocks and building blocks	A-18
Table H-1	CEI Architectural components.	H-4
Table I-1	Detail on Management of IT Infrastructure Events.	I-6

Abstract

Co-ordinated event management across system, network and application environments is a challenging task. The wide diversity of industry and commercial standards, differing business and technical requirements and a huge variety of environments mean there are no simple solutions. This thesis proposes a highly scaleable, flexible and resilient event management architecture that has been applied to the outsourcing activities of HP Services worldwide.

Our solution is based on industry standards such as SNMP and commercial products. It provides a framework for all aspects of event management, including event detection, logging, notification, and correlation. It was initially applied and refined in an outsourcing IT environment, then further developed in larger outsourcing environments. It was developed using a standard solution architecture methodology (known as ITSA) that enabled the partly developed architectures to be continually refined, improved and deployed. The technology aspects of the solution work closely with ITIL event management processes.

To achieve a unified event display and a standardised event message format, all events from all sources are reduced to a standard format that includes the "raw" event information plus business intelligence, called the *business string*, added to the event for display and routing purposes. This extra information identifies the nature of the event and allows filtered displays of events. It is extracted from configuration management extensions added to the standard event management tools. The extended format is flexible enough to handle the different commercial tools.

The first generation of the solution was based on Computer Associates' Unicenter TNG and was called the Event Monitoring Utility (EMU). This was later significantly extended by switching to HP OpenView, and the extra development of further central event management functions, especially event correlation, in a solution called DECADE.

Significant agent extensions were achieved by the creation and deployment of a solution called SMSPI, which included an extended configuration management and policy database, and further event automation.

The extended solution is now deployed across HP Services' entire global outsourced environment. The solution has proven very successful, winning two Computer Associates Software Achievement Awards, including the Grand Prize, and generating two US patents. It will be progressively deployed to several million servers and network devices globally over the next few years.

The work described here is at once self-contained and a basis for on-going development of event management in the face of ever more complex systems, and increasing demands for more detailed event management.