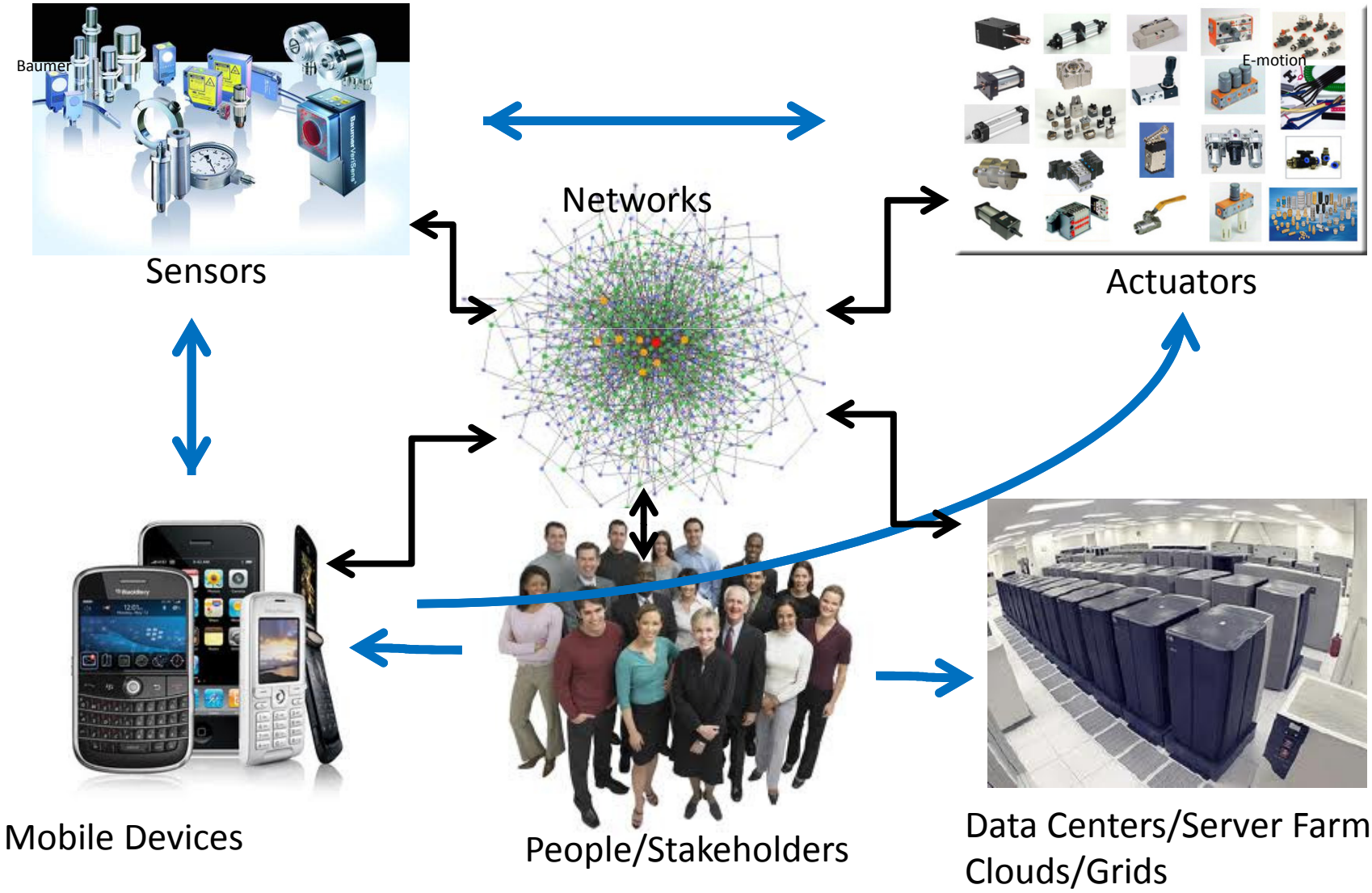
Towards Highly-Available Open Systems: the SHIP-IT Approach

高可用性オープン·システムに向けて：SHIP-ITのアプローチ

Miroslaw Malek
Humboldt University Berlin

DEOS Meeting
Tokyo, March 7, 2012

The Age of Open Systems
- An ever more Complex World



The Permanent Challenge

- Ever-increasing systems **complexity**
  - Growing connectivity, chip density and interoperability
  - Growing number of functionalities
- Increasing **uncertainty**
  - Ever-growing number of attacks and threats, novice users and third-party or open-source software, COTS
  - Ever new failure modes
  - Dynamicity (frequent configurations, reconfigurations, updates, upgrades and patches, ad hoc extensions)
- Increasing real-**time** requirements
  - Systems proliferation to applications in all domains of human activity where many of them require real time
  - Growing users expectations regarding timeliness

Therefore, dependability is and will remain the permanent challenge.

The Three Tyrants*

- **Complexity**
  - Growth in practice can hardly be stopped
  - Striving for new functional features
  - Striving for improved properties (e.g., higher performance)
  - Striving for having everybody and everything on the network
  - Open system, adding environment, including people
- **Time**
  - Time can neither be stopped nor regained
  - Disparity between physical and logical time

- **Uncertainty**
  - Can be controlled to a limited extent, we have "to cope" with it
  - New failure modes, new environmental conditions, new attacks

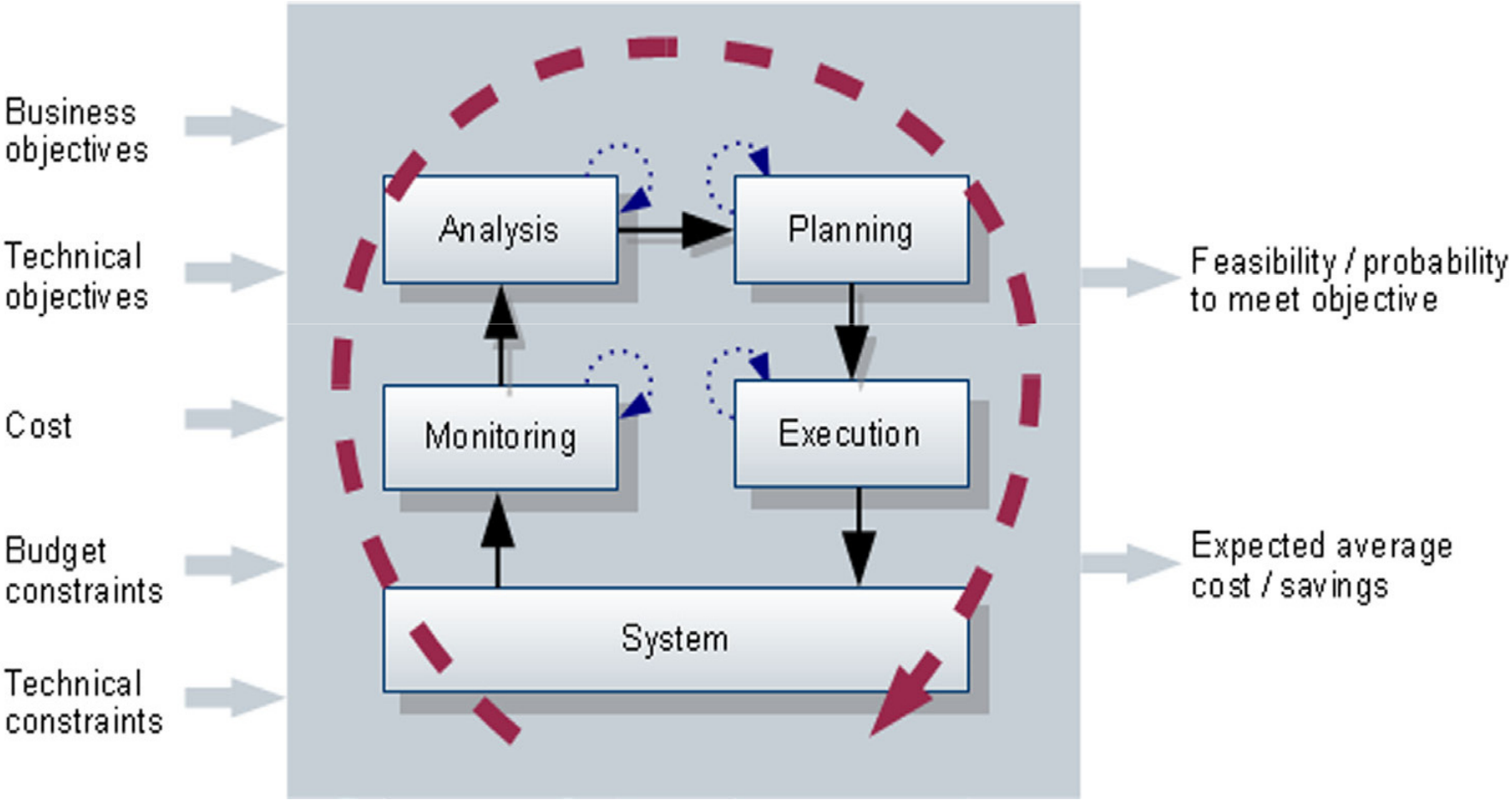
***Inspired by a quote from Johann Gottfried von Herder (1744-1803): Die zwei größten Tyrannen der Erde: der Zufall und die Zeit**
"Two biggest tyrants on Earth are: the chance and the time."

Our Philosophy
and a holistic Approach

- Faults, errors and failures are common events so let us treat them as part of the system behavior and learn how to cope with them (include them upfront in specification)

- Monitor, Analyze, Plan and Execute (along the lines of IBM‘s autonomic computing)

Methodology



Goldszmidt, Malek, et al, Wheels within a Wheel, 2012

Our approach is based on dual focus:

1) **Comprehensive online service availability planning, control and evaluation (SHIP-IT) –** covered in this talk, and

2) Proactive fault management including seamless failure avoidance techniques using runtime monitoring and prediction.

What is SHIP-IT?

- SHIP-IT is a holistic methodology and a software tool that encompasses modeling of **S**oftware, **H**ardware, **I**nfrastructure, **P**ersonnel and **IT**-organization to control and optimize business processes and services

- SHIP-IT combines quantitative and qualitative modeling and methods and brings together for the first time classical models such as Reliability Block Diagrams or Fault Trees with reference models such as CobiT and ITIL which incorporate IT management and organization (qq-plane)

- Developed by HUB and AvailabilityPlus, sponsored by German Government, started in April 2008

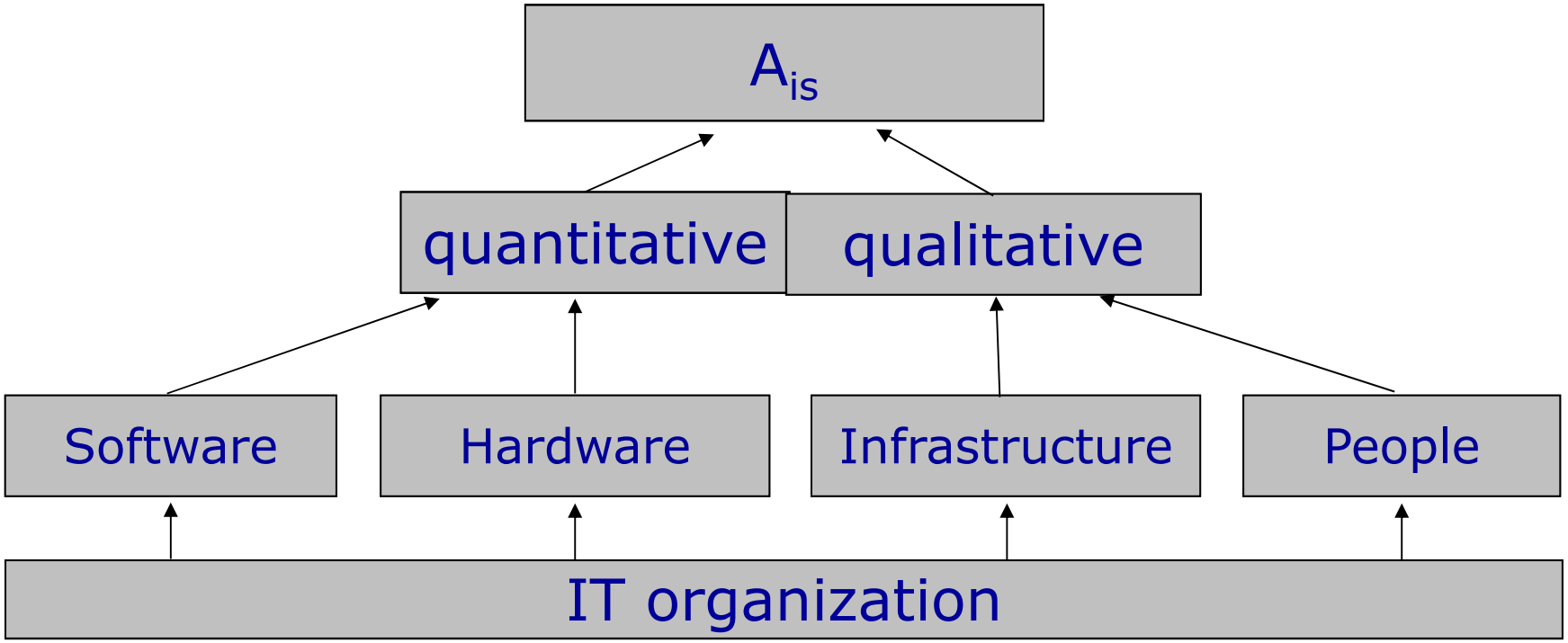
What benefits does the SHIP-IT bring?

- Comprehensive, modular, customized, evolutionary and efficient Planning and Management of Availability
- Assessment of the Availability-IS status on line and a comparison with Availability-SHOULD-BE
- Single-point-of-failure (SPOF) identification
- Process management and service optimization with respect to availability

What other factors can be managed?

- Time to Market (TTM)
- Total Cost of Ownership (TCO)
- Standardization and Certification
- Explicit qualitative assessment and management (what processes and how)

Hierarchy of SHIP-IT



Infrastructure encompasses interoperability, organization, sometimes communication and environment (the open system issues)

CobiT – IT-Control and Management

- CobiT (Control Objectives for information and related Technology) refers to control objectives which should be considered and implemented in an organization to ensure a reliable use of IT.
- For that purpose CobiT defines seven criteria arranged in the following groups:
  - Quality of IT
    - Effectiveness
    - Efficiency
  - Security
    - Confidentiality
    - Integrity
    - Availability
  - Correctness
    - Compliance
    - Reliability

CobiT and Dependability

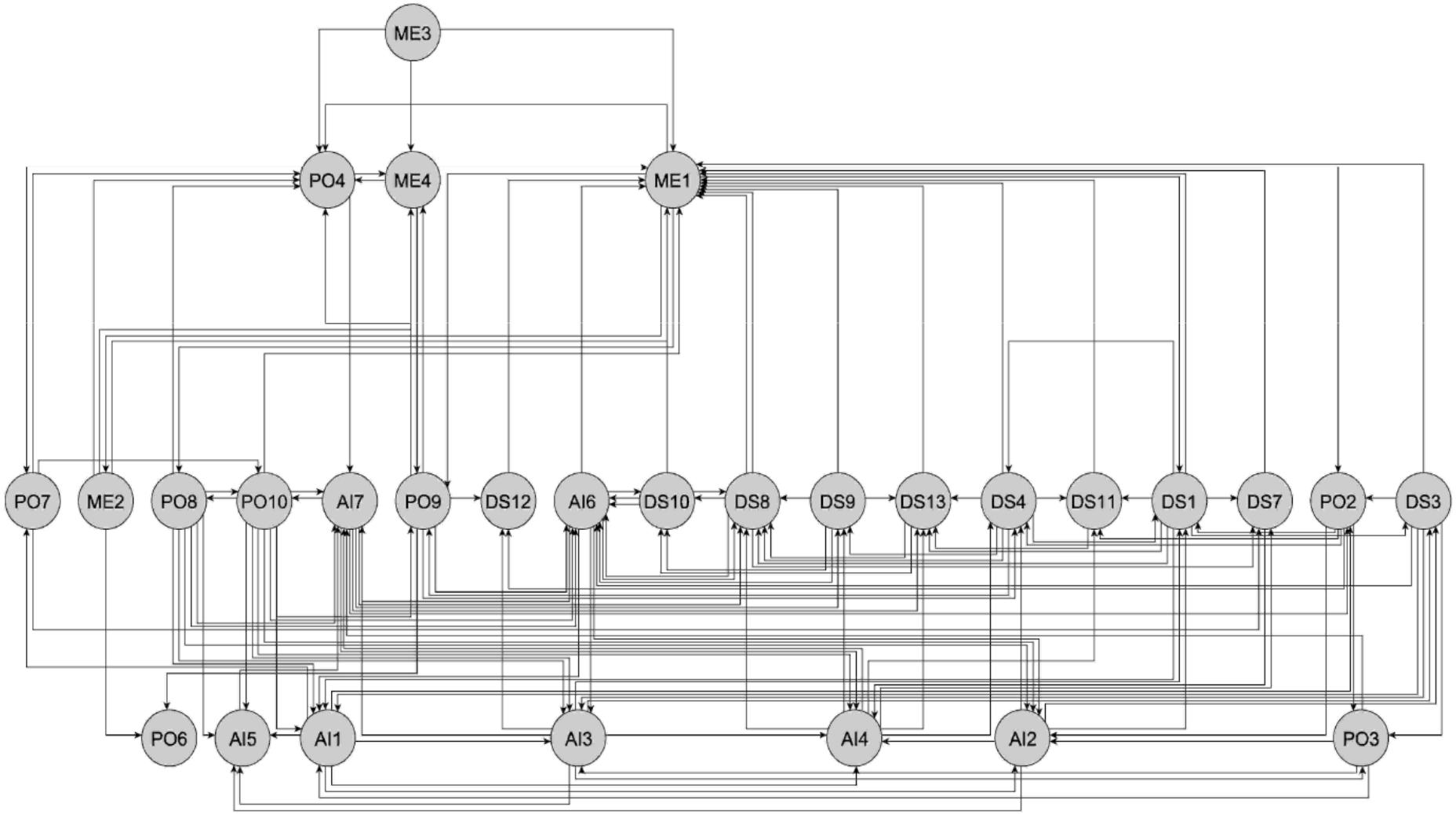
- Out of the total of 34 process areas, only 29 process areas of CobiT relevant to dependability were analyzed.
- They were selected with respect to nine areas of IT Infrastructure Library (ITIL):
  - Availability Management
  - Service Level Management
  - Configuration Management
  - Change Management
  - Release Management
  - Incident Management
  - Problem Management
  - IT Service Continuity Management
  - Capacity Management (for ITILv3)

Quantitative Approach

- IT organization can be described as the alignment of IT processes in accordance with given standards.
- Implementing IT processes in an organized manner as proposed in the generic reference models facilitates their traceability, assessability, comparability.
- This corresponds to the fulfillment level of the standards.
- We propose to use analytical approaches to the generic approaches in order to quantitatively evaluate IT organization.

[Goldschmidt, Dittrich , Malek, PRDC 2009]

Relations among CobiT Processes Concerning Dependability



What Can We Do: Process Criticality Index

- We propose to evaluate process areas by applying the process criticality index measure.

- The idea behind the process criticality index is to identify the importance of vertices with respect to the number of flows (path traversals).

- We use this centrality measure to calculate the normalized betweenness centrality of each process area in CobiT.

Criticality of CobiT Processes with Respect to Availability

Process area	C'_B in percentage	Description
ME1	23,11%	Monitor and Evaluate IT Performance
AI7	9,70%	Install and Accredit Solutions and Changes
PO9	6,23%	Assess and Manage IT Risks
DS1	6,15%	Define and Manage Service Levels
AI6	5,85%	Manage Changes
PO10	5,73%	Manage Projects
PO2	5,15%	Define the Information Architecture
PO4	4,37%	Define the IT Processes, Organisation and Relationships
PO8	4,26%	Manage Quality
DS4	3,93%	Ensure Continuous Service
AI4	3,93%	Enable Operation and Use
AI3	3,18%	Acquire and Maintain Technology Infrastructure
AI1	3,00%	Identify Automated Solutions
AI2	2,49%	Acquire and Maintain Application Software
DS8	2,44%	Manage Service Desk and Incidents
DS3	1,75%	Manage Performance and Capacity
PO7	1,60%	Manage IT Human Resources
DS13	1,14%	Manage Operations
ME4	1,09%	Provide IT Governance
DS7	1,05%	Educate and Train Users
ME2	1,04%	Monitor and Evaluate Internal Control
DS9	1,04%	Manage the Configuration
PO3	0,72%	Determine Technological Direction
DS12	0,44%	Manage the Physical Environment
DS11	0,26%	Manage Data
DS10	0,21%	Manage Problems
AI5	0,15%	Procure IT Resources
PO6	0,00%	Communicate Management Aims and Direction
ME3	0,00%	Ensure Regulatory Compliance

Open Issues

- The problem is very complex so our proposed solution is to include only selected areas directly concerning IT organization dependability and prioritize them (criticality index)
- Need for field data to verify the impact of various processes
- Using such methods should also help to analyze and rank the process areas of other reference models such as CMMI, MOF or SPiCE (but this must be tested).
- We need to solve the problem of quantifying improvement in maturity level in terms of availability enhancement

Problem: IT Planning and Control

They are:

- Ad hoc
- Arbitrarily selective
- Very little or not sustainable
- Low level of maturity
- No business process focus
- Unclear success criteria
- Do not consider the open system challenge

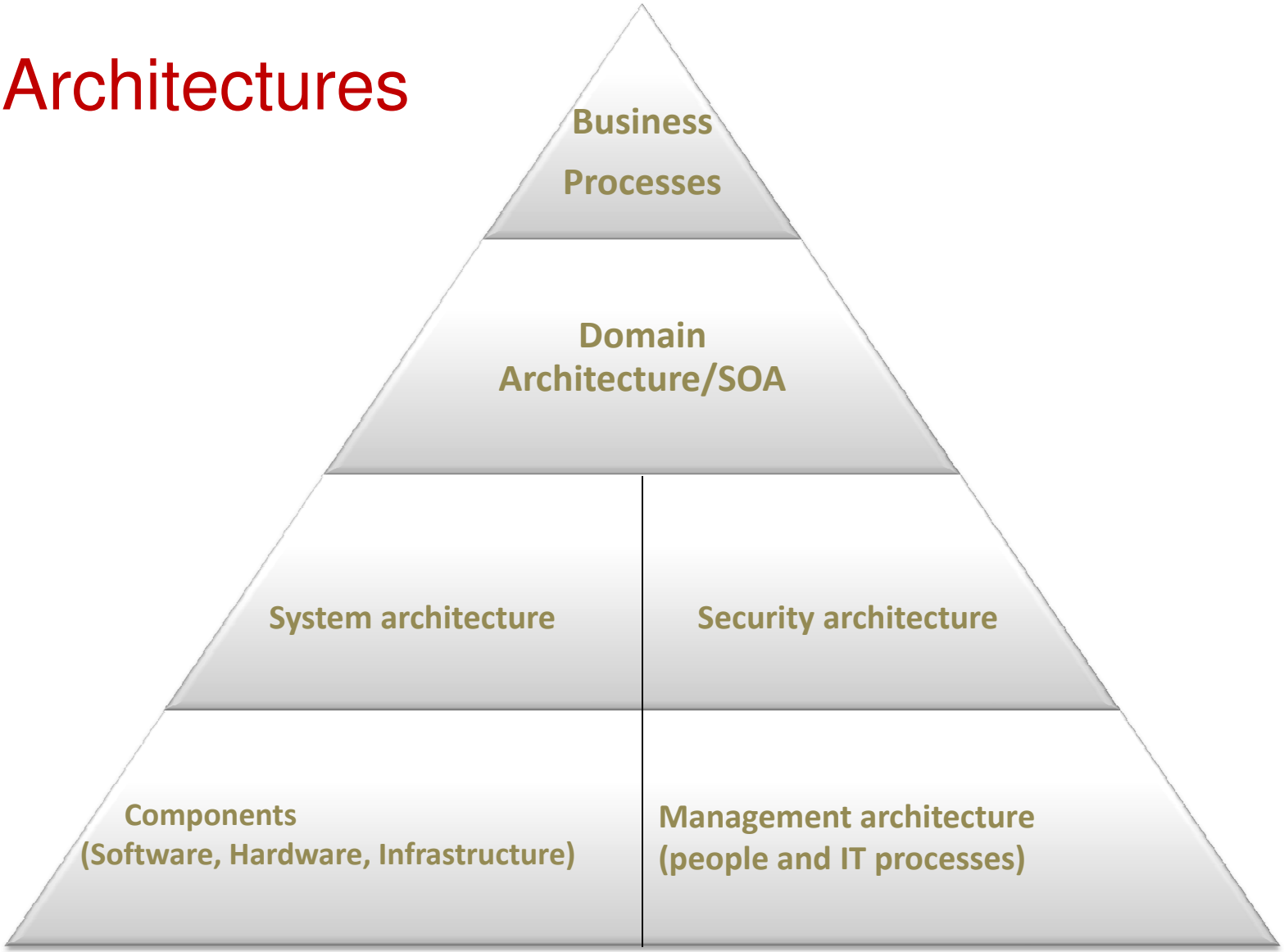
Consequences

- Downtime
- High cost
- Unclear IT contribution

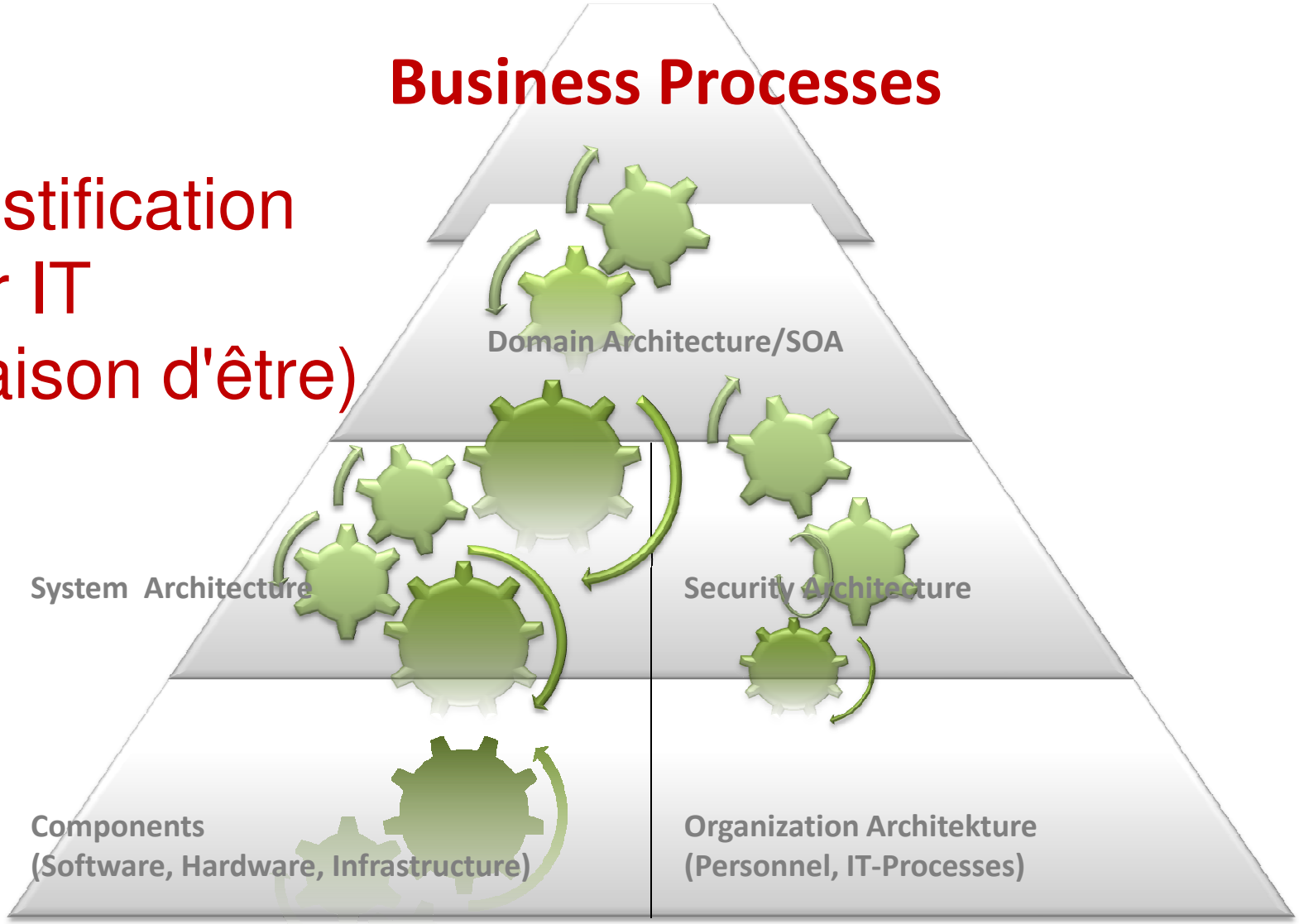
The Solution – SHIP-IT

Comprehensively planned and controlled IT architecture with focus on business processes

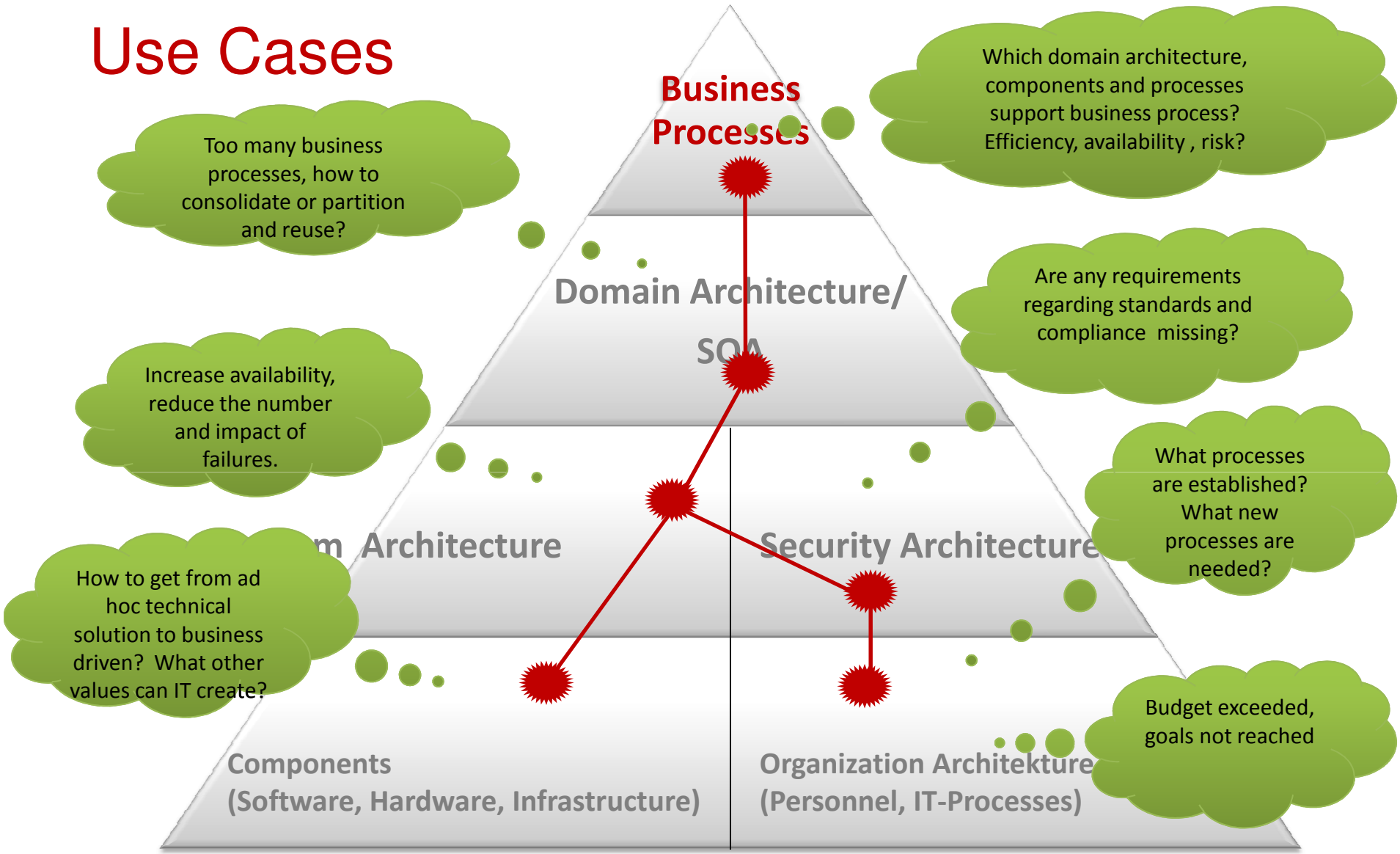
IT Architectures



Justification for IT (raison d'être)

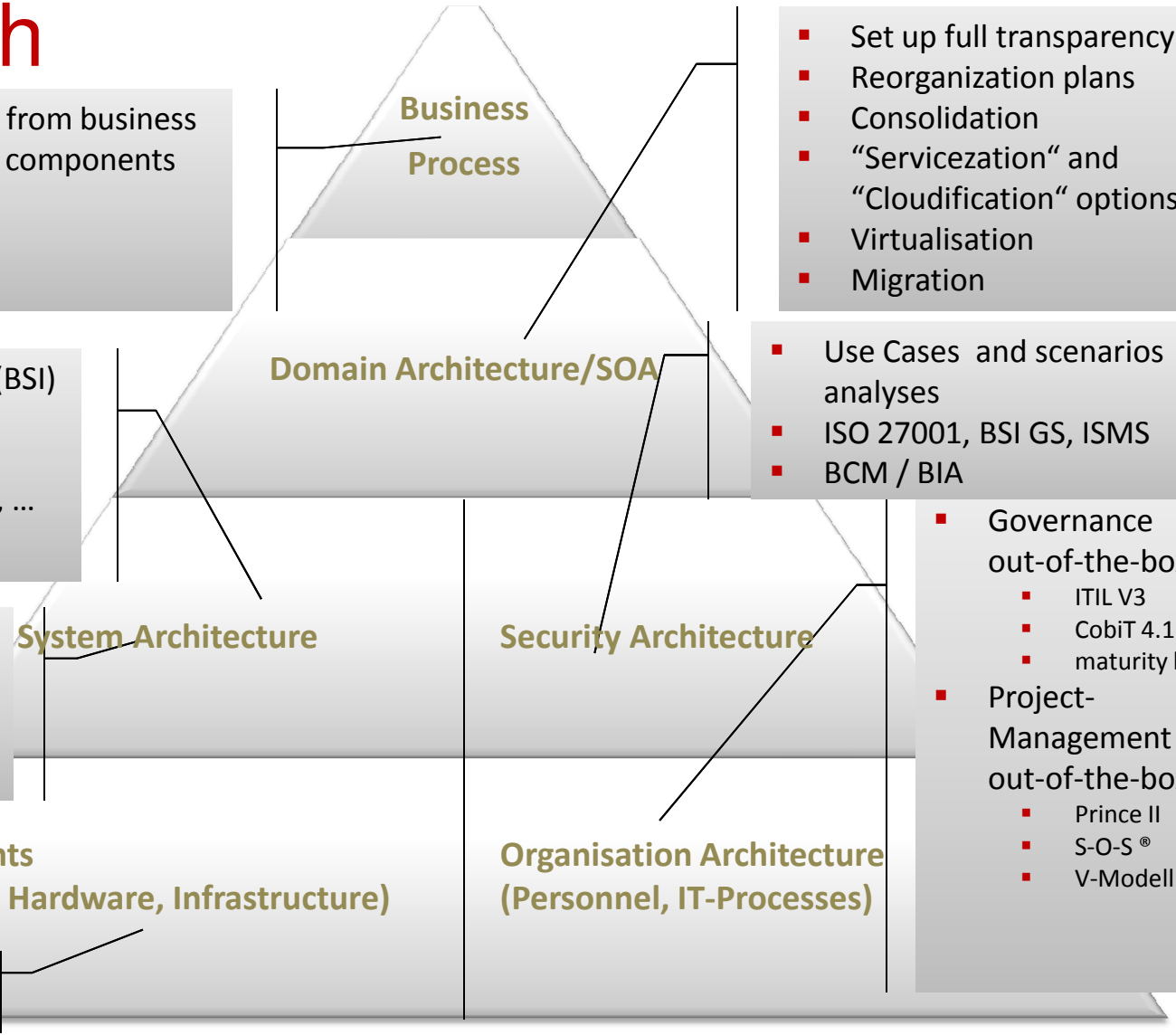


Use Cases


Business Processes
Domain Architecture/ SOA
m Architecture
Security Architecture
Components (Software, Hardware, Infrastructure)
Organization Architekture (Personnel, IT-Processes)
Too many business processes, how to consolidate or partition and reuse?
Which domain architecture, components and processes support business process? Efficiency, availability , risk?
Are any requirements regarding standards and compliance missing?
Increase availability, reduce the number and impact of failures.
What processes are established? What new processes are needed?
How to get from ad hoc technical solution to business driven? What other values can IT create?
Budget exceeded, goals not reached

Approach

- Specify dependencies from business process all the way to components analytically



- Set up full transparency
- Reorganization plans
- Consolidation
- "Servicezation" and "Cloudification" options
- Virtualisation
- Migration

- Use Cases and scenarios analyses
- ISO 27001, BSI GS, ISMS
- BCM / BIA

- Reference architectures (BSI)
- Plan and evaluate goal architecture
- Network, storage, server, …

- Benchmarks
- Audits
- HA Compendium
- Data centers database

- Reliability Database

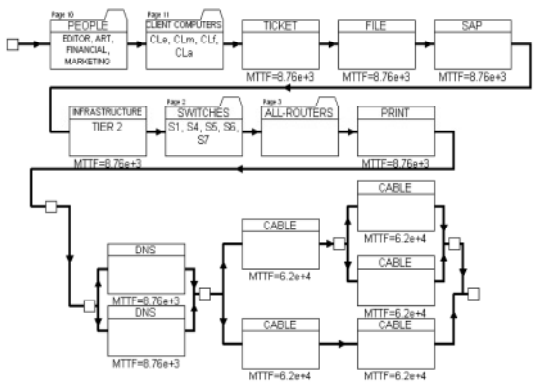
- Governance out-of-the-box
  - ITIL V3
  - CobiT 4.1
  - maturity levels
- Project-Management out-of-the-box
  - Prince II
  - S-O-S ®
  - V-Modell XT

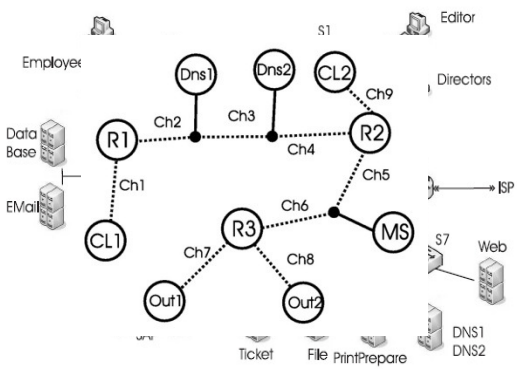
Computing A_{is} of a Service at a Glance

Service specification in
a high-level modeling language
(e.g., UML activity diagram, BPMN)

	Client 1	Client 2
MTTF	1060	1280
MTTR	1.79	1.83
A	0.99834	0.99858

u_1	u_2	A_s
0.5	0.5	0.99846
0.6	0.4	0.998436
0.9	0.1	0.99834
0.1	0.9	0.998556



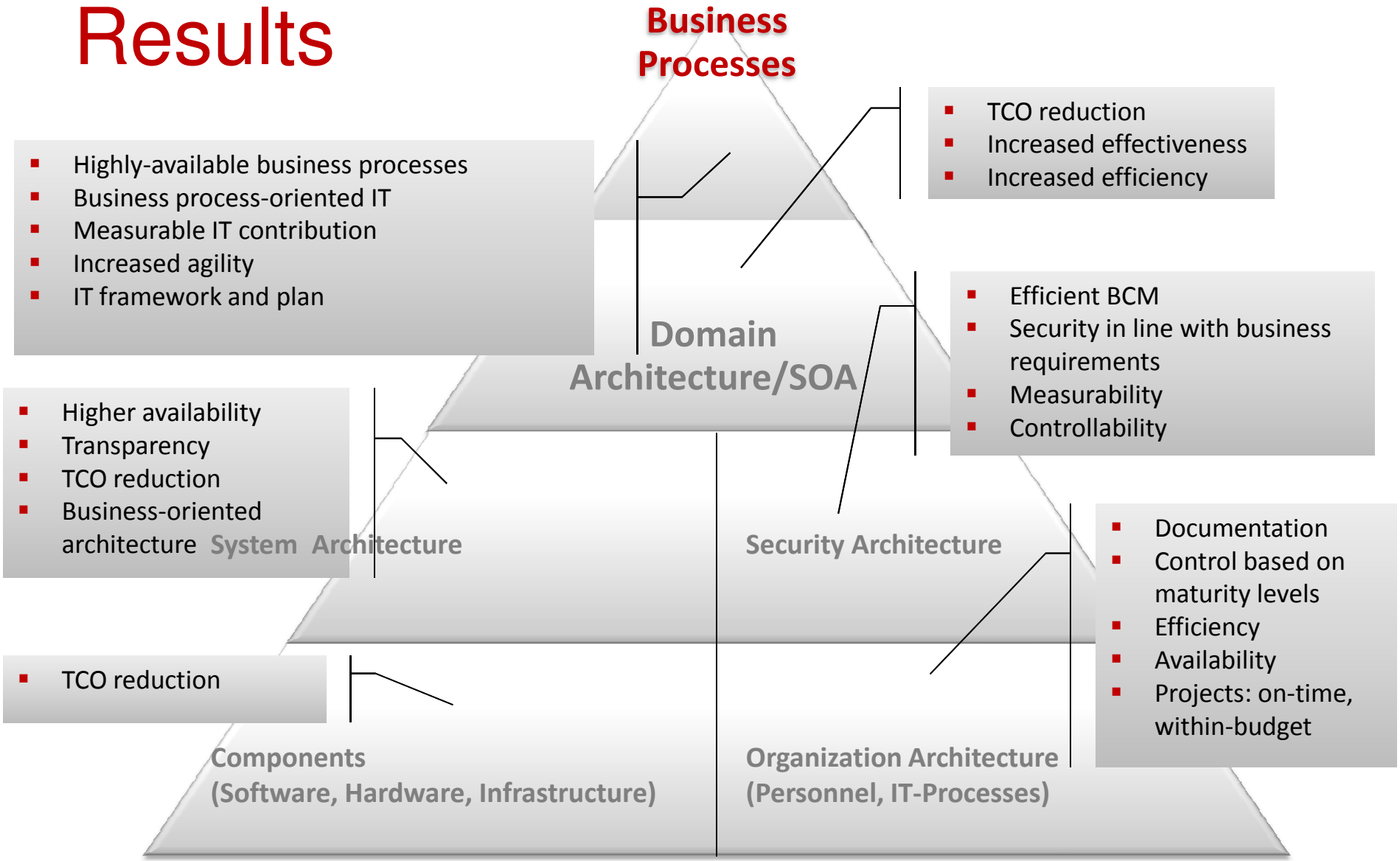


$$CL_1\text{: } (CL_1 \rightarrow DNS)\&(CL_1 \rightarrow MS)\&(MS \rightarrow DNS)\&(MS \rightarrow OUT) = CL_1\&MS\&R_1\&R_2\&R_3\&CH_1\&CH_2\&CH_3\&CH_4\&CH_5\&CH_6\&(DNS_1 \,||\, DNS_2)\&(CH_7\&OUT_1 \,||\, CH_8\&OUT_2)$$

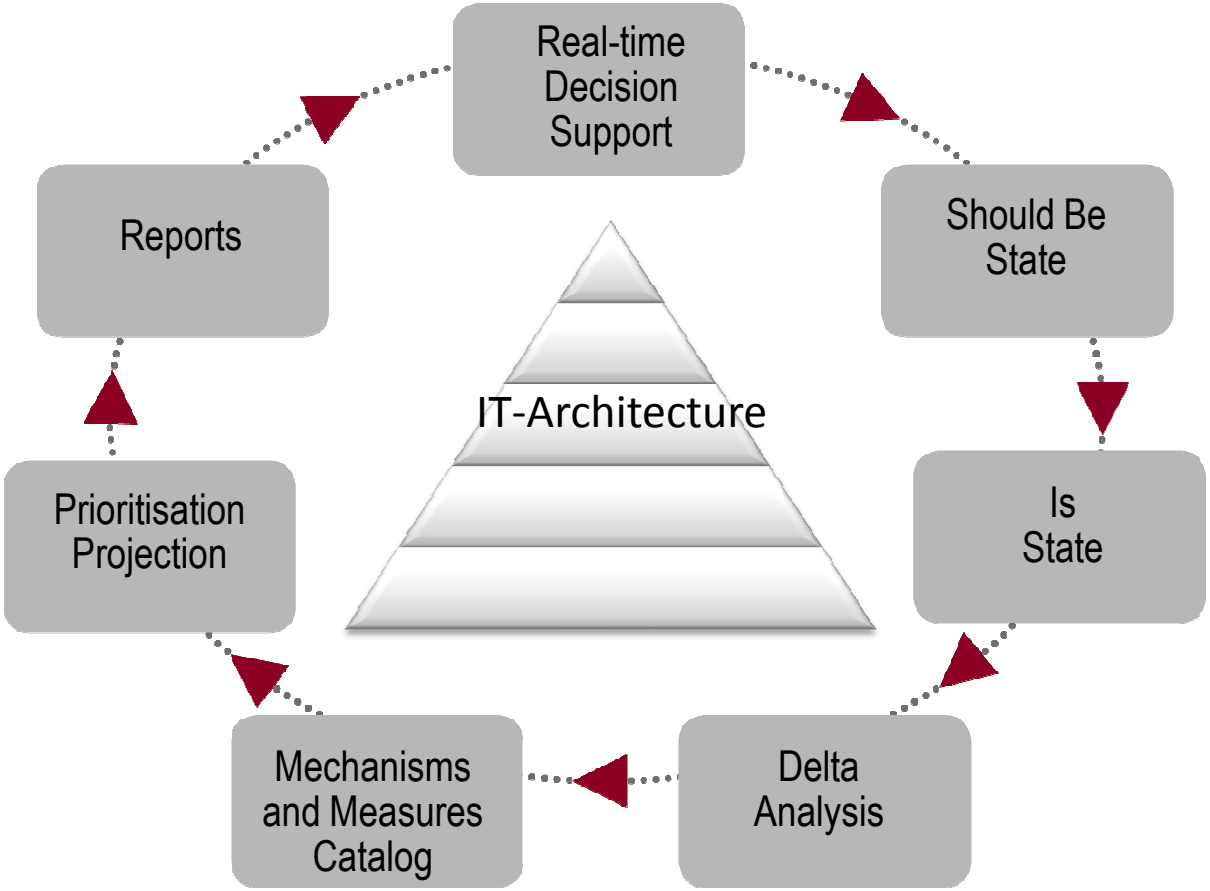
$$CL_2\text{: } (CL_2 \rightarrow DNS)\&(CL_2 \rightarrow MS)\&(MS \rightarrow DNS)\&(MS \rightarrow OUT) = CL_2\&MS\&R_2\&R_3\&CH_9\&CH_4\&CH_5\&CH_6\&(CH_3\&DNS_1 \,||\, DNS_2)\&(CH_7\&OUT_1 \,||\, CH_8\&OUT_2)$$

Malek . Milanovic and Milic, ISAS 2008

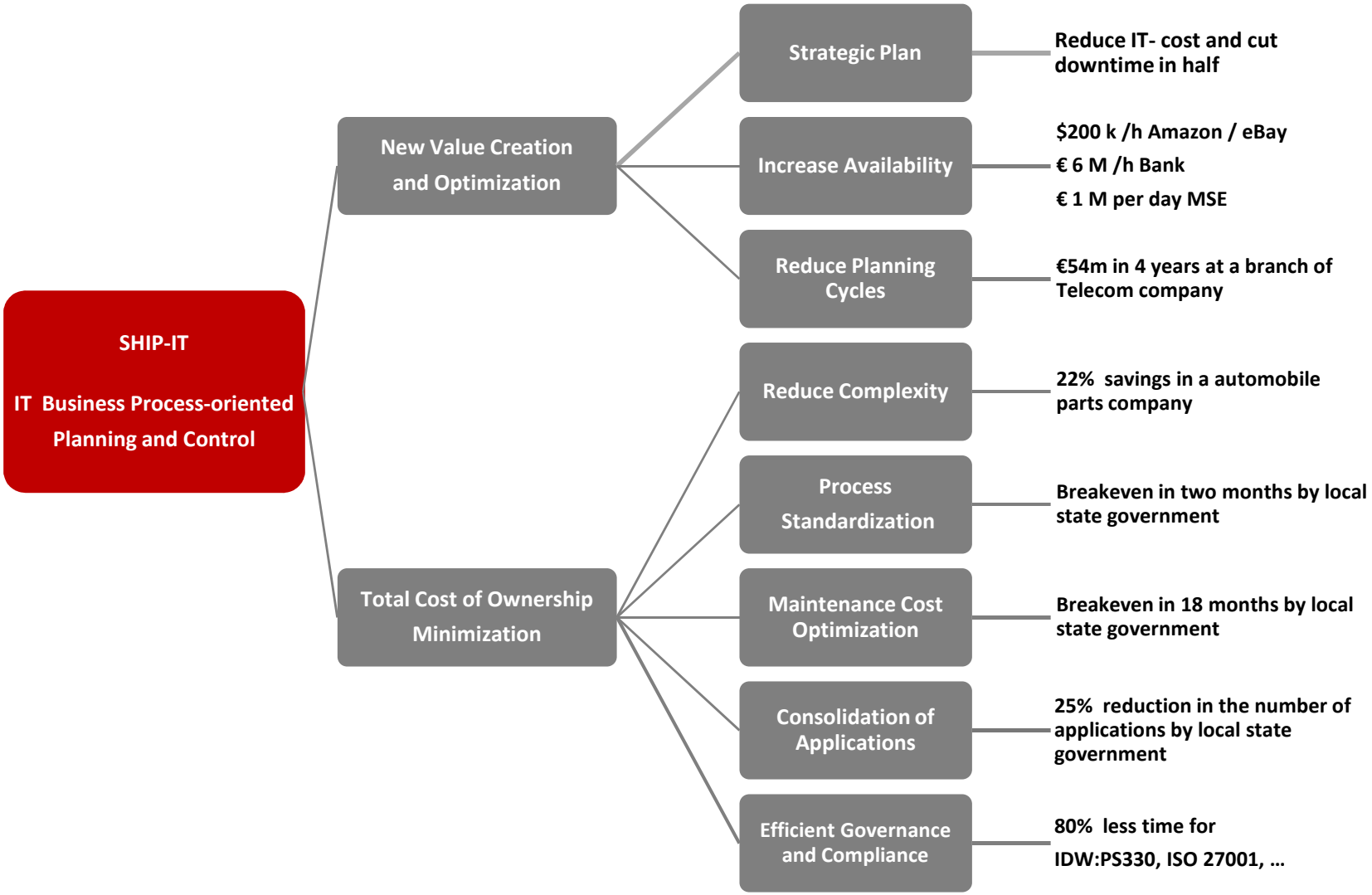
Results


Business Processes
Highly-available business processes
Business process-oriented IT
Measurable IT contribution
Increased agility
IT framework and plan
TCO reduction
Increased effectiveness
Increased efficiency
Domain Architecture/SOA
Efficient BCM
Security in line with business requirements
Measurability
Controllability
Higher availability
Transparency
TCO reduction
Business-oriented architecture
System Architecture
Security Architecture
Documentation
Control based on maturity levels
Efficiency
Availability
Projects: on-time, within-budget
TCO reduction
Components (Software, Hardware, Infrastructure)
Organization Architecture (Personnel, IT-Processes)

SHIP-IT is a Framework and a Tool for Comprehensive IT Planning und Control



Return on Knowledge and Investment



The AMP Principle

- Analyze the Past
- Monitor the Present
- Predict the Future

to increase

Open Systems Dependability