

Praxisbericht 3

Hochverfügbarkeit auf Basis von Fujitsu-Siemens Produkten

Name: Artur Neumann

Klasse: F6H9



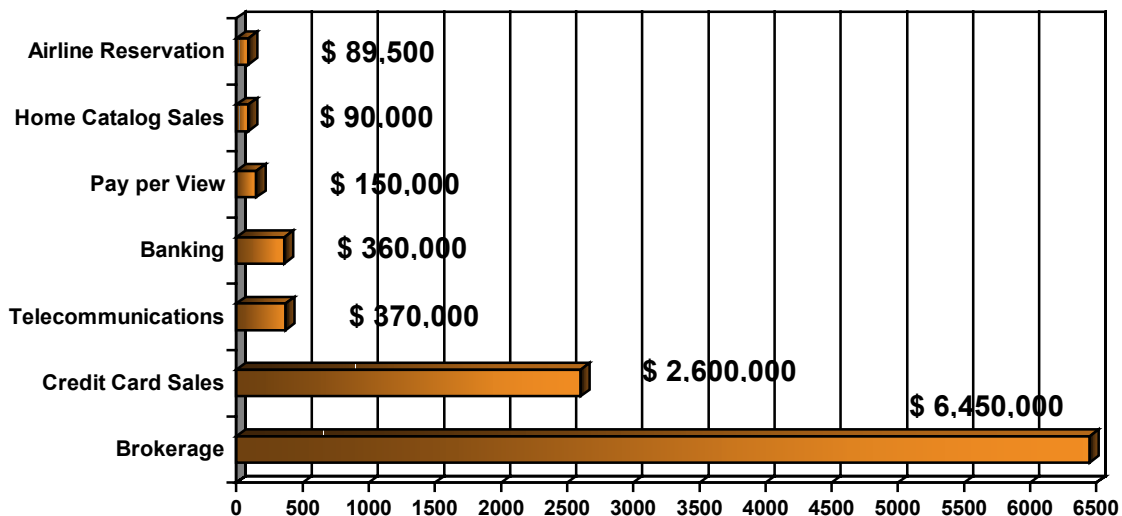
Inhaltsverzeichnis

Inhaltsverzeichnis	2
1. Wofür Hochverfügbarkeit (HV)?	3
<i>Ausfallkosten pro Stunde</i>	3
<i>Wodurch kann es zu Ausfallzeiten kommen?</i>	4
2. Hochverfügbarkeits- Lösungen	5
<i>Bildliche Darstellung des Konzept der Hochverfügbarkeit</i>	5
<i>Redundante Hardware</i>	5
<i>Redundante Hardware</i>	6
<i>Disaster Recovery</i>	6
<i>Datensicherung</i>	7
<i>Storage Area Network (SAN)</i>	7
3. Beispiel für eine HV Lösung.....	8
4. Quellen und Links	11

1. Wofür Hochverfügbarkeit (HV)?

Die Wichtigkeit von Hochverfügbarkeit lässt sich schnell an ein paar Beispielen zeigen. Wenn z.B. die Computer-Systeme einer Bank oder eines Produktionsbetriebes, der rund um die Uhr produziert, ausfallen entstehen enorme Kosten durch den Stillstand des Unternehmens. Des weiteren werden auch Kunden verschreckt wenn sie z.B. keine Bankgeschäfte mehr tätigen können oder der Aktienhandel nicht ordnungsgemäß abgewickelt wird. Oder was passiert wenn ein Unternehmen seine Kundendaten oder eine Bank die Kontendaten verliert? Die Ausfallkosten sind meistens erheblich und können auch zur Pleite eines Unternehmens führen. Die langfristigen Kosten sind noch viel höher. Diese entstehen dadurch dass das Unternehmen einen schlechten Ruf bekommt und die Kunden dem Unternehmen nicht mehr vertrauen und zur Konkurrenz wechseln.

Ausfallkosten pro Stunde



Beispiel Verfügbarkeitslevel Banken:

99,5 % → 99,9 % = 35 Std = \$ 12,600,000 vermiedene Kosten

99,9 % → 99,99% = 8 Std = \$ 2,880,000 vermiedene Kosten

(Quelle und weitere Informationen: [3])

Wodurch kann es zu Ausfallzeiten kommen?

1. Systemausfälle

Plattenausfälle

Stromprobleme

Prozessorfehler

Speicherfehler

Systemausfälle können z.B. durch fehlerhafte Produkte oder durch begrenzte Lebensdauer von bestimmten Geräten z.B. Festplatten hervorgerufen werden.

2. Bedienungsfehler

Auch der beste Techniker ist nur ein Mensch und einem Menschen unterlaufen Fehler. Solche Fehler können in der EDV verheerende Folgen haben.

3. Umwelt

Sturm

Wasser,

Erdbeben

Umweltkatastrophen können jederzeit und überall passieren. Und meistens sind sie schwer bis gar nicht vorhersehbar und noch schwieriger ist es, solche Katastrophen zu verhindern oder aufzuhalten.

4. Vandalismus

Spätestens seit dem 11 September 2001 wissen wir welche Ausmaße der Vandalismus und die pure Zerstörungswut annehmen kann.

5. Hacker

Besonderst die Computeranlagen von großen und renommierten Unternehmen sind immer wieder Ziel von Computerkriminalität.

6. Computer Viren

Computer Viren sind schon seit langem keine Seltenheit mehr. Und um solche zu erstellen sind auch keine tiefen Computerkenntnisse nötig und somit ist dies keine große Schwierigkeit. Viren können auf unterschiedlichste Art und Weise Computer und Computer-Netze lahm legen, z.B. durch den direkten Befehl der Server (Beispiel „Code Red“ Virus) oder auch durch Befehl der Clients, welche dann eine Überlastung der Systeme hervorrufen (Beispiel „I love you“ Virus).

7. Sabotage

Ein Unternehmen hat sicherlich viele Feinde. Das geht von Mitbewerbern über verärgerte Mitarbeiter bis hin zu Leuten die einfach Spass an Zerstörung haben oder aus anderen Gründen über das Unternehmen verärgert sind.

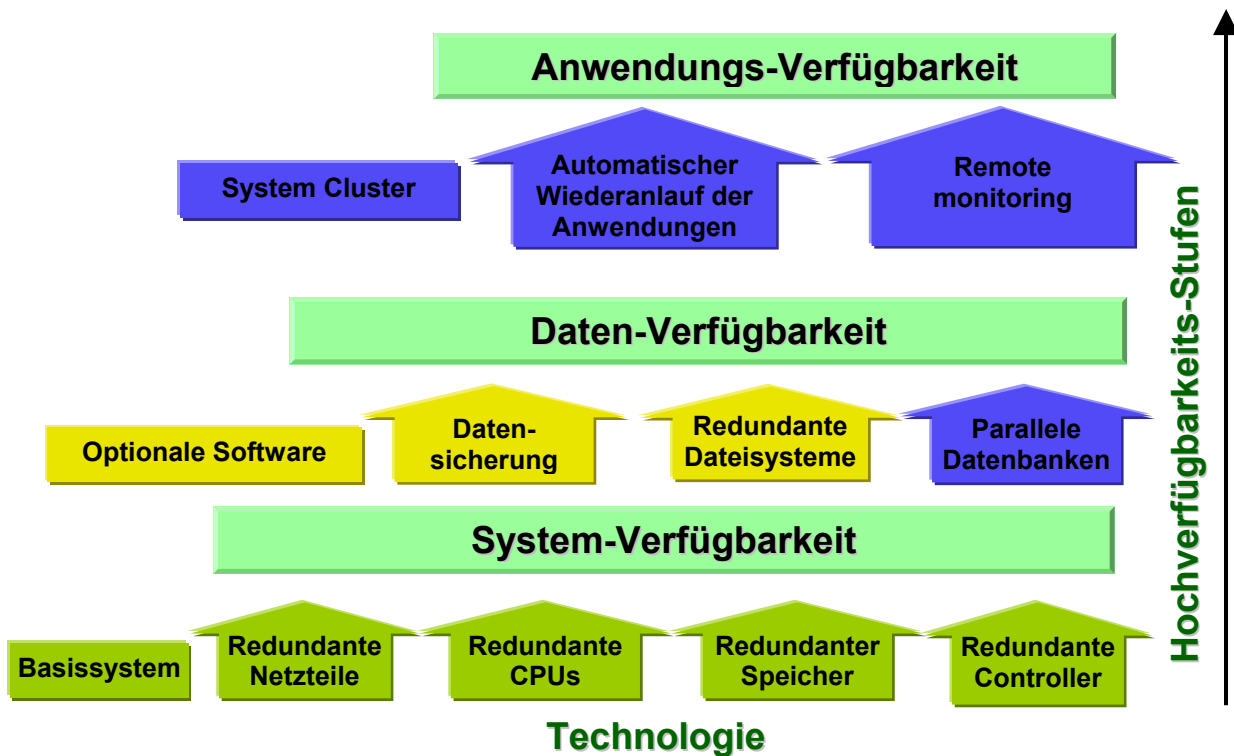
8. Geplante Ausfallzeiten z.B. für Wartungsarbeiten

Es müssen immer wieder neue Softwarestände eingespielt oder Hardwarekomponenten getauscht werden. Des weiteren kann es auch vorkommen das ein Rechenzentrum umziehen oder erweitert werden muss. Und trotzdem müssen die Dienstleistungen dieses Rechenzentrums weiter zur Verfügung stehen.

Durch Hochverfügbarkeitskonzepte sollen die Ausfallzeiten trotz dieser ganzen Probleme auf ein Mindestmass reduziert bzw. im Idealfall komplett verhindert werden.

2. Hochverfügbarkeits- Lösungen

Bildliche Darstellung des Konzept der Hochverfügbarkeit



Redundante Hardware

(Basissystem/Optionale Software)

Die Ausfallsicherheit wird dadurch gewährleistet, dass alle Komponenten bei denen es möglich ist und die für den Betrieb notwendig sind, redundant ausgelegt sind und sich zum Teil gegenseitig überwachen. Das geht sogar soweit das komplette Rechner redundant ausgelegt werden. Wenn nun ein Hardware - Fehler auftritt, wird dieser automatisch bemerkt, eine redundante Komponente kann die Aufgaben übernehmen und eine Fehlermeldung wird automatisch generiert. Zusätzlich werden Geräte installiert die nur dafür da sind eine reibungslosen Betrieb zu gewährleisten z.B. Unterbrechungsfreie Stromversorgung (USV). Ein weiterer Schritt ist es die Daten auf mehreren Festplatten gleichzeitig zu pflegen, damit beim Ausfall einzelner Festplatten die Daten weiterhin zur Verfügung stehen.

Disaster Recovery

(System Cluster)

Disaster Recovery geht noch ein Schritt weiter und beschäftigt sich mit dem Thema, was passiert, wenn redundante Hardware nicht ausreicht. Wir haben gesehen wie die meisten Hardware-Fehler abgefangen werden können. Es können jedoch auch andere Fälle eintreten. Was passiert z.B, wenn in einem Rechenzentrum ein Brand ausbricht, ein Gebäude einstürzt oder durch Naturkatastrophen ein komplette Rechenzentrum außer Betrieb gesetzt wird? Aus diesem Grund ist es notwendig, dass wichtige Daten, wie z.B. bei einer Bank die Konteninformationen, nicht nur in einem Rechenzentrum, sondern in mindestens zwei Rechenzentren gespeichert und auch bearbeitet werden müssen. Disaster Recovery beschäftigt dich mit der Technik die solche, teilweise mehrere Kilometer auseinanderliegenden, Rechenzentren zur Zusammenarbeit bringt. Durch Disaster Recovery wird sichergestellt das sich solche Computer-Anlagen gegenseitig überwachen und auch im Fehlerfall die Aufgaben des anderen übernehmen.

Datensicherung

Wenn solche Anstrengungen im Bereich Hardware-Redundanz und Disaster Recovery getroffen werden, kann man sich vielleicht fragen, wofür man dann noch Datensicherung braucht. Dafür gibt es im wesentlichen zwei Gründe:

1. Speicherplatz ist teuer. Wenn der Datenbestand ständig, schnell wächst, wird es irgendwann nötig, Daten, die aufbewahrt werden müssen, aber nicht im ständigen Einsatz sind, auszulagern (z.B. auf Bändern).
2. Zum anderen schützen HV und Disaster Recovery nicht vor logischen Fehlern. Wenn der Mensch einen Fehler macht, werden diese Daten problemlos von der Hardware gespeichert. Wird dieser Fehler entdeckt, so ist es wichtig, dass man auf einen noch gültigen Datenbestand zurückgreifen kann.

Aus diesen Gründen ist es wichtig, dass die Daten zusätzlich per Datensicherung geschützt werden.

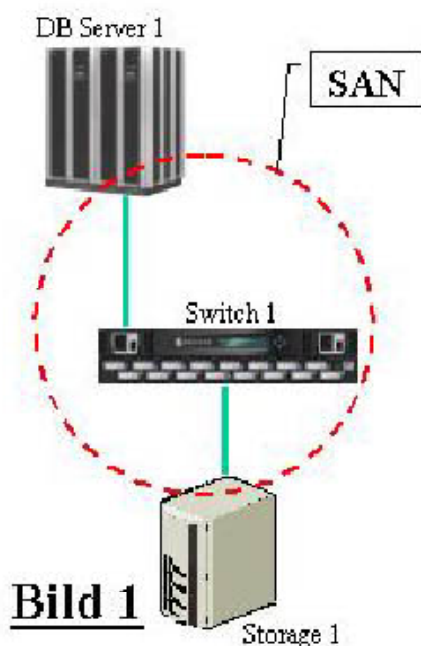
Die Sicherung größerer Datenmengen geschieht meistens auf Datenbänder (Tapes). Entweder haben die Server selber Bandlaufwerke oder aber es gibt zentrale Server die sich mit der Datensicherung beschäftigen. Ein Tool um solche Datensicherungen Netzwerkweit zu erstellen ist der „Networker“.

Storage Area Network (SAN)

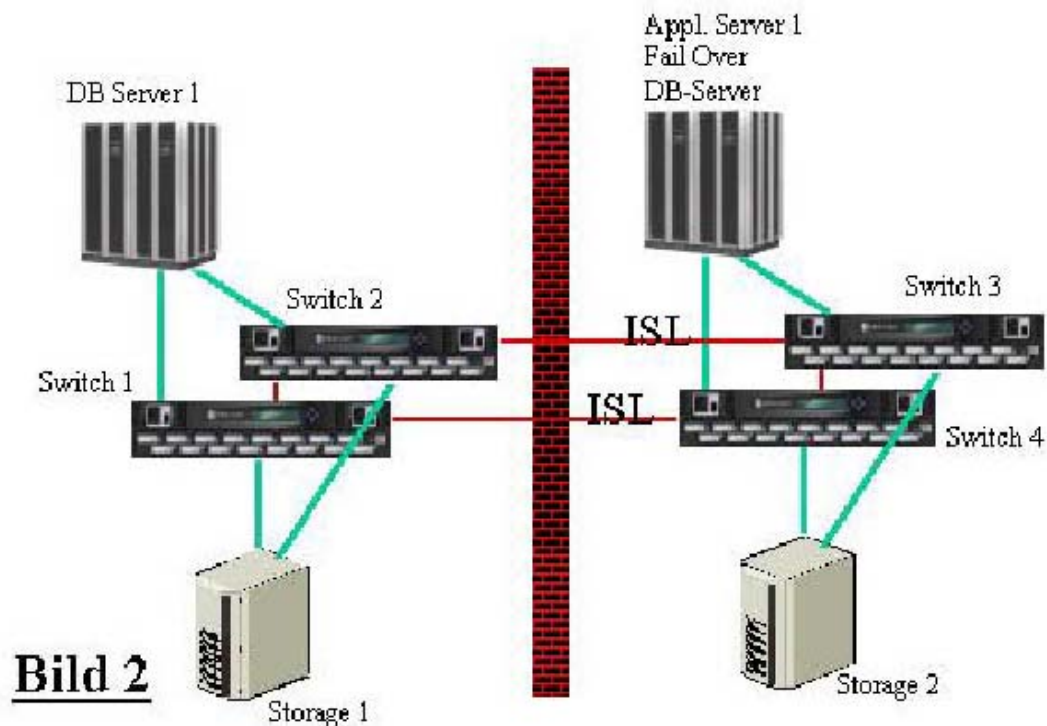
SAN ist ein Netzwerk, um Speicher Systeme mit Hilfe von Fibre Channel Komponenten (spezielle Speicherhardware) flexibel und orteungebunden an Server anzuschließen. SAN hat hierbei die Vorteile von Netzwerktechniken /-protokollen (TCP/IP), wie gute Adressierbarkeit, dynamischer Konfigurationsänderung und großen Entfernungen, und Vorteile von Speicheranschlusstechniken (SCSI), wie großer Datendurchsatz, großen Datenblöcken und gesicherter Datenübertragung, verbunden. So können Netzwerke mit Speicherkomponenten aufgebaut werden, die auch auf weite Entfernung (mehrere Kilometer) eine schnelle und gesicherte Übertragung gewährleisten.

3. Beispiel für eine HV Lösung

Nun möchte ich anhand eines einfachen Beispiels verdeutlichen, wie ein HV - Konzept für eine Datenbank aussehen kann und wie diese einzelnen Komponenten zusammenwirken. Bei diesem Konzept sollen Daten auf eine Datenbank gespeichert werden, unter Berücksichtigung aller Bereiche der Hochverfügbarkeit die weiter oben aufgeführt wurden. Hierfür benötigt man zunächst einen Datenbank Server (DB-Server), auf dem die Programme laufen, die benötigt werden, um die Daten der Anwender einzulesen und dann auf einem Storage System (z.B. EMC² Symmetrix) zu speichern. Letzteres geschieht über ein SAN, bei dem ein Switch (Netzwerkkomponente) eine logische Verbindung zwischen den Controllern (Anschlüssen) des Datenbank Servers und des Storage Systems darstellt. Dieses zeigt Bild 1. Um die Hochverfügbarkeit hier schon zu erhöhen, werden im Normalfall die Festplatten des Datenbank Servers und des Storage Systems gespiegelt, das heißt es existiert von jeder Festplatte eine 1:1 Kopie auf einer anderen Festplatte. Wenn nun eine Festplatte defekt wird, kann diese einfach ausgetauscht werden, ohne dass der laufende Betrieb unterbrochen werden muss. Des weiteren bieten moderne Storage-Systeme eine sogenannte Hot-Spare Funktion. Dafür sind in dem Speicherschrank eine oder mehrere Festplatten vorhanden die zunächst nicht verwendet werden. Sobald aber die Intelligenz einer Festplatte meldet das sie demnächst ein Defekt aufweisen könnte werden die kompletten Daten von dieser Festplatte auf die Hot-Spare-Festplatte kopiert. Sobald das erledigt ist arbeitet das System nur noch mit der Hot-Spare-Festplatte und die alte Festplatte kann ausgetauscht werden. Nach dem Austausch wird die neue Festplatte als Hot-Spare Bereich verwendet.



Um das SAN hochverfügbar zu gestalten, werden nun alle SAN Komponenten, das heißt alle Controller, Leitungen und Switches, doppelt ausgelegt. Um die Server ebenfalls hochverfügbar zu machen, gibt es auch diese doppelt. Zusammen mit zwei weiteren Switches werden diese Server räumlich von einander getrennt, das heißt es gibt zwei Rechenzentren, die durchaus einige Kilometer voneinander entfernt sein können. Hierdurch wird auch ein Disaster Protection vorbereitet. Über einen Inter Switch Link (ISL, SAN Verbindung zwischen Switches) existiert nun eine Konfiguration, bei der eine einzelne Komponente oder Server ausfallen kann, ohne dass der Betrieb gestört wird. Bei Ausfall einer SAN Komponente oder einer Leitung existiert immer noch ein zweiter Weg, über dem die Datenbank Server beide Storage Systeme erreichen können. Fällt ein komplettes Rechenzentrum aus, so ist das andere immer noch arbeitsfähig und das weiterhin mit einem hochverfügbaren SAN. Siehe Bild 2.



Damit die beiden Server sich gegenseitig überwachen existiert eine Cluster Foundation (CF). Die CF ist eine Lebendüberwachung über meistens 2 herkömmliche LAN Verbindungen. Über diese Verbindungen ist es den Servern möglich zu kontrollieren ob der Partner noch funktionsfähig ist. Diese Überwachung und die Ein- und Ausgliederung aus dem Cluster ist in der CF-Software integriert.

Der komplette Cluster wird überwacht und administriert über die Cluster Console die auch an einer der CF Leitungen angeschlossen ist.

Im Normalbetrieb arbeitet der erste Server als Datenbank Server (DB Server 1) und der zweite Server als Application Server, auf dem Anwendungsprogramme der Benutzer laufen, welche sich dann an den DB-Server 1 verbinden, um Daten von der Datenbank zu holen oder in die Datenbank abzulegen.

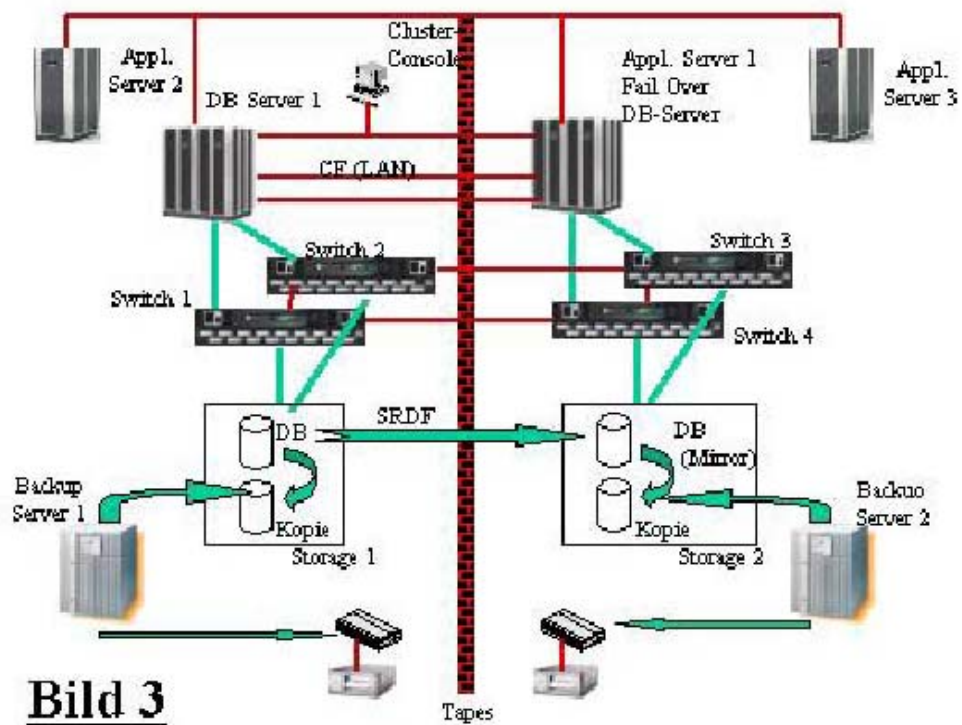
Wenn nun der DB Server 1 ausfällt, bemerkt dieses der zweite Server über die CF und ändert automatisch seine Funktionalität in einen Ersatz DB Server (Fail Over DB Server). Im Normalfall stehen weitere Application Server zur Verfügung (wegen Disaster Protection in jedem Rechenzentrum), die den Wegfall des ersten Application Servers (der jetzt ja als DB Server dient,) kompensieren.

Das zweite Storage System enthält einen kompletten Spiegel der Daten (Mirror) des ersten Storage-Systems. Die Synchronisation geschieht über mehrere SRDF (Symmetrix Remote Data Facility) Leitungen welche die beiden Storage-Systeme verbinden. Im Normalbetrieb greift der DB-Server 1 auf das erste Storage System zu. Fällt nun dieses Storage System aus greift der DB Server 1 auf den Mirror auf dem zweiten Storage System zu. Ähnlich funktioniert das Ganze im Fehlerfall mit dem Fail Over DB Server. Auch dieser greift zunächst auf das erste Storage System und erst bei Ausfall dieses System auf das zweite Storage System zu.

Durch diese Konfiguration erhält man eine sehr hohe Verfügbarkeit und Disaster Protection.

Um nun auch noch eine Datensicherung zu realisieren, gibt es zwei weitere Server, die als Back Up Server dienen. Diese greifen auf eine lokale Kopie der Storage Systeme zu, die temporär erstellt wird. Die Daten, die gesichert werden sollen, werden von den Datenbank Servern auf Datenbändern (Tapes) zur Archivierung gespeichert.

Das Bild 3 zeigt nun die komplette Lösung mit allen Komponenten.



4. Quellen und Links

- [1] <http://www.fujitsu-siemens.de/rl/aboutus/index2.html>
- [2] http://extranet.fujitsu-siemens.com/cisnet/cis/cis_cibs/cps_solution_en.html
- [3] products² CD Stand November 2001 / 2nd release