Entwicklung einer Backup und Recovery Strategie für die Oracle8-Infrastruktur des IMW

Düsing, C.; Jach-Reinke, H.-J.

Das Informationssystem eines Unternehmens stellt oftmals eine lebensnotwendige Struktur dar, auf deren Erhaltung und Instandhaltung ein sehr großer Wert gelegt werden muß. Der Aufbau und die Inhalte einer Backup und Recovery Strategie sollen hier am Beispiel einer bestehenden Oracle Infrastruktur aufgezeigt werden.

The information system often represents an essential part of a company, which must be maintained for a healthy existence. This article points at the development process and the contents of a Backup and Recovery strategy exemplified on an existing Oracle infrastructure.

1 Die Notwendigkeit eines Backup und Recovery

Am Institut für Maschinenwesen wurde am Beginn dieses Jahres eine Migration des vorhandenen Datenbanksystems auf die aktuelle Oracle 8.i Datenbank durchgeführt. Dieses Datenbankmanagementsystem wird zur Zeit in verschiedenen Projekten, wie z.B. SIMNET /1/ und KARE /2/ eingesetzt, der Einsatz in der Lehre ist geplant.

Es ist somit absolut notwendig, die Datenbank für die Benutzung bereitzuhalten. Bei Eintritt eines Fehlers soll die Datenbank so schnell wie möglich wieder betriebsbereit sein und keine oder nur sehr wenige Daten verloren gehen. Um die Daten vor verschiedenen Fehlern zu schützen, ist es wichtig, regelmäßige Backups der Datenbank durchzuführen, denn diese bilden die Grundlage für ein entsprechendes Recovery der Daten.

Die Entwicklung eines solchen Strategiekonzeptes soll am Beispiel der Oracle Infrastruktur des IMW erläutert werden.

1.1 Datenbankverwaltungsziele bei Backup und Recovery

Die Anforderungen einer Sicherungsstrategie lassen sich generell in vier Zielstellungen einteilen /3/:

- Schutz der Datenbank vor möglichen Fehlern
- Erhöhung der Mean-Time-Between-Failure (MTBF)
- Reduzierung der Mean-Time-To-Recover (MTTR)
- Minimierung des Datenverlustes

Diese allgemeinen Erwartungen an ein Datenbankmanagementsystem, wie z. B. möglichst hohe Verfügbarkeit oder Ausschluß eines Datenverlustes müssen in der Regel jeweils der speziellen Situation angepaßt werden.

1.2 Definition einer Backup und Recovery Strategie

Um ein Sicherungskonzept in eine bestimmte Unternehmensstruktur einfügen zu können, werden die Anforderungen an dieses in drei Bereiche eingeteilt, welche die Backupstrategie definieren:

- Geschäftsanforderungen
- Operationale Anforderungen
- Technische Anforderungen

Die Auswirkungen der Ausfallzeit auf die Geschäftsabläufe können erheblich sein. Die Kosten einer eventuellen Ausfallzeit und der Datenverluste müssen quantifiziert werden und mit den Kosten verglichen werden, die durch die Minimierung der Ausfallzeit und die Minimierung der Datenverluste entstehen.

Die Art des Backup und Recovery sind stark vom Typ der operationalen Anforderungen abhängig. Die richtige Konfiguration der Datenbank ist Voraussetzung dafür, daß eine Datenbank z. B. rund um die Uhr, sieben Tage die Woche verfügbar ist. Diese Aspekte sind direkt mit den technischen Ansprüchen verknüpft.

Die technischen Anforderungen stellen die Basis für die Entwicklung einer Backup und Recovery Strategie dar. Generell gilt, daß genügend Systemressourcen für ein Backup zur Verfügung gestellt werden müssen, so daß die Performance der Datenbankanwendung nur geringfügig beeinflusst wird. So muß z. B. für physikalische und logische Kopien der Daten genügend Speicherplatz vorhanden sein. Da beide Arten jedoch die Systemleistung unterschiedlich beeinflussen, ist es im Einzelfall abzu-

wägen, welche Art der Kopien und in welchem Umfang diese benutzt werden können.

Durch eine gründliche Analyse dieser Anforderungen werden die Informationen gesammelt, die zur Einrichtung eines Backup Konzeptes erforderlich sind.

1.3 Test einer Backup und Recovery Strategie

Die einzige Möglichkeit sicherzustellen, daß die geplante Strategie die MTTR reduziert und die MTBF erhöht, ist ein regelmäßiger Test der Backups in Bezug auf Gültigkeit und Funktionalität. Das Recovery einer Datenbank kann nur so gut wie die verfügbaren Backups sein. Dies bedeutet, daß bei jeder strukturellen Veränderung der Datenbank der Backupplan den neuen Anforderungen angepaßt und erneut getestet werden muß. Dieses sind die Minimalanforderungen für die Testhäufigkeit einer Datenbank. Bei starken Veränderungen der Transaktionslast in der Datenbank sollten auf jeden Fall in regelmäßigen Abstände zusätzliche Tests durchgeführt werden.

2 Gesamtübersicht über das Backup-Schema

Ein Backup und Recovery Schema setzt sich aus insgesamt drei Teilen zusammen (siehe **Bild 1**) /4/ :

- BACKUP
- RESTORE
- RECOVERY

2.1 Backup

Das BACKUP kann in ein physisches und ein logisches Backup unterteilt werden.

Das physische Backup entspricht einer Kopie von den Betriebssystemdateien, welche die Datenbankstruktur repräsentieren, das logische Backup entspricht einem Export von Teilen oder der gesamten Datenbank aus dem Datenbankmanagementsystem heraus. Ein physisches Backup kann sowohl „offline“, d. h. bei heruntergefahrener Datenbank, als auch „online“, also während des laufenden Betriebes, durchgeführt werden.

2.2 Restore

Unter dem Begriff RESTORE versteht man in diesem Zusammenhang die Wiederherstellung von einer oder mehrerer defekter Datendateien einer Datenbank. Das logische Restore ist gleichbedeutend mit einem Import von vorher ausgelagerten Daten. Das physische Restore kann in vollständig und unvollständig unterteilt werden. Die Begriffe vollständig und unvollständig sind im Zusammenhang auf die Vollständigkeit der Daten zu interpretieren. Beim vollständigen Restore wird nur die defekte Datei durch ihre Sicherung ersetzt, wohingegen bei einem unvollständigen Restore alle Datendateien durch ihre Sicherung ersetzt werden. Unvollständig bedeutet hier, daß absolut ein Datenverlust eintritt, da alle, auch aktuellen, Datendateien durch ältere Kopien ersetzt werden.

2.3 Recovery

Das RECOVERY wird immer dann verwendet, wenn kein Restore möglich, oder z. B. Datenverlust inakzeptabel und nur durch eine Recoveryprozedur wiederherstellbar ist.

Für den Fall, daß alle Datendateien der Datenbank physisch noch vorhanden sind, kann ein sogenanntes Instance Recovery durchgeführt werden.

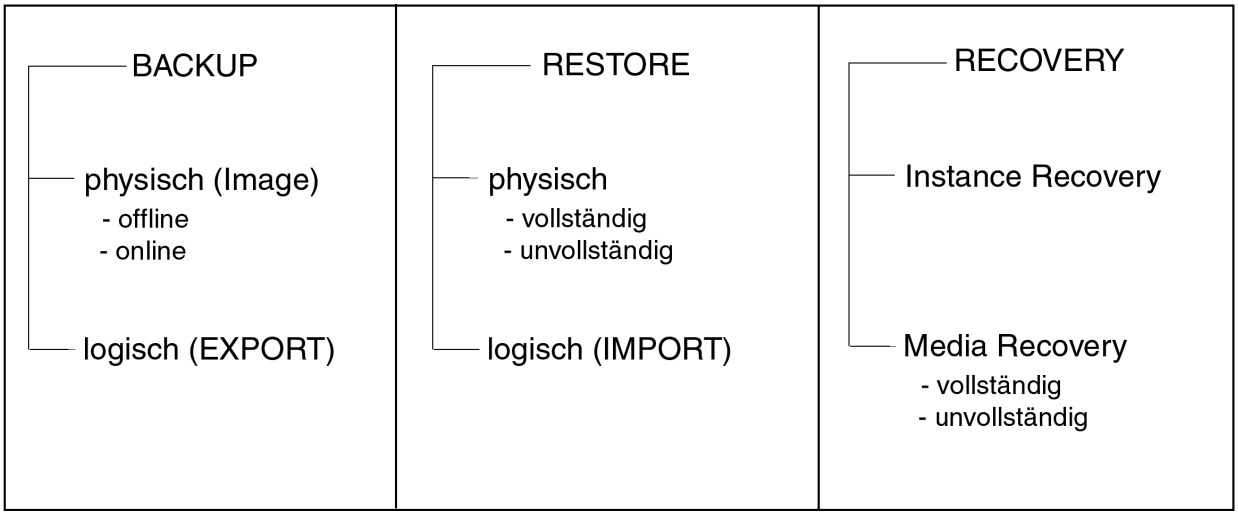

Bild 1: Drei Module eines Oracle Backup Schemas

Dies tritt z. B. bei einem Stromausfall oder bei Fehlern in der Software ein. Ein Instance Recovery wird beim erneuten Starten der Datenbank automatisch durchgeführt, d. h. es ist keine spezielle Aktion durch den Administrator erforderlich.

Bei dem Verlust oder Beschädigung einer Festplatte oder Datendatei muß ein sogenanntes „Media – Recovery“ durchgeführt werden.

Bei einem Verlust von Datendateien oder den sogenannten Kontrolldateien ist ein vollständiges Recovery möglich.

Die Kontrolldateien enthalten alle Informationen, die zur Sicherstellung der Datenbankintegrität benötigt werden. Eine Voraussetzung für ein vollständiges Recovery in diesem Sinne ist, daß ein gültiges Backup und alle archivierten Redo-Log-Dateien seit dem Zeitpunkt dieses Backups existieren. Die Redo-Log-Dateien enthalten einen Datensatz mit den an der Datenbank vorgenommenen Veränderungen. Diese Veränderungen an der Datenbank können somit nach Einspielen der letzten gültigen Sicherung bis zum Zeitpunkt des Absturzes der Datenbank wieder vollzogen werden. Somit entsteht bei dieser Methode kein Datenverlust.

Sollte der Verlust oder die Beschädigung einer aktiven Redo-Log-Datei eintreten, ist nur noch ein unvollständiges Recovery möglich. Dies bedeutet, daß nur noch Daten bis zu dem Zeitpunkt der zuletzt aktiven Redo-Log-Datei, welche die Veränderungen an den Daten enthält, zurückgeholt werden können. Somit entsteht in diesem Fall immer ein Datenverlust.

3 Definition der Anforderungen des IMW

Die Anforderungen des Instituts für Maschinenwesen an die Verfügbarkeit des Oracle Servers und die Backup und Recovery Strategie basieren auf der Tatsache, daß es sich überwiegend um ein System handelt, auf dem Prototypen für Projekte entwickelt werden.

Daraus ergeben sich zusammengefaßt folgende geschäftliche, technische und operationale Anforderungen:

- Die MTBF soll soweit wie möglich erhöht und die MTTR reduziert werden, um bei einem Ausfall den Arbeitsprozeß nicht unnötig lange aufzuhalten.
- Es soll kein Datenverlust auftreten.
- Da die Transaktionslast der Anwendungen auf dem Server stark schwanken kann, soll die Strategie so flexibel wie möglich sein, damit notwendige Änderungen schnell und ohne Beeinflussung des normalen Betriebes durchgeführt werden können.
- Die Datenbank soll innerhalb der Woche im 24-Stunden Betrieb laufen, so daß längere Transaktionen auch während der Nacht bearbeitet werden können. An Wochenenden besteht die Möglichkeit den Server für bis zu zwei Stunden in der Nacht aus dem Betrieb zu nehmen.
- Die Backup und Recovery Strategie soll in regelmäßigen Abständen getestet werden.
- Backup Kopien sollen dezentral aufbewahrt werden.
- Der Backup-Plan sollte gut dokumentiert und gepflegt sein.
- Es sollen redundante physikalische Kopien der Datendateien auf dem System verfügbar sein.
- Die Datenbank soll so konfiguriert sein, daß sie gegen bestimmte Fehler immun ist.

4 Kurzbeschreibung des Oracle-Servers am IMW

Als Grundlage für die Backup und Recovery Strategie soll an dieser Stelle kurz der Oracle8-Server des Instituts für Maschinenwesen und dessen Architektur vorgestellt werden, **Bild 2**.

Bild 2: Oracle Server des IMW, rechts daneben: Externes SCSI Gehäuse mit drei weiteren Festplatten

Der Server basiert auf einer PC-Architektur mit einem 400 MHz Intel Prozessor und 256 MB Arbeitsspeicher.

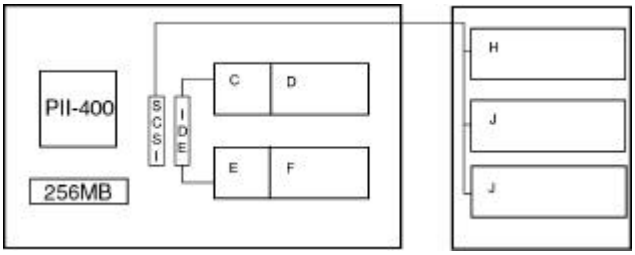

Bild 3: Struktur des Oracle-Servers des IMW

Diese Ressourcen sind für das derzeitige Transaktionsvolumen vollkommen ausreichend. Das System ist jedoch so ausgelegt, daß eine Vergrößerung der Systemressourcen bei Bedarf jederzeit möglich ist. Als Datenspeichermedien werden für die Datenbank aus Performancegründen nur Festplatten eingesetzt /5/. In dem 19“-Gehäuse sind intern zwei identische Festplatten an den IDE-Bus angeschlossen, in einem externen Gehäuse befinden sich drei weitere, ebenfalls gleich große Festplatten, welche über einen externen SCSI-Anschluß angesprochen werden, **Bild 3**. Durch die Verwendung verschiedener Bussysteme wird die anfallende I/O - Last auf verschiedene Kanäle verteilt, damit es nicht zu Leistungseinbrüchen kommt. Diesen physischen Laufwerken sind sechs logische Laufwerke (C – J) zugewiesen.

5 Struktur des Backup

Um eine strukturelle Beschreibung des Backup zu geben, werden einige wichtige Zusatzinformationen über die Architektur des Datenbankmanagementsystems Oracle benötigt. Im folgenden Abschnitt werden die für die Erläuterung wichtigen Datenstrukturen kurz zusammengefaßt vorgestellt.

5.1 Datenstrukturen der Oracle Architektur

Die Oracle Datenbank repräsentiert die physikalischen Strukturen und besteht aus Betriebssystemdateien, den sogenannten Datenbank-Dateien, **Bild 4**.

Innerhalb der eigentlichen Datenbank existieren drei Arten von Dateien, die für das Backup von Bedeutung sind:

- Die *Kontrolldateien* enthalten Informationen, die zur Erhaltung und Prüfung der Datenbankintegrität benötigt werden. Eine Datenbank benötigt mindestens eine Kontrolldatei.
- Die *Redo Log Dateien* enthalten einen Datensatz mit den an der Datenbank vorgenommenen Änderungen. Dadurch können die Daten bei Fehlern wiederhergestellt werden. Für die Erhaltung der Funktionalität der Datenbank werden immer mindestens zwei dieser Dateien benötigt, da es sich hierbei um einen zyklischen Buffer handelt, d. h. die Dateien werden immer wieder beschrieben. Ist die eine Datei voll, werden die Änderungen in der nächsten festgehalten, bis diese wiederum voll ist, und die erste wieder beschrieben wird.
- In den *Datendateien* werden die eigentlichen Objekte der Benutzer einer Datenbank festgehalten, wie z. B. die Tabellen und Relationen mit zugehörigen Definitionen sowie Namen, Paßwörter und Priviligien.

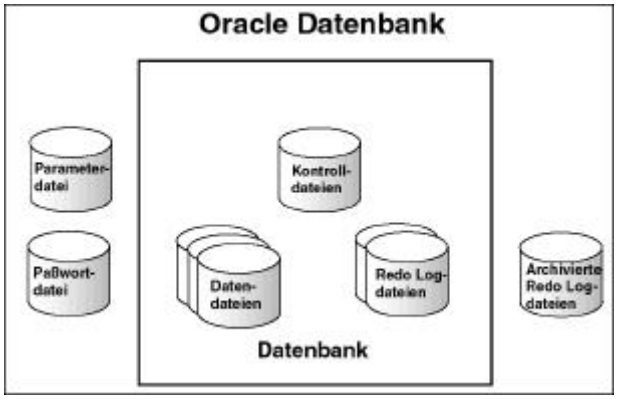

Bild 4: Betriebssystemdateien einer Oracle Datenbank

Außerhalb dieses Bereiches der Datenbank existieren weitere Betriebssystemdateien, welche unter anderem für die Datenbankintegrität und den laufenden Betrieb von Bedeutung sind:

- In der *Parameterdatei* befinden sich alle für den Betrieb der Datenbank wichtigen Parameter. Beim Hochfahren der Datenbank wird diese Datei eingelesen und ihr Inhalt verarbeitet. Ohne diese Datei kann eine Datenbank nicht wieder hochgefahren werden.
- Die *Paßwortdatei* beinhaltet alle Informationen, welche einem Benutzer zugeordnet werden, um sich bei der Datenbank authentifizieren zu können.
- Die sogenannten *archivierten Redo Log-Dateien* werden angelegt, wenn die Datenbank im ARCHIVE-Modus betrieben wird. Im ARCHIVE-Modus wird von den Redo Log-Dateien, bevor sie überschrieben werden, eine Sicherungskopie gemacht, die archivierte Redo Log-Datei, mit deren Hilfe auch länger zurückliegende Veränderungen an der Datenbank wieder zurückgerollt werden können.

5.2 Aufbau der Backupstrategie im IMW

Die Struktur des Backup am Oracle8-Server des IMW läßt sich im allgemeinen in drei Bereiche aufteilen:

1. Spiegelung von Dateien, die für den Betrieb der Datenbank unmittelbar von Bedeutung sind.
2. Betreiben der Datenbank im ARCHIVE-Modus.
3. Regelmäßiges Backup der gesamten Datenbank.
4. Spiegelung der Backupdateien auf dezentralen Medien.

Das sogenannte Spiegeln von Dateien stellt die bevorzugte Methode dar, um die Ausfallsicherheit zu erhöhen und die Notwendigkeit eines Recovery zu reduzieren, indem man bei laufender Datenbank ein Restore durchführen kann. Im laufenden Betrieb werden die gerade verwendeten Datenbankdateien auf mehreren Speichermedien gesichert. Fällt dann eine dieser Dateien zum Beispiel aufgrund eines Hardwarefehlers aus, so kann die Datenbank weiter betrieben und die Fehlerquelle währenddessen beseitigt werden. In diesem Fall handelt es sich bei den gespiegelten Datenbankdateien um die Kontrolldateien (CTRLn) und die Redo Log-Dateien (RLGn). Die Kontrolldateien werden hier auf drei und die Redo Log-Dateien auf zwei unabhängigen Festplatten gespeichert, um beim Ausfall einer Festplatte auf laufende Platten noch zugreifen zu können, **Bild 5**.

Die vorliegende Datenbank wurde so konfiguriert, daß die Redo Log-Dateien archiviert werden. Um ein erfolgreiches Recovery durchführen zu können, werden immer ein komplettes Backup der Datenbank sowie alle Redo Log-Dateien seit dem Zeitpunkt des letzten Backups benötigt. Wäre dies nicht der Fall, so könnte nur ein unvollständiges Recovery durchgeführt werden, was immer mit dem Verlust von Daten verbunden wäre. Durch den ARCHIVE-Modus der Datenbank werden immer alle Redo Log-Dateien archiviert, so daß bis zum Zeitpunkt des letzten gültigen Backups immer alle benötigten Redo Log-Dateien zur Verfügung stehen. Diese Archivdateien (ARCHn) werden auf zwei verschiedenen Festplatten gespiegelt um hier ebenfalls das Ausfallrisiko zu verringern und im Notfall eine zweite Kopie vorliegen zu haben. Wie in **Bild 5** zu erkennen ist, werden die Archive und die eigentlichen Redo Log-Dateien, sowie ihre Spiegelungen auf verschiedenen physikalischen Festplatten gespeichert.

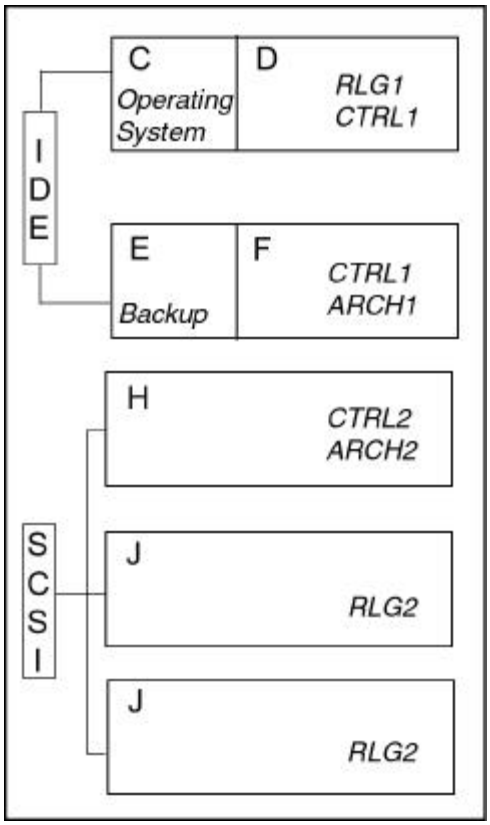

Bild 5: Verteilung der Betriebssystemdateien auf physisch unterschiedliche Laufwerke

Der Grund dafür liegt darin, daß für beide Prozesse eine hohe I/O-Last anfällt, welche so auf verschiedene Festplatten und Bussysteme verteilt werden kann, so daß es nicht zu gravierenden Einbrüchen in der Performance kommt.

Das Backup einer Oracle Datenbank bedeutet, daß Kopien aller Betriebssystemdateien angefertigt werden. Dieses kann generell auf zwei verschiedene Arten geschehen.

- Offline Backup: Die Datenbank wird heruntergefahren und die Kopie der Betriebssystemdateien wird angefertigt. Dies hat den Nachteil, daß die Datenbank heruntergefahren werden muß und somit während dieser Zeit kein Arbeiten an der Datenbank möglich ist.
- Online Backup: Während die Datenbank geöffnet ist, werden die Betriebssystemdateien kopiert. Dies bedingt, daß die Tablespaces einzeln in einen sogenannten Backup Modus gesetzt, kopiert und anschließend wieder in den normalen Modus gesetzt werden müssen, so daß die Konsistenz der Datenbank gewahrt bleibt. Dadurch dauert dieses Verfahren wesentlich länger als bei einem Offline Backup und die gesamte Performance der Datenbank sinkt in dieser Zeit stark ab.

In der Oracle-Infrastruktur des IMW werden beide Methoden verwendet. Die Durchführung des Backup wird jeweils von Skripten durchgeführt, die zu diesem Zweck programmiert worden sind. Diese werden nach einem Zeitplan ausgeführt, so daß kein Eingreifen von außen mehr erforderlich ist. Das Offline Backup wird jeden ersten eines Monats um 01:00 Uhr durchgeführt, das Online Backup jeden Samstag um 22:00 Uhr, somit also zu den Zeiten an denen die wenigsten Zugriffe auf die Datenbank zu verzeichnen sind. Die Betriebssystemdateien, welche die Datenbank repräsentieren, werden auf dem logischen Laufwerk E gesichert.

Die so gesicherten Backupdateien werden anschließend auf den zentralen Fileserver des IMW gespeichert, so daß zwei voneinander unabhängige Kopien existieren. Diese werden innerhalb der Nacht vom zentralen Backup des Rechenzentrums erfaßt und gesichert, so daß immer ein dezentrales Backup vorhanden ist. Dies bedeutet, daß bei dem schlimmsten der anzunehmenden Fälle, dem totalen Zusammenbruch des Oracle-Servers und des Fileservers immer noch eine Kopie außerhalb des Institutes vorliegt, welche bei Bedarf zurückgewonnen werden kann.

Das Backup und Recovery des IMW wurde bis zur endgültigen Fassung der Strategie mehrmals getestet und verifiziert. Bei dem heutigen Stand ist es nur noch nach Veränderungen der Datenbankstruktur nötig, die Strategie entsprechend anzupassen und wieder zu testen.

Das bestehende Konzept entspricht nun allen in Kapitel 3 aufgezählten geschäftlichen, operationalen und technischen Anforderungen des IMW. Größere Veränderungen der Strategie sind nur noch bei beträchtlichen Modifikationen des Servers oder der Datenbank z. B. infolge stark erhöhter Transaktionslast nötig.

6 Zusammenfassung

Am Beispiel der bestehenden Oracle Infrastruktur des IMW konnte die Planung, Entwurf und Aufbau einer Backup und Recovery Strategie für das Datenbankmanagementsystem Oracle aufgezeigt werden. Ein solches Backup ist für jedes Unternehmen, das produktiv mit einem solchen System arbeitet, unerläßlich. Eine entsprechende Strategie muß den speziellen Strukturen eines Unternehmens, basierend auf den Kenntnissen über die geschäftlichen, operationalen und technischen Anforderungen, angepaßt werden. Der Aufbau und Test einer den speziellen Erwartungen entsprechenden Strategie ist zumeist ein langwieriger, iterativer Prozeß. Selbst nach der Fertigstellung und Inbetriebnahme ist in der Regel noch eine regelmäßige Wartung und Validierung nötig.

7 Literatur

/1/ Goltz, M.; Schmitt, R.: SIMNET – Workflow Management for Simultaneous Engineering Networks; IMW Institutsmitteilung Nr. 23; Clausthal 1998

/2/ Heimannsfeld, K.; Judith, M.: KARE – Knowlegde Acquistion and Sharing for Requirement Engineering; IMW Institutsmitteilung Nr. 23; Clausthal 1998

/3/ Oracle Education; Oracle 8 Datenbankadministration: Backup & Recovery; Oracle Press, München, 1999

/4/ Velpuri, V.; Adkoli, A.: Oracle 8 Backup & Recovery Handbook; Osborne/McGraw-Hill; Berkeley; 1998

/5/ Gurry, M.; Corrigan, P.: Oracle Performance Tuning; O´Reilly and Associates; Cambridge; 1996