Common Alarm Management (CAM) for Swisscom mobile

Autor(en): **Sellin, Rüdiger**

Objekttyp: **Article**

Zeitschrift: **Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology**

Band (Jahr): **81 (2003)**

Heft 10

PDF erstellt am: **31.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-876689

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Comprehensive Fault Management with CAM

Common Alarm Management (CAM) for Swisscom Mobile

With the still growing competition on the Swiss telecommunications market fault management effectiveness for a mobile operator, for example, is highly critical. Sun Microsystems has implemented a complete new umbrella management system for market leader Swisscom Mobile. CAM provides a service-oriented overview and enables Swisscom to handle all alarm management processes in a reliable and proactive way.

Quite often network management systems and the managed network are extended together. In this respect Swisscom Mobile's Network Operations make no exception. The rise of the Swiss GSM network called NATEL D GSM as the successor of the analogue

RÜDIGER SELLIN

NATEL C is a success story. Therefore, it is no surprise that the traffic on the GSM network is growing as well as the number of services running on NATEL D GSM. Besides the network and traffic growth, a number of new systems (such as the GPRS infrastructure) and networks (such as the PWLAN hotspots) were added over the years. Most of these networks and systems are not maintained on the same management platform. Technical operations related to Fault or Performance Management are a highly critical, complex and demanding task. Due to mobile market saturation and the progressing customer's expectations it is essential to recognise network and service malfunctions without any smoke screens.

Consequently, Swisscom Mobile's Network Operations Centre must be able to perform a proactive service and network management. Here included is a correlation of faults before an unnecessary number of reports are created. To meet these requirements, it is important

- to obtain a quick overview on important alarms,
- to get a service-oriented alarming,
- to access further alarm information to perform a quick alarm triage,
- to have the possibility for fast intervention in case of critical events.

The CAM Project

The Common Alarm Management (CAM) addresses these needs and delivers a centralised, easy, efficient and reliable system for managing today's and tomorrow's wireless infrastructure (fig. 1). Swisscom Mobile decided to bring the extensive operations infrastructure into a structure with three management layers: the basic Network Management (NM Layer) with element and mostly technology-specific OSSs, the Network Management Centre (NMC Layer) area including OSSs with higher, non-vendor-specific OSSs and finally the Service Management (SM Layer). SM deals with management processes like Quality of Service (QoS) Assurance, Performance and Configuration Management (PM, CM), Coverage, leading to an overall Service Level Management (SLM) as shown in figure 1.

There, the red box comprises the centre of CAM, showing the main targets for the CAM development:

- a regional and a centralised monitoring of all active systems and networks of Swisscom Mobile including the ones required for billing data or for specially tailored customer solutions,
- provisioning of a comprehensive management overview to reach fast triages and short intervention times,
- recognition of all faults which effect the customer directly,
- service-oriented alarming with alarm correlation and filtering.

As stated in the introduction above, a number of managed networks (physical lines, transmission systems, network elements like switches, registers and antennas), managing IT systems (mainly work station computers) and additional infrastructure (security systems, storage, some PCs etc.) are necessary to operate a nation wide mobile network like NATEL D GSM. After an intensive evaluation process, Swisscom Mobile selected Sun Microsystems who had been already the OSS HW supplier right from the beginning and already knew the management environment. In addition, Sun had already had experience in implementing complex OSS systems, so this choice promised a lower risk at a lower realisation time. Sun itself selected Micromuse's Product Netcool from its own Management SW portfolio. Figure 2 shows every partner and his role in the CAM project.

As a next step, Sun Microsystems has analysed the requirements and prepared interviews with specialists from the different network areas. The following networks were integrated in the CAM:

- OSS FM (Ericssons Fault Management Element Manager for the NATEL D GSM network)
- Tellabs MartisDXX (DXX network)
- Repeater from the suppliers Allgon, Mikom and Comlab
- VAS Platform (BigBrother) for Value Added Services (Voice Mailbox, SMS etc.)

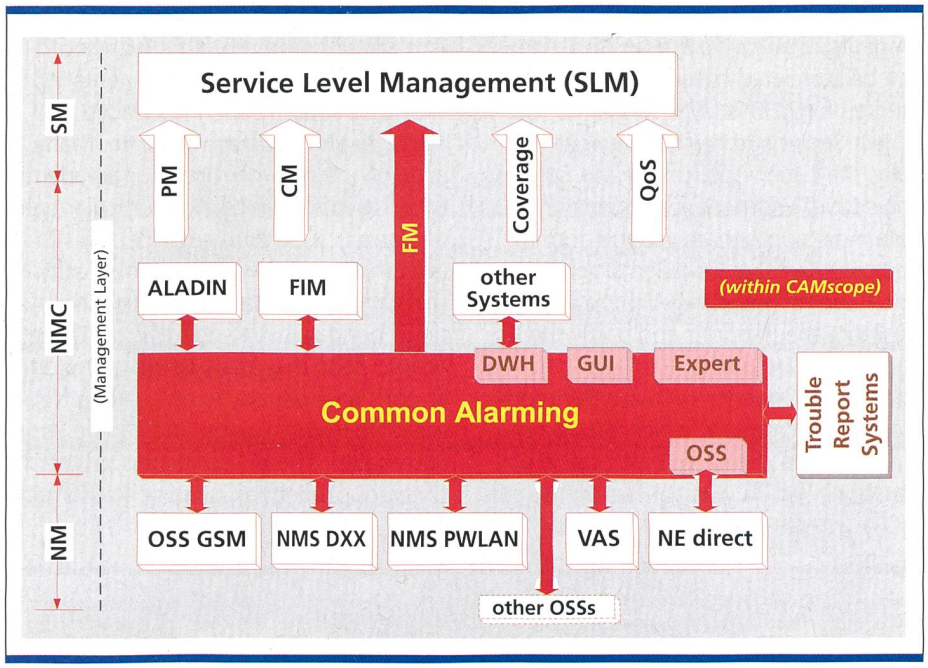

Fig. 1. Scope of CAM.

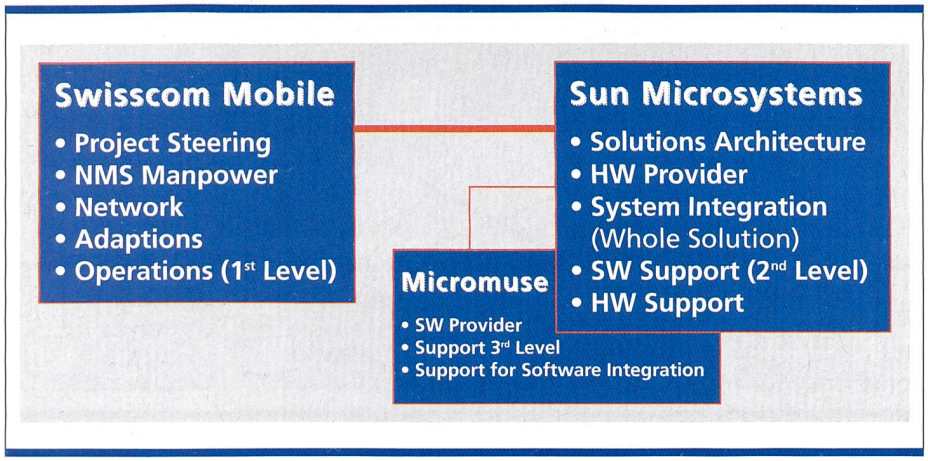

Fig. 2. Project Organisation.

- Cisco Works for PWLAN, for the internal O&M intranet (a kind of management network) and for the GPRS Network
- Siemens NetManager for SS7 Signalling at the STP Network
- Netcool end-to-end test system for GPRS and WAP Services
- SOG (Service Order Gateway)
- BGW (Billing Order Gateway)
- Firewall Management (NetScreen Global Pro)
- ATM NMS 5620 Node Manager
- NMS to Control and Monitor the OSS Computer Systems (BMC Patrol)
- ADC Metrica for PM Thresholds
- OSA Parlay System (Aepona)

The CAM supports comprehensive fault management capabilities and delivers a value-added solution for the technical requirements identified in managing all these different networks and systems. The CAM solution is designed to provide a highly scalable and easy-to-use fault management platform. Sun Microsystems sees the following benefits for Swisscom Mobile by introducing CAM:

- Event Reduction: Reduces the number of events that network operators have to deal with and allows them to be more productive and focused on the problems that affect the network.
- Reduced Effort: The unified method of presentation reduces training needs and allows operators to be deployed in a more flexible manner across technologies, which reduces the overall effort.
- Fault Prioritisation: Leverages a network operator's existing data and information stores in the handling of network and service problems based on services or customers affected, and makes the whole network operations more effective in dealing with the issues that really matter.
- Reduced Mean-Time-to-Repair (MTR): The CAM reduces the MTR on network problems by minimising the time required to locate the source of problems. Through automatic diagnostics the operator can scale back on operations resources.
- Enables Managed Services: As an optional extension, CAM could provide Swisscom Mobile with the ability to deliver managed services required in the new mobile data services environment through end-to-end management and testing of Internet and WAP services.

Due to its modularity and scalability, new functions (like the Service Level Management) and networks can be integrated easily into the CAM solution later.

HW and SW Architecture

According to figure 3, the basic HW delivered by Sun comprises six servers with different functions and is designed for a high operations security. The CAM HW Architecture is based on a production and a test environment. As the central HW instance of the latter, the Test Server makes it possible to test a new functionality or changed rules in the real environment without disturbing or endangering it. The Test Server even receives alarms from productive OSSs via the gateway that creates a „real-life" impression of the current situation in the network. All other servers are part of the production environment. The Primary Server forms its centre and provides the basic CAM functions whereas the Backup Server takes over these functions in case of a Primary Server failure. The switching from the Primary to the Backup Server happens practically without any interruption for the user. In this case, a dialogue box appears on the screen and points the user to the HW failure. The Archive Server is responsible for the storage of historical data and runs an Oracle database (DB) internally. (Note: The Object Server (OS) within the Primary and the Backup Server employs a RAM DB for the storage of alarms.) The Probe Server contends the Probes for the systems for which no appropriate Probes are available and therefore could not be installed on them directly. Finally, the Recovery

Server stores flash-image-data for the fast recovery of the system. The Recovery Server has been integrated into the already existing Backup-System.
Swisscom Mobile uses the following Sun HW (as indicated in fig. 3):
- Sun V480 (one per Primary, Backup and Recovery Object Server)
- Sun V120 (Probe Server)
- Sun V480 and Sun StorEdge 3310 (Archive Server)
- Sun V280R and Sun StorEdge S1 (Recovery Server)
- Sun V280R (Test Server)

The Object Server is fail save with the application SW from Netcool. All CAM systems are linked via „Recovery-Net" to the Recovery Server, which supports the fast recovery of all servers using a flash-image mechanism. The Sun V480 come with 10/100/1000 Mb, the V280R with 10/100 Mb Ethernet on board. Swisscom Mobile uses the existing O&M intranet for all communication possibilities as for example „Data Recovery" (for the traffic of the recovery mechanism based on flash-images), „Webtop and Desktop GUI's" (display data traffic), „Probe Connection" (traffic coming from Probe Server or direct adapted Probes) or the „Archive-Info" (traffic from and to the Archive Server).
The SW architecture for CAM is based up on Netcool from Microbes. The basic idea behind Netcool is to gather management information as close to the managed system as possible. For this purpose, so-called „Probes" are installed on the vendor-specific NM OSSs from where the relevant information is collected directly. If this is not possible, the Probe Server plays this role for the Object Server and collects the management information on the target system. If necessary (i.e. if a Probe cannot be installed), the Probe Server uses the Simple Network Management Protocol (SNMP) and polls the appropriate SNMP Agents (SNMP traps). The Object Server is divided in a Core Server (in fig. 4 „P_Object Server") and a Display Server („P_Display Obj Server"). The Webtop as the graphical interface exists on the Primary Server only (non-redundant).
The layered structure of the CAM system (fig. 5) comprises the Data Collection, the Data Correlation and the Display Layer. The Data Collection Layer is responsible for gathering all data relevant for the alarm management and contains the Probe and the Probe Server. In the Data Correlation Layer these data are aggregated in a real-time repository and can be correlated based on the implemented logic. This layer comprises the Object Server and the Impact Server. Finally, the Client Application and Business Logic Layer visualises live and historical data in an appropriate variable format and can therefore be called Display Layer too. Consequently, the Webtop, the Desktop, the Reporter and partly the Impact Server are part of this layer.
The Virtual Operator (VO) is a SW module from Micromuse, which allows running routines in case of particular alarm situations (fig. 4). It is able to launch predefined scripts based on defined events. This allows communication with southbound applications or components in case they support open interfaces through which to communicate. Many actions of a network operator are identical for every instance of a particular type of alarm (i. e. to ping a device). This requires the operator to perform exactly the same action sometimes thousands of times per day just to quit alarms. These actions consume many hours of the operator's time per day in an average Network Operation Centre and can be easily automated. The VO solves this problem of tedious repetition by taking automatic

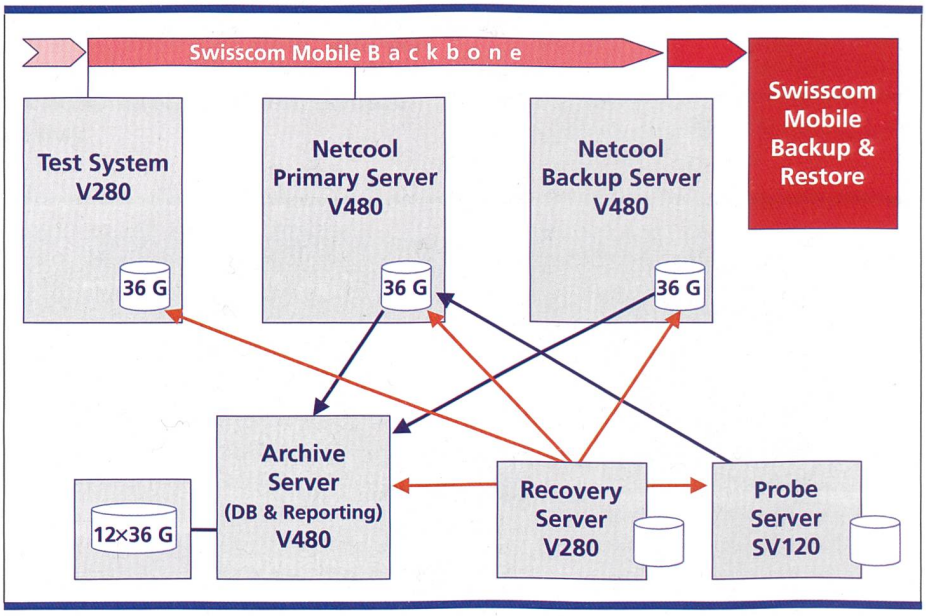

Fig. 3. HW Architecture.

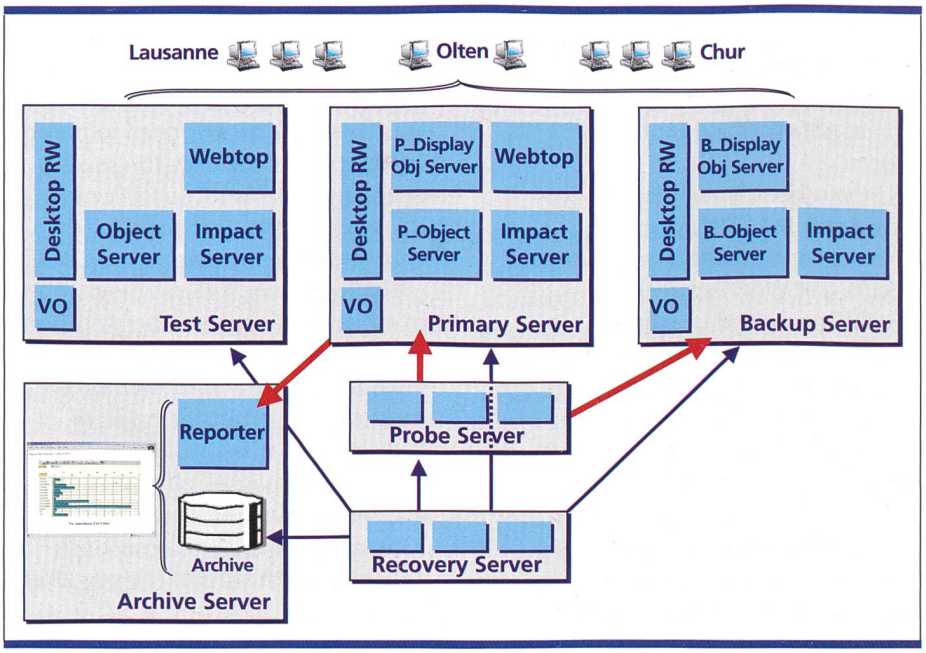

Fig. 4. SW Architecture.

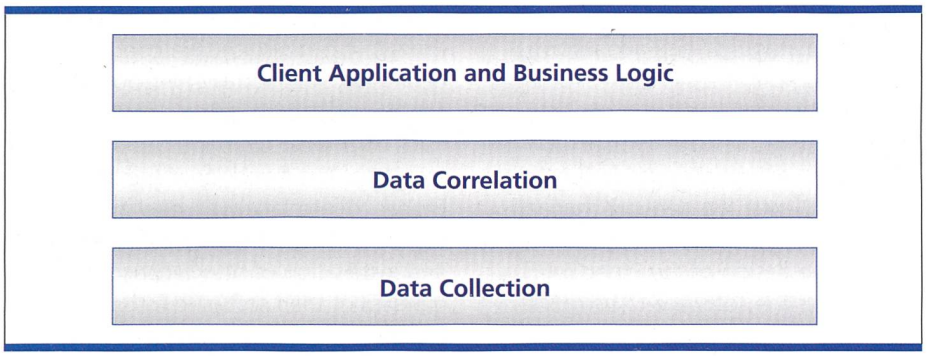

Fig. 5. Layered Architecture.

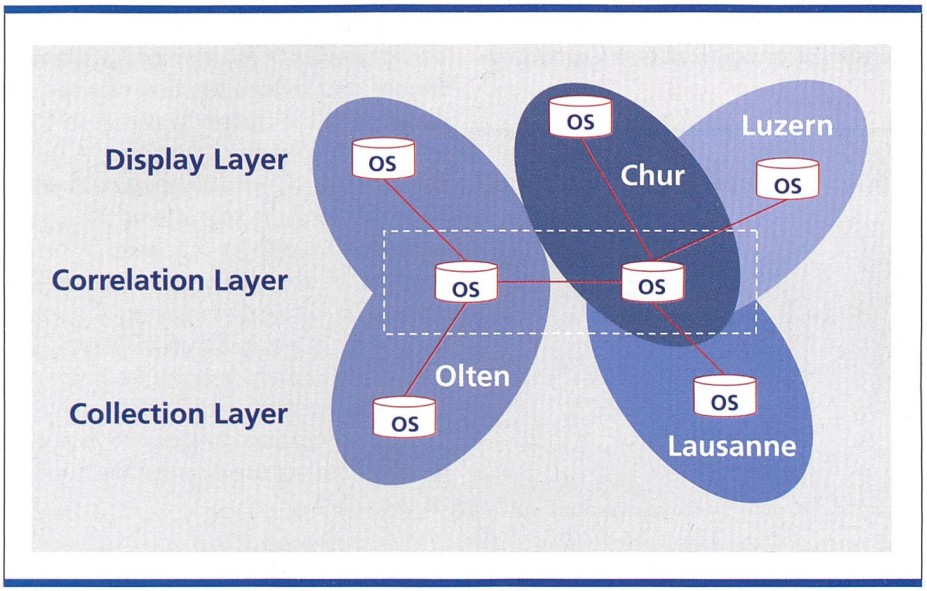

Fig. 6. Scalable Architecture.

action on events which it has been programmed to handle, the highly appreciated effect being that the operator spends his spare time on tasks that cannot be automated so easily. Such tasks can be performed with the help of a SW routine instead. The Reporter is used to feed the processed information into an Oracle RDBMS. Because of the usage of Impact and its event enrichment capabilities, the events are written with well-consolidated and enriched data to the archive database. This process assists the report definition and provides the basic functionality of a Data Warehouse. The Reporter application complements the real-time focus of the Netcool application by capturing, analysing, and presenting event data generated over various timeframes.

Data Collection and Correlation

The Netcool architecture is highly scalable. As in comparable installations, the events in the management environment of Swisscom Mobile allow alarm filtering and de-duplication (that is the avoidance of alarm duplication for example through filtering of already reported and therefore known alarms). The system power based on the event rates reported for the CAM is:

- 500 events per second for a period of 1–3 seconds
- 200 events per second sustained over a period of 60–180 seconds
- 200 000 events per day approximately on average per day.

The Probes attached to the managed systems parse, format, filter and forward the events directly to the Object Server as in the case of Swisscom Mobile or alternatively to a collection of Object Servers. The expected event rate is 2.3 per second based on the reported 200 000 on average per day by Swisscom Mobile. This will grow in the future as new applications and services are bolted on the network. Therefore, Sun designed the architecture so that it can support future additional components. The Probes forward the events to the Object Server (located within both, the Primary and the Backup Server).

The number of required Object Servers in the future depends on the number of connections to the Object Server, the event rate and the number of resident events into the Object Server. Sun recommends the following numbers against those metrics and with the role played by those Object Servers for optimal performance:

- 50 Probe connections max per Object Server (no desktops)
- 300 events per second sustained on average (assuming that there is no duplication of events)
- 20 000 resident events on average

These figures were checked against the number of events collected, as well as the number of resident events. Given an increasing number of events with the introduction of further networks or new services, an increasing number of Probes and higher estimated event rates, probably more than one Object Server will be needed for events collection or displaying.

The Object Server data repository is the heart of the Common Alarm System where all events are collected initially in real-time in a standardised format. It is a real-time, memory resident, active database server, which consolidates, associates, and normalises information from the Probes by assigning information to tables and fields. Repeated information is automatically de-duplicated using a configurable identifier information. All application functions are active threads running within the database engine. The Object Server turns information such as faults, alarms, warning and datagram messages into objects that can be easily manipulated by operator-driven correlation, associations and filters. This also allows the creation of logical service groups, which can include end-to-end applications, departments or business units. This process produces accessible, meaningful information on the status of any component or group within the business process chain.

Netcool Probes collect the plain events. Probes are software based collectors, kinds of lightweight pieces of code that push information coming from network devices, systems or any other source into the Object Server. Essentially, they are passive software listeners that identify and collect information via a large variety of interfaces or technologies like SNMP,

TL1, CORBA, Q3, Syslog, Logfile, API and others. The information is normalised into a common format. Using a connection-oriented transport protocol, the data is then pushed into the Object Server. These Probes enable operators to collect and interpret information from disparate network management consoles, transmission infrastructure, telephony devices, data networks, LANs and WANs, and applications. More than 300 pre-built Netcool Probes allow the monitoring of practically any network device or system.

The Probes collect syslog messages, trap receipts and other heavily requested applications, using rules and lookup tables to define, categorise and add information to events. They also have standard system properties that tell them how and where to store the data. Probes have different supersets of executable functions depending upon the network management platform for which they are designed. The design of the Probe mechanism allows the software to be quickly installed and immediately operational. It is based on the exclusive management paradigm, which enables the Probes to recognise all relevant information from the managed system without requiring the user to configure all fault/event/data-gram information. The SW design allows users to customise the Netcool Probe's behaviour. Additionally, Netcool Probes can be configured, using a sophisticated rules engine, to filter and translate certain data. The flexibility of the Netcool Probes to interface with new and existing technologies enables the adoption and installation of new technologies, regardless of their software foundation.

It is possible to build different functional layers with a Netcool solution (as in fig. 5) or to adapt the solution architecture to technology, organisational or geographical criteria instead (as in fig. 6). Within the CAM solution of Swisscom Mobile, the layered solution was selected with the option to switch to the latter possibility at a later point. A distribution of the Object Server (OS) is possible should some management processes have to be managed by another team at another locality. (Note: Today, the whole CAM system – except some Probes – is installed in Olten where the Primary and the Backup Server are located in different rooms. The other locations mentioned in figure 6 should reflect the possible distribution of the OSs.)

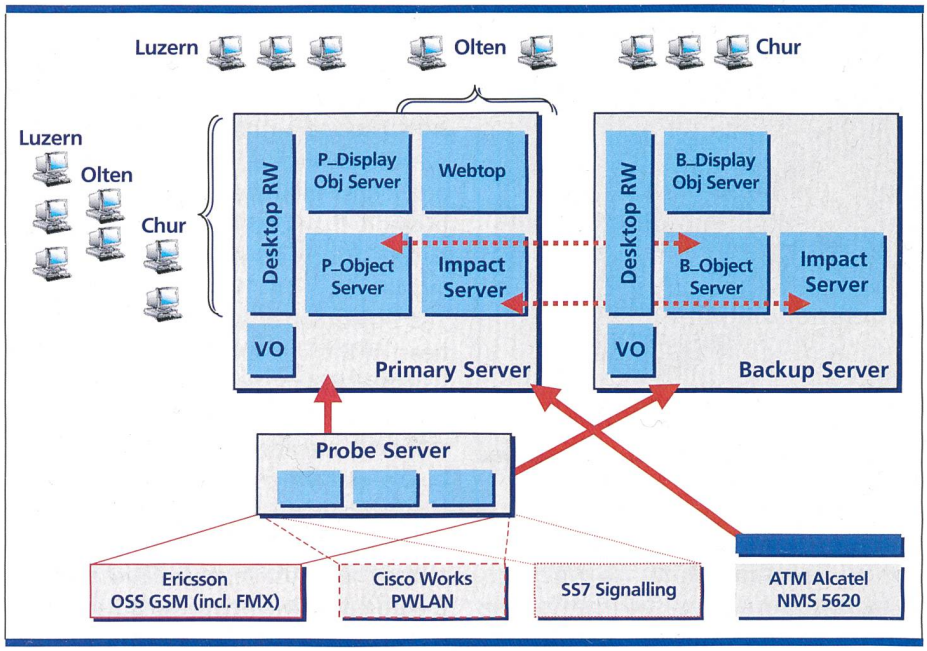

Fig. 7. Operations Security.

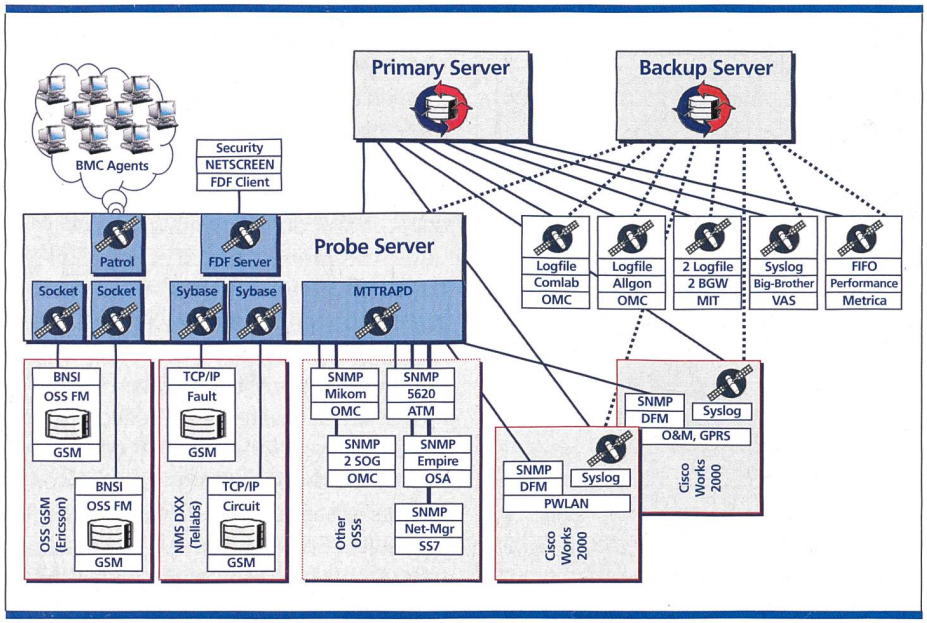

Fig. 8. OSS Integration.

Operations Security

In the standard operation (fig. 7) all Probes send their alarms to the Primary Object Server (the Object Server within the Primary Server). The bi-directional gateway listens to all inserts and updates on the Primary Object Server and updates the respective tables on the Backup Object Server (the Object Server within the Backup Server). The transfer gateway sends the alarms to the Display Object Servers on both systems. If the operator connects to the Virtual Object Server „CAM", it points to the Primary Object Server as long as it is available. Any manual modifications to the alarms (acknowledge, delete, clear, etc.) are executed on both Display Servers (Primary and Backup Server). Any changes are therefore reflected in the Backup Object Server through the bi-directional gateway between the Primary and Backup Server. Administrative changes to users or tools are also transferred through this gateway from the Primary to the Backup Server. Through these automated processes running in the background, Netcool maximises the operations security and prepares the whole system well should of problems occur.

The automatic „Heartbeat Check" checks whether the heartbeat alarm (transferred by the gateway) is older than twice the heartbeat frequency. Should this fault be the case, an automatic process would
- activate all other automations on the Backup Server
- start the Virtual Operator on the Backup server
- generate a „Memory" alert to remember that above actions have been performed already

The Probes would check the availability of the Primary Server and continue sending alarms as long as the connection to the Primary Server is established. If the Primary Object Server is not reachable, the Probes then try to connect to the Backup Object Server who then receives all alarms. The Backup Server is now up and running. As there is no Webtop Server on this system, only the native Desktop GUI can be used. For the unlikely case that both Object Servers are unreachable, all data would be stored locally and forwarded to the Object Server as soon as any of the two Object Servers is reachable again.

After the recovery of all processes on the Primary Server, the Probes realise that the connection has been re-established and switch back to the Primary Object Server. At that time the whole Primary Server is fully available again and the operators are automatically re-connected to that system. The automatic „Heartbeat Check" reaches the Backup Object Server through the gateway. The „HeartbeatCheckFallback" automation would
- stop the virtual Operator
- de-activate all automations except the „HeartbeatCheck" automation
- delete the „Memory" alert

Now the Backup Server is in standby mode until the heartbeat alert disappears next time.

Glossary and Terms

ALADIN	ALarm ADministration and INtervention (SCM own development)
Allgon	Supplier of radio repeater
API	Application Programming Interface
ATM	Asynchronous Transfer Mode
BGW	Billing Gateway
Big Brother	An „Open Source" product for the supervision of Swisscom Mobile's server infrastructure in Luzern
BMC	Supplier of the software „BMC Patrol" for server supervision
CAM	Common Alarm Management
CM	Configuration Management
CN-OSS	Core Network OSS (Ericsson Product)
Comlab	Supplier of the repeater used for the „Lötschbergtunnel"
CORBA	Common Object Request Broker Architecture
DB	Database
DFM	Device Fault Manager (Function of Cisco Works 2000, SNMP-Agent)
DWH	Data Ware House
DXX	Digital Cross Connect
Empire	Supplier of the OSA serving on the interface between the service and the SS7 platform
FDF	Foreign Data Feeds
FIFO	First In, First Out
FIM	Fault Info Management (SCM own development)
FM	Fault Management
FMX	Fault Management Expert (Expert System of Ericsson OSS)
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications (in CH: NATEL D)
GUI	Graphical User Interface
HW	Hardware
IP	Internet Protocol
LAN	Local Area Network
Mikom	Supplier of repeater (was recently taken over by Andrew)
MTTRAPD	Multi-Thread TRAPD Probe (for the integration of SNMP)
NE	Network Element
Net-Mgr	Network Manager (Siemens Product)
NM	Network Management
NMC	Network Management Centre
NML	Network Management Layer
NMS	Network Management System
O&M	Operation and Maintenance
OS	Object Server
OSA	Open Service Access
OSS	Operations Support Systems
PM	Performance Management
PWLAN	Public Wireless LAN (Swisscom Mobile Service)
Q3	Standardised Management Interface within the TMN architecture
QoS	Quality of Service
RO	Read Only
RW	Read Write
SCM	Swisscom Mobile
SLM	Service Level Management
SM	Service Management
SML	Service Management Layer
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOG	Service Order Gateway
SS7	Signalling System No. 7
SW	Software
TCP	Transmission Control Protocol
TMN	Telecommunications Management Network
VAS	Value Added Services (Additional mobile Services)
VO	Virtual Operator (SW module from Micromuse which allows to run routines in case of particular alarm situations)
WAN	Wide Area Network
WAP	Wireless Application Protocol
WLAN	Wireless LAN

OSS Integration

In the past decade, many solutions were designed and installed with the claim to provide a comprising overview about all existing managed networks and elements. In fact, only very few suppliers fulfilled these promises, mostly combined with complicated architectures, a long time for the realisation and/or an unfavourable cost effectiveness. The long experience in realising such „mega-projects" was proof that many solutions are brilliant when starting on a „green field" without considering the existing infrastructure. One of the strengths of Netcool is the fact that it offers a range of system integration paths for both standardised or vendor-specific environments (e. g. SNMP, TL1, CORBA, Q3 or Syslog, Logfile and API). In addition, more than 300 pre-built Netcool Probes allow to monitor practically any network device or system – a major advantage compared to most of the available management solutions on the market. By using a connection-oriented transport protocol for transferring the data to the Object Server, the transmission security is not left to chance. And because the information is normalised into a common format, it is presented in a unified way to the operators.

All these advantages apply to the Common Alarm Management (CAM) System for Swisscom Mobile too. As reflected in figure 8, it is obvious that an already existing, multi-vendor environment has been integrated here. By placing the Probe close to or inside the managed system, the failover mechanisms and the store-and-forward-mode as described in the chapters above reach their full effect. It should be noted that every Probe has two active paths to the Primary (normal lines) and to the Backup Server (dotted lines), either directly or via the Probe Server. By this, both Servers are always up-to-date and a fast switching (failover) from the Primary to the Backup Server without any loss of management data becomes possible.

Conclusion

With the increasing traffic on mobile networks and the greatly increasing number of mobile services delivered on them, it was a necessity to come up with a comprehensive management solution to handle all alarms on one platform. The CAM system from Sun Microsystems and Micromuse provides Swisscom Mobile with a coherent and comprehensive overview on the real network situation. Due to high and quite tough competition, the time pressure and the economic conditions have to be considered when such projects are realised. Thanks to the thorough planning and project steering, resulting in a close partnership between Swisscom Mobile and Sun, the CAM system could be realised within a short timeframe. Especially when one considers the complexity of the quickly grown management environment at Swisscom Mobile's network operations, this practically unique CAM system is meeting high expectations. And the CAM story making further headway – with the management of more networks and IT systems, ensuring the quality of new voice, broadband data and video services. 3

Rüdiger Sellin *is a telecommunications engineer from the Fachhochschule Düsseldorf in Germany. After developing Software and Systems for OSI applications, he joined Swisscom (the former Telecom PTT) in 1992. During the course of his intensive standardisation work at ITU-T and ETSI, he helped to build up Swisscom's GSM Network Management Centre and was responsible for functional testing. In addition, he has written many articles for telecom magazines and led telecom seminars in Europe. Since November 2000, he has been responsible for Swisscom Mobile's technical communications in telecom magazines as a PR Manager.*

The author would like to express his sincere thanks to René Luyten (CAM Project Leader at Swisscom Mobile) and to Ekhard Konrath (Project Management at Sun Microsystems) for their valuable and extensive input to the basic material for this article and for their active and helpful interaction with the author.

Further information from Swisscom Mobile and Sun Microsystems: www.swisscom-mobile.ch and www.sun.com

Zusammenfassung

Umfassendes Fehlermanagement mit CAM

Unter dem Eindruck eines härter werdenden Wettbewerbs im schweizerischen Mobilkommunikationsmarkt ist die Effizienz in der Erkennung und gezielten Beseitigung von Fehlfunktionen eine höchst kritische Grösse. Bei einer stets wachsenden Anzahl von Netzen sowie von Basis- und Zusatzdiensten ist das Fehlermanagement eine komplexe Aufgabe. Swisscom Mobile hat darum an Sun Microsystems den Auftrag für ein umfassendes Common Alarm Management (CAM) System erteilt, das mit dem Produkt «Netcool» von Micromuse realisiert wird.

CAM behandelt alle Alarmprozesse zuverlässig und proaktiv und ergänzt als «Umbrella Management System» die bestehende Infrastruktur optimal. Mit CAM werden nicht nur die Netze und Service-Plattformen überwacht, sondern auch andere wichtige Betriebseinrichtungen von Swisscom Mobile, wie Network Management Systeme und interne Datennetze.


LESCH+FREI
Ich will,
dass nie etwas
zwischen uns kommt.
Spin the globe: Enge Beziehungen machen das
Leben lebenswert. Unsere innovativen Lösungen sorgen dafür,
dass Sie miteinander in Kontakt bleiben.
In diesem Sinne gehören auch wir zu Ihrem Beziehungsnetz.
Und das soll auch so bleiben.
SIEMENS
Global network of innovation
www.siemens.ch