Prof. Dr. Holger Schlingloff

Institut für Informatik der Humboldt Universität

und

Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik

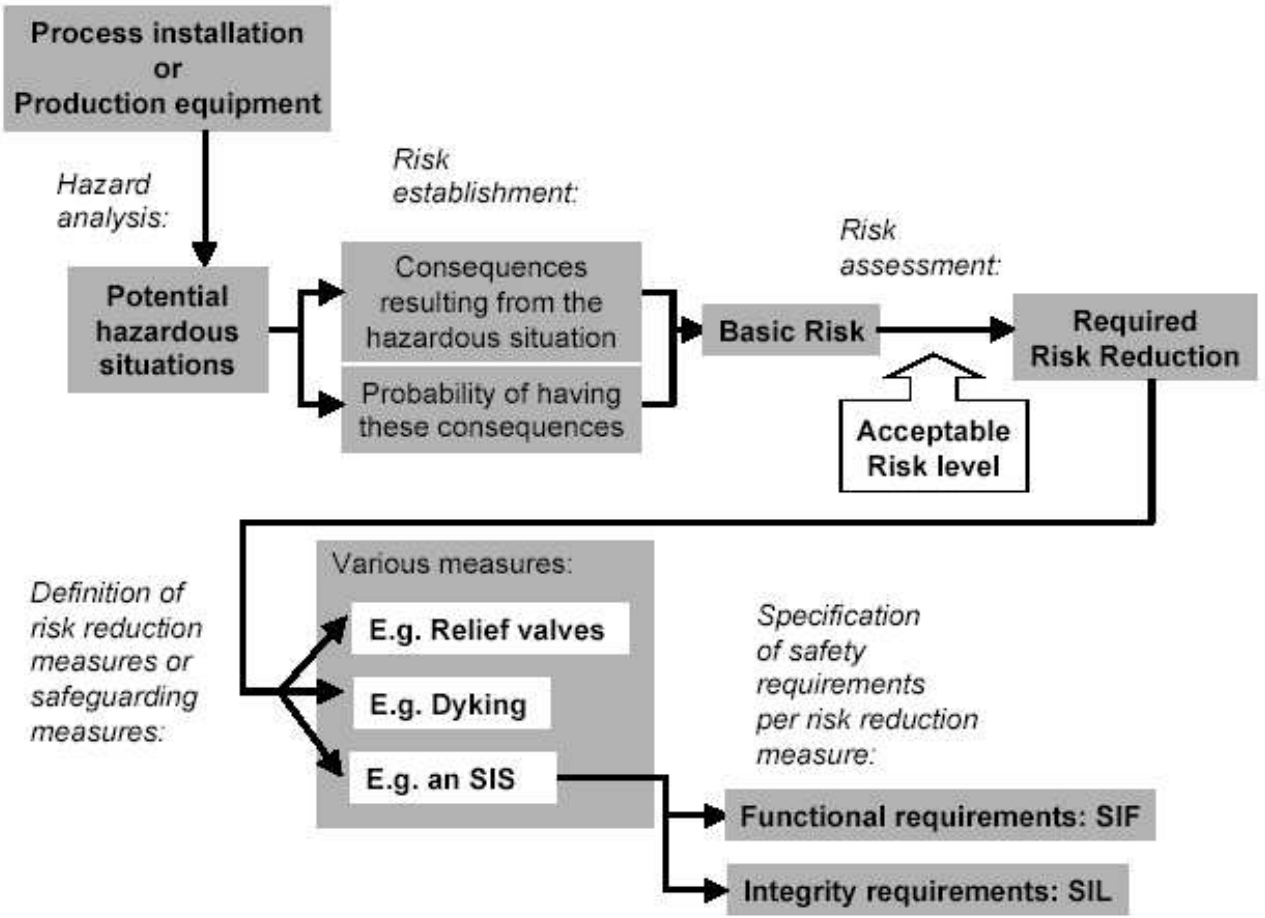
Fraunhofer Institut
Rechnerarchitektur
und Softwaretechnik

- Gefährdung: potentielle Schadensquelle
- Risiko: Verbindung / Kombination der Auftretenswahrscheinlichkeit eines Schadens und des zugehörigen Schadensausmaßes

Risiko = Eintrittswahrscheinlichkeit * Schadensausmaß

- Auftretenswahrscheinlichkeit: der Parameter des Risikos, der Auskunft über die Wahrscheinlichkeit gibt, mit der eine identifizierte Gefährdung bzw. ihre Ursache in der Praxis tatsächlich auftreten könnte.
  - Eintrittswahrscheinlichkeit
  - Entdeckungswahrscheinlichkeit
  - Möglichkeit zur Gefahrenabwendung
- Schadensausmaß: qualitatives Maß für die möglichen Folgen / Konsequenzen einer Gefährdung

- Sicherheit: Freiheit von nicht akzeptablen Risiken



Fraunhofer Institut Rechnerarchitektur und Softwaretechnik

- medizinisches Bestrahlungsgerät
- zwischen 1985 und 1987 mehrere Unfälle mit Toten
- große öffentliche Aufmerksamkeit, gut dokumentiert

- Vorgängermodelle ohne Computersteuerung
  - für zusätzliche Komfortfunktionen nachrüstbar
  - mechanische und elektrische Sicherheitseinrichtungen
- Neue Teilchenbeschleunigungstechnologie
  - Dual mode: Elektronen- und Photonenstrahl, variable Applikationstiefe
  - Computersteuerung (PDP-11) notwendig
  - Sicherheitsfunktionalität in Software verlagert

- Aufgaben der Steuerung
  - Positionierung des Behandlungstisches
  - Einstellen der Strahlungsenergie
  - Formung und Abflachung des Strahls (mechanisch)
- Architektur
  - Reuse von früheren Softwaremodulen
  - ehemalige Komfortfunktionen jetzt sicherheitsrelevant
- Mensch-Maschine-Schnittstelle
  - Operator Interface, schnelle Eingabemöglichkeit
  - Abbruch durch „suspend“ und „pause-resume“
  - kryptische Fehlermeldungen, häufig auftretend
  - keine zuverlässige visuelle Rückmeldung

- Sicherheitsanalyse mit Fault Trees
  - Konzentration auf Hardwareausfälle
  - Programmierfehler werden anderweitig behandelt
  - nicht dokumentierte / begründete Annahmen
    - „ Computer selects wrong energy“: 10^{-11}
    - „ Computer selects wrong mode“: $4*10^{-9}$

- Unfälle wurden anfänglich nicht gemeldet
  - kommerzielle Interessen, Schadensersatzklagen
  - Kette der Weiterleitung nicht durchgängig, Behörde erfährt nur von 1% aller Unfälle
  - Keine Rückmeldung zu anderen Installationen

- Fehlerpatches
  - fehlertolerante Positionssensoren für Tisch
  - „ Sicherheitsverbesserung um 5 Größenordnungen“
  - erneuter Einsatz ohne genaue Fehleranalyse
  - Kliniken beginnen selbst Sperrvorrichtungen zu bauen
  - Ärzte beginnen mit der Fehlersuche
  - Anweisung: Abkleben der „Cursor-Up“-Taste

- Softwareprobleme
  - Software wird (bis heute) geheim gehalten
  - Parallele tasks, gemeinsame Variable, racing, Überlauf

- zusätzliche Sicherheitsvorrichtungen
  - Nothalt-Knopf
  - Unabhängige Überwachung der Tischposition
  - Unabhängige Hardwaresperre für Strahl

  - Software-Nothalt
  - Neue Benutzungsoberfläche
    - visuelles Feedback
    - Fehlermeldungen

  - Trennung von Sicherheits- und Benutzungsfunktionalität

- Lektionen
  - blindes Vertrauen der Benutzer in die Software
  - Zuverlässigkeit ist nicht gleich Sicherheit
  - Fehlerverfolgung
  - Trennung von Sicherheits- und Benutzungsfunktionen
    - ProfiSafe
  - Sicherheitsdesign *vor* der Systemimplementierung

- Risiko = Eintrittswahrscheinlichkeit * Schadensausmaß
  - z.B. Aktienkursverlust
- Problem bei sehr kleinen und sehr großen Zahlen
  - sehr großer Schaden bei sehr geringer Wahrscheinlichkeit
- Problem der numerischen Einschätzung
  - Kosten bei Personenschaden?
  - Wahrscheinlichkeit von Katastrophen?

- ALARP-Prinzip: „As Low As Reasonably Possible“
  - Wenn ein Risiko mit vertretbarem Aufwand reduziert werden kann, sollte dies getan werden
  - Oft auch: Wenn das Risiko nicht reduziert werden kann, muss der Nutzen des Systems (Nutzungsdauer * Gewinn) den Schaden übersteigen

	U.S. Automobiles	U.S. Commercial Aircraft
Deployed Units	~100,000,000	~10,000
Operating hours/year	~30,000 Million	~55 Million
Cost per vehicle	~$20,000	~$65 Million
Mortalities/year	42,000	~350
Accidents/year	21 Million	170
Mortalities / Million Hours	0.71	6.4
Operator Training	Low	High
Redundancy Levels	Brakes only	All flight-critical systems

- Katastrophen werden subjektiv höher gewichtet

- Oftmals nur qualitative Abschätzung
  - Gefährdungsklassen (z.B. zivile Luftfahrt)
    - Catastrophic (10^{-9}/h): Kein sicherer Flug möglich
    - Critical (10^{-7}/h): Große Beeinträchtigung, Todesfälle
    - Major (10^{-5}/h): Signifikante Probleme, Verletzungen
    - Minor (10^{-3}/h): Geringe Reduktion der Sicherheitsfunktionen
    - No effect (10^{-2}/h): Kein Einfluss auf die Sicherheit
  - Eintrittswahrscheinlichkeitsklassen
    - Extremely improbable (< 10^{-8}/h)
    - Extremely remote (10^{-6}/h - 10^{-8}/h)
    - Remote (10^{-5}/h - 10^{-6}/h)
    - Reasonably probable (10^{-3}/h - 10^{-5}/h)
    - Frequent (10^{-3}/h - 1/h)

- „ Pareto-Regel“: 80% der Probleme stammen aus 20% der Risiken
- Zweck
  - Identifikation von Ereignissen die zu Unfällen führen können
  - Auswirkungen auf das System analysieren
- Techniken
  - FMEA: Failure modes and effects analysis
  - FMECA: Failure modes, effects and criticality analysis
  - FTA: Fault tree analysis
  - ETA: Event tree analysis
  - HAZOP: Hazard and operability studies

- Failure Mode and Effects Analysis
  - verbreitetste Methode
  - Konsequenzen von Komponentenversagen
  - Vorwärtsanalyse
- Produkt- und Prozess-Sicht
  - System- oder Produkt-FMEA
    - systematische Analyse der möglichen Funktionsfehler
    - Berechnung der funktionalen Zusammenhänge der Komponenten
  - Prozess-FMEA
    - Analyse möglicher Fehler im Herstellungsprozess
    - Berücksichtigung der beteiligten Akteure
- Failure Mode, Effects and Criticality Analysis
  - zusätzliche Spalten
    - Kritikalität
    - Maßnahmen

- Analyse jeder Komponente
  - mögliche Fehler
  - Ursachen für den Fehler
  - verbundenes Risiko
- Risikoprioritätszahl = A * E * B
  - A = P(Auftreten): Eintrittswahrscheinlichkeit
  - E = P(Entdeckung): Wahrscheinlichkeit, dass Fehler sich auswirkt bevor er entdeckt und beseitigt werden kann
  - B = Bedeutung: Gewicht der Folgen

1. Abgrenzen der Betrachtungseinheit

   (Systemstruktur)

2. Funktionsanalyse

   - Zusammenhänge den einzelnen Elementen aufzeigen
   - Funktionskritische Merkmale erkennen

3. Fehleranalyse

   Ausfallart und -ursachen

   Ausfallfolgen

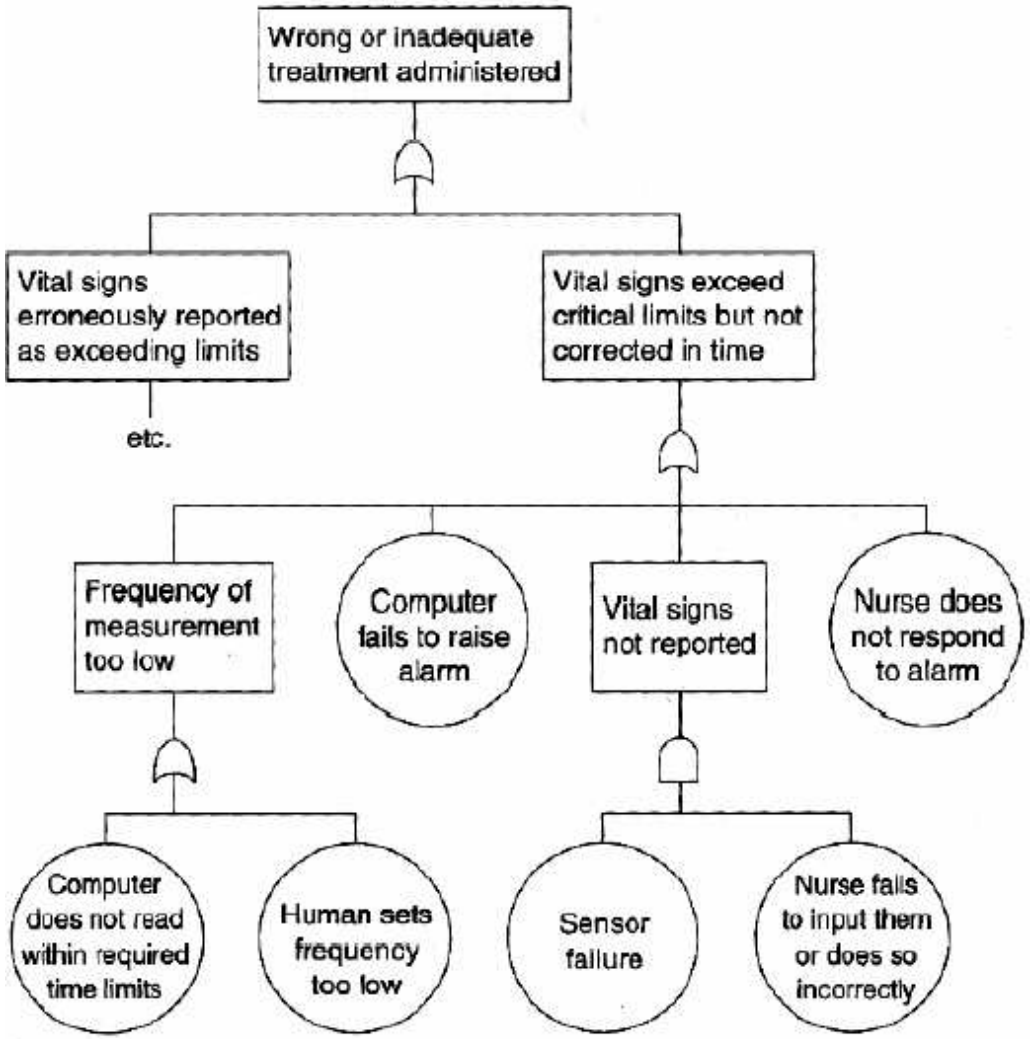
4. Risikobewertung

5. Verbesserungsmaßnahmen

- Vermeidung von Fehlerursachen!

- Bei hohen Auftrittswahrscheinlichkeiten
  - Qualitätssicherung stärken
- Bei geringen Erkennungswahrscheinlichkeiten
  - Möglichkeit der Fehleroffenbarung einbauen
- Bei schwerwiegenden Folgen
  - Auswirkungen begrenzen

- Top-Down
  - Wurzelknoten: Schadensereignis
  - Nachfolger: Ereignisse die dazu führen
  - Und-/ Oder-Baum



- Vorwärtsanalyse (umgekehrte Richtung)
  - Start mit Schadensereignis
  - Konsequenzen
  - erweitert um Wahrscheinlichkeiten

- Hazard and operability studies
- Identifikation von Gefährdungen als Abweichungen vom Normalbetrieb
  - Definition der Aktivitäten
  - Identifikation denkbarer Abweichungen
  - Anhand von Wörtern der Spezifikation
    - Leitwort + Systemfunktion = Abweichung
    - Kein, zuviel, zuwenig, teilweise, gleich, später, …
    - Druck, Temperatur, Durchsatz, Antrieb
  - Ursachen und Auswirkungen
  - Maßnahmen

RISK		Probability				
		Very High	High	Medium	Low	Very Low
Conse-quence	Very High	Very High	Very High	High	High	Medium
	High	Very High	High	Medium	Medium	Low
	Medium	High	Medium	Medium	Low	Low
	Low	High	Medium	Low	Low	Very Low
	Very Low	Medium	Low	Low	Very Low	Very Low