Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

International Association for PSAM

HOCHSCHULE FÜR TECHNIK, WIRTSCHAFT UND VERWALTUNG ZÜRICH

Laboratorium für Sicherheitsanalytik
INSTITUT FÜR ENERGIETECHNIK

Risk Analysis Related Issues of IT-Systems: Case Studies in Review

Frank Möhle
Andreas Fischer

University of
Applied Sciences Zurich

Ralf Mock

Swiss Federal Institute
of Technology Zurich

PSAM 6, San Juan, Puerto Rico USA, June 27th, 2002

Table of Content

- **Positioning of Risk Analysis**
  - in a Company's Decision Making Process
  - Nuclear Power Generation
  - IT-Networks
- **A Three-step Concept of Risk Analysis**
- **Case Studies: Learning by Doing!**
  - Telecommunication
  - Banking
  - Internet Application Service
  - Educational
- **Experiences in Risk Analyses**
- **Conclusions for Risk Analysts of IT-Systems**

Positioning of Risk Analysis

- in a Company's Decision Making Process -

		Decision Level		
		Operational Control	Management Control	Strategic Planning
Decision Making	Structured	„Best Practice“		
	Semi structured	Established Risk Analysis Techniques		
	Unstructured			

M. Diergardt, ETHZ-LSA, Jan. 2002

Positioning of Risk Analysis

- Nuclear Power Generation -

System Characteristics

- **Topology**
  Complex, local
- **Stability**
  Unmodified basic system design during system operation
- **Mean Time of System Operation**
  40 to 45 years

Risk Analysis Characteristics

- **Duration (CH)**
  ≈ 3 years (without peer review)
- **Costs (CH)**
  ≈ 1.8 – 2 Mio. USD per PRA
- **Data Evaluation**
  Well developed incident and equipment documentation
- **Analysis Techniques**
  Established and approved techniques
- **Results**
  Long term usability of PRA results

Positioning of RSA-Analysis

- IT-Networks -

System Characteristics

- **Topology**
  Complex, networked
- **Stability**
  Permanent variations of hardware, software, data, etc.
- **Mean Time of System Operation**
  ≈ 2 years

Risk Analysis Characteristics

- **Duration:** 3 to 6 months required
- **Costs:** ????
- **Data Evaluation**
  Worse incident and equipment documentation
- **Analysis Techniques**
  Established and approved checklist approaches (“Best Practises”)
- **Results**
  - Short term usefullness
  - Applying Occam's razor

A Three-step Concept of Risk Analysis

Step 1 Implementation of simplified risk analysis techniques • Fast system screening • Efficient risk ranking • Highly practicable techniques. **Tasks** • Company specific questionnaires • Simplified FMEA	**Step 2** Creation of (simplified) system models • In-depth analysis of operation problems specified in Step 1 • Usage of new and /or advanced modelling techniques **Tasks** • Generalized Stochastic Petri Nets • Model parameter assessments by expert judgments

Step 3
Refining the results of Step 1 and 2

Tasks
- Model upgrade
- Plant specific data evaluation for parameter assessments

Case Studies: Learning by Doing!

- **Branch:** Telecommunication
- **Case study:** Swisscom AG
- **Goals**
  - Fast system screening
  - Hot spot identification
  - Identification of financial risks
- **Techniques:** Step 1 & 2 approaches

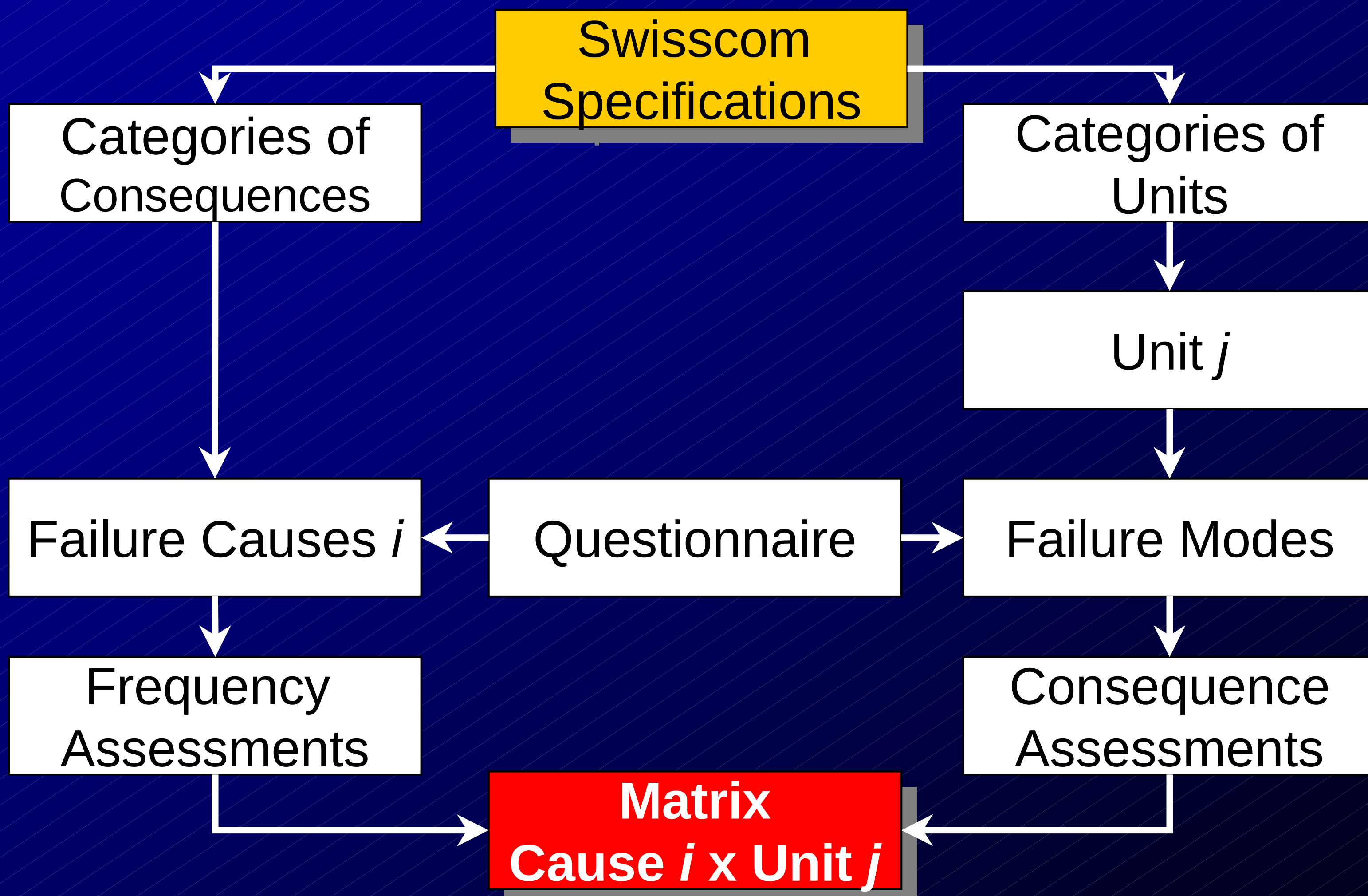
- **Branch:** Banking
- **Case study:** UBS Warburg
- **Goals**
  - Fast system screening
  - Hot spot identification
  - Identification of business risks
- **Techniques:** Step 1 approaches

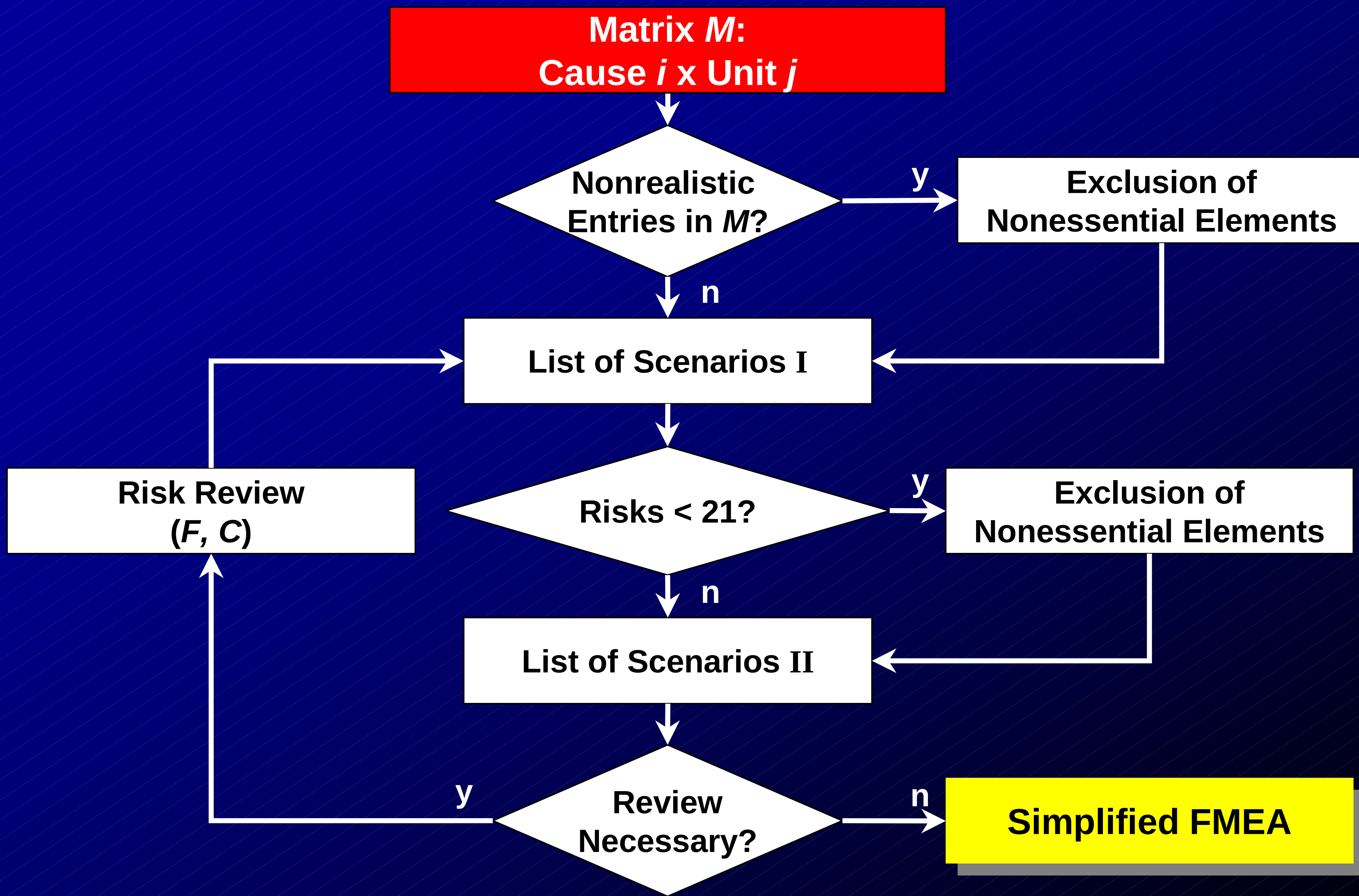
- **Branch:** Internet application service
- **Case study:** ASP
- **Goals**
  - Fast system screening
  - Assessment of reliability figures
  - Comparison of design versions
- **Techniques:** Step 1 - 3 approaches

- **Branch:** Educational
- **Case study:** Univ. of Applied Sciences.
- **Goals**
  - System modelling
  - Log-file analysis
- **Techniques:** Step 3 approaches

Case Study: Telecommunication

Step 1: Simplified FMEA Methodology




Matrix M:
Cause i x Unit j
Nonrealistic Entries in M?
y
Exclusion of Nonessential Elements
n
List of Scenarios I
Risk Review (F, C)
Risks < 21?
y
Exclusion of Nonessential Elements
n
List of Scenarios II
y
Review Necessary?
n
Simplified FMEA

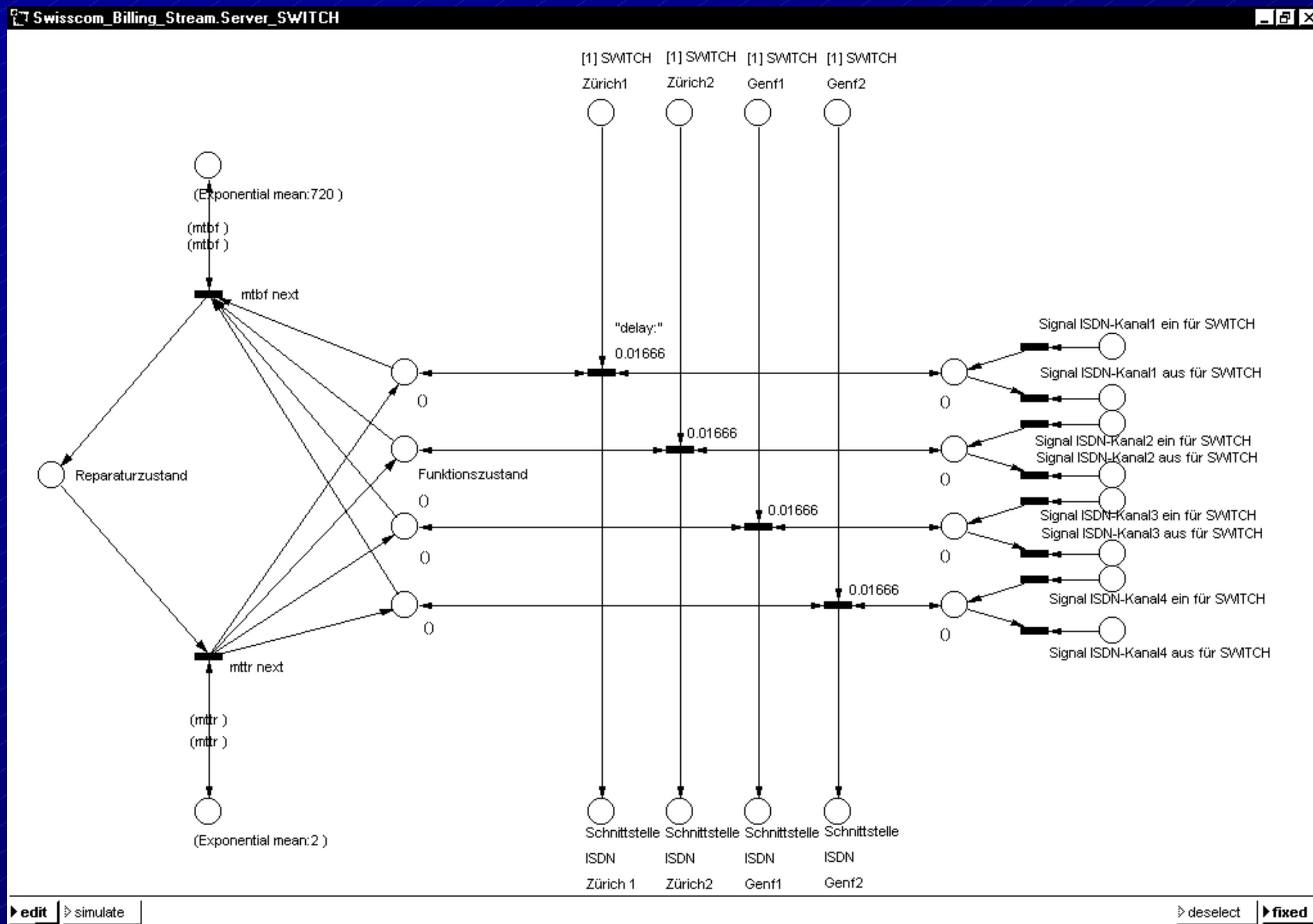
Result: Simplified FMEA of all Modules (Excerpt)

Module	Unit	Item	Failure Mode	Failure Causes	Consequence	*F*	*C*	Risk
SAP	Application	Application SW	Modification	Maloperation	Inconsistent billing	4	7	28
Gateway	Network interface	Router ISDN	Failure	Maloperation	No billing	5	5	25
Gateway	Information	Reference data	Stolen/ deleted	Vandalism	Perturbed billing	4	6	24
Gateway	Information	Reference data	Stolen/ deleted	Organisation problems	Perturbed billing	4	6	24
LAN	Information	Reference data	Unapproved insight	Organisation problems	Loss of image	4	6	24

Risk =
- **Frequency • Consequence**
- ***F, C*: 10 categories each**

Risk Ranking
- **Maximum: 100**
- **Medium: 25.**

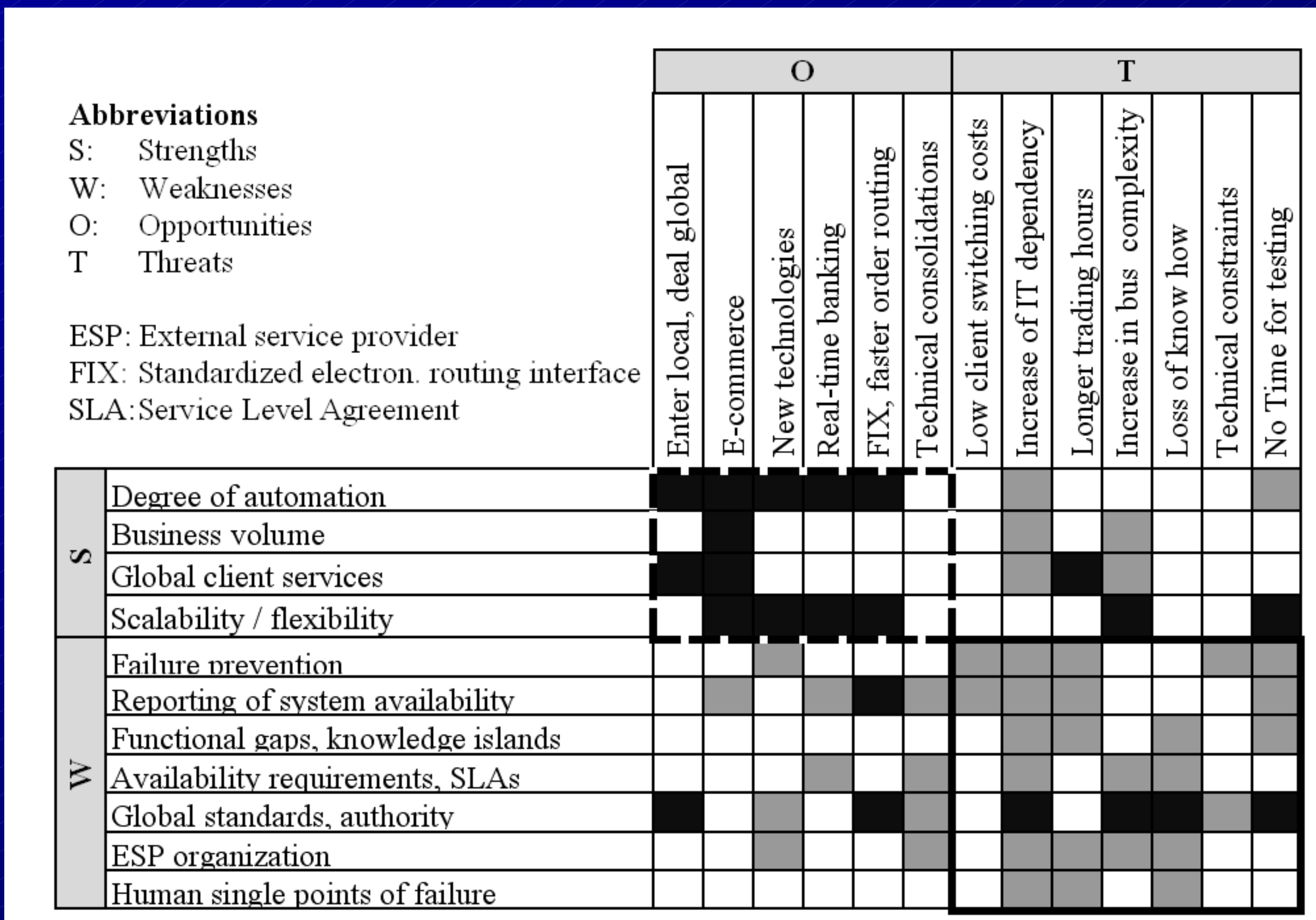
Step 2: Generalized Stochastic Petri Net



Bottle neck identification of data flow

Case Study: Banking

Step 1: SWOT-Analysis and FMEA of CaTS



Squares

Interferences

- Black: positive
- Grey: negative
- White: balanced

SWOT: Strengths/Weaknesses, Opportunities/Threats

Adopted FMEA Technique: Methodological Steps

A: Starting Point

Function	→ Business executive flow (e.g., trades from CaTS to X")
failure	→ Set of failing configuration items (CI)
affecting	
CaTS-	→ Capital Market Trading System
subsystem *i*	→ **Layers**

Layers

Technical: CI_T: {server, …}

Application: CI_A: {file transfer protocol, …}

Subsystems: CI_S: {UBS specific application, …}

B: Assessments

Expert Judgements (Using 10 Classes Classsification Schemes)

• TTR_i : *T*ime *t*o recover of subsystem *i*) • $CI_{R,i}$: „CI-reliability“	} CI-availability $A_i = TTR_i \cdot CI_{R,i}$
• $R_{fin,i}$: Financial risk • $R_{rep,i}$: Reputation risk	} Impact of *i* with regard to CaTS $I_{i,\text{ CaTs}} = R_{fin,i} \cdot R_{rep,\,i}$
• $I_{f,\,i}$: Impact	} Function impact with regard to *i*

C: Computations

- Function impact with regard to CaTS: $I_{f,CaTS} = I_{i,CaTS} \cdot I_{f,i} \cdot \left[\sum_{i=1}^{n} I_{f,i} \right]^{-1}$
- Function priority number: $P_f = A_i \cdot I_{f,\,CaTS}$

Failing Function *f*	Affected Subsystem *i*	Impact	Failure Cause (Failing CI)	Availability		Function Impact $I_{f,\,CaTS}$	Function Priority P_f
				CI	A_i		

D: Some Results

Most „risky“ functions

- Orders and cancellation requests to SWX (derivates, shares)
- Market funds to CaTS (derivates)
- Orders and cancellations to SWX (bounds)
- Market funds to CaTS (shares), ….

Case Study: Internet Application Service

Step 1

- **Definition of functional modules**
  - Characterization of the ASP data center network
- **Fishbone Diagram**
- **FMEA**

Results: „most important risks“

- „Loss of privacy“ due to
  - Data manipulation
  - Hacker attacks
- Server failures due to data manipulation
- Viruses, hacker attacks, etc.

Step 2 + 3

Server availabilities in dependancy of operating systems

- Markovian state diagram

Results: single server system

- **Operating System**: WINDOWS 2000 is ≈ 3x more stable than WINDOW NT 4.0
- **Limitations:** Poor database, exclusion of human factors, etc.

Case Study: Educational

- In Progress-

Step 3

Usage of Logfiles for Risk Analysis Purposes

- Solving the „filtering problem"
- Triggering sophisticated system models or simulation

Experiences in Risk Analyses

	SAG	UBS	ASP	UAS
Resources				
• Project duration (months)	6	3	3	?
• Man power	team	team	small team	team
Analysis goals				
• Simple risk representation	must	must	must	na
• Minute availability figures	no	may be	may be	nice to have
• Risk assessment	must	nice to have	must	nice to have
• Fast system screening	must	must	must	na
• System modeling	nice to have	nice to have	may be	must
• System optimization	must	must	must	na

Legend: no — may be — nice to have — must

Conclusions for Risk Analysts of IT-Systems

A successful analysis meets the IT-branch's demands

- Implementation of fast system screening techniques
- Results in traffic light representation
- Clear suggestions for system optimization measurements

Areas of Conflict

- The preferred "quick and dirty" techniques will be soon obsolete
- Established risk analysis system modeling techniques are ponderous and too slow

The IT-branch Rejects

- Complex system modeling
- Detailed availability analyses (i.e. no figures)

Challenges

- Integration of all available knowledge sources
- Reconsideration of accustomed analysis approaches
- Meeting the challenge of new demands, e.g. vulnerability analysis