Ein **Datenbanksystem** **verwaltet**

- **dauerhaft**
- **große Mengen** von (**strukturierten**) **Daten**
- für **viele Benutzer**(**-gruppen**) mit unterschiedlichen Nutzungswünschen
- **effizient** und
- **sicher**, **d.h. zuverlässig**, **korrekt** und **vertrauenswürdig**;
- es bearbeitet also (ad-hoc und eingebettete) **Anfragen** und **Änderungen**.

Das System läuft.

Die Daten stimmen.
Die Operationen auch.

Die Benutzer sind authorisiert.

Das System läuft.
selbst bei Hardwareausfall,
Softwareabstürzen,
sehr hohem Durchsatz.

Die Daten stimmen mit der realen Welt überein.
Die Daten sind erforderlich.
Es gibt keine Widersprüche.
und keine Datenlücken (Vollständigkeit).

Die Operationen stimmen auch. Es läuft das Originalprogramm.
Es gibt keine (Ver-)Fälschungen,
keine Trojanischen Pferde,
keine Viren.

Die Benutzer sind authorisiert.
Es gibt keine Maskeraden (Vortäuschung falscher Identitäten),
Handlungen können Benutzern zugeordnet werden.
Pseudonyme (mehrere Kennungen pro Benutzer) sind manchmal nützlich.

Wirksame Sicherheitsmaßnahmen

Das System läuft.

- Redundanz (z.B. Stromversorgung, Sicherungskopien, Plattenspiegel, mehrfache Prozeßausführung, Netzwerke mit mehreren Wegen)
- Isolation (z.B. Zugangsschutz (räumliche Trennung), Trennung vom Netz),
- Protokollierung und Eindring-Überwachung

Die Daten und Operationen stimmen.

- Integritätsbedingungen
- Kryptographie: Redundante Codes (Veränderungen von Daten und Operationen können erkannt und ggf. korrigiert werden),
  Digitale Signaturen (Authentizität der Daten und Operationen).

Die Benutzer sind authorisiert.

- Benutzeridentifikation / -authentisierung, Benutzergruppen, Rollen,
- Sichten für Benutzergruppen,
- Zugriffskontrolle (Zugriff auf Daten verhindern),
- Kryptographie: Verschlüsselung (Interpretation der Daten verhindern)