Visualization of Risk

Models, Methods and Tools

Alexander M. Ernst
Software Engineering for Business Information Systems (sebis)
Ernst Denert-Stiftungslehrstuhl
Technische Universität München, Faculty for Informatics

wwwmatthes.in.tum.de

What is does *risk* mean in this presentation?

Requirements for Risk Assessment Methodologies

(Technical Guide, The Open Group 2009)

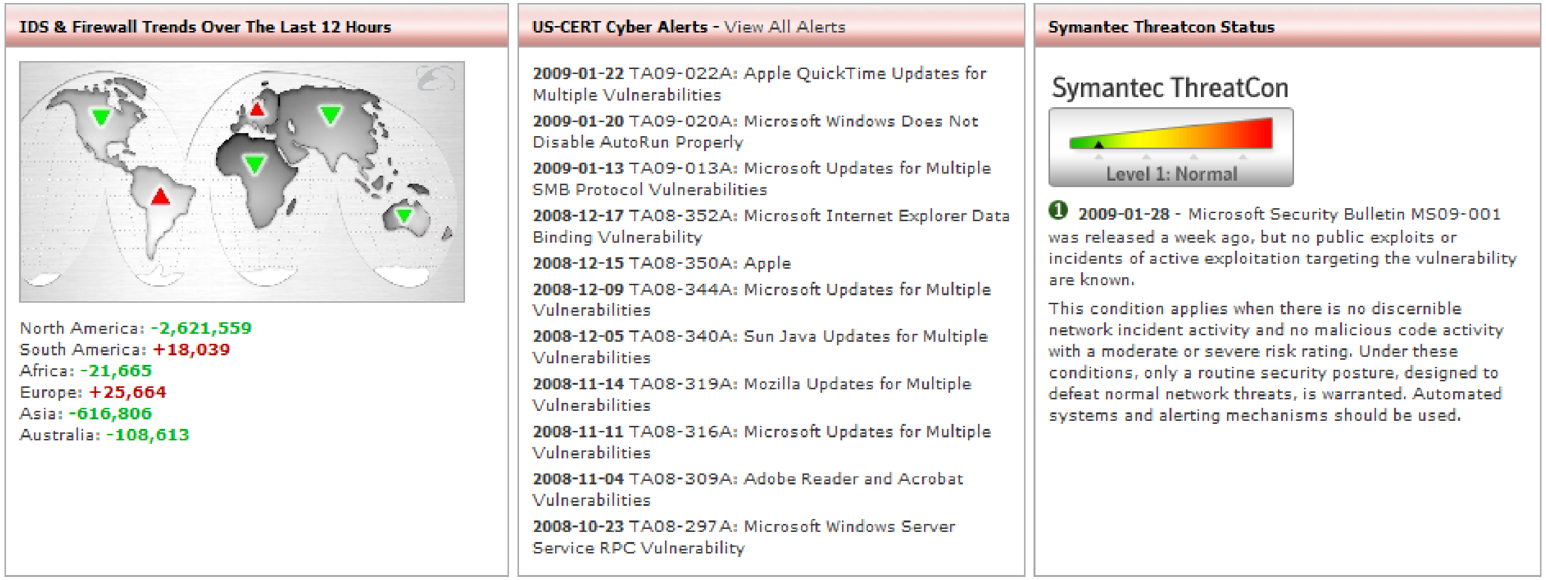
- The probable frequency and probable magnitude of future loss.

Risk Taxonomy

(Technical Standard, The Open Group 2009)

- How often bad things happen, and how bad they are when they occur.

Visualization of risk –
What you are currently using



IDS & Firewall Trends Over The Last 12 Hours

North America:	-2,621,559
South America:	+18,039
Africa:	-21,665
Europe:	+25,664
Asia:	-616,806
Australia:	-108,613

US-CERT Cyber Alerts - View All Alerts

2009-01-22 TA09-022A: Apple QuickTime Updates for Multiple Vulnerabilities

2009-01-20 TA09-020A: Microsoft Windows Does Not Disable AutoRun Properly

2009-01-13 TA09-013A: Microsoft Updates for Multiple SMB Protocol Vulnerabilities

2008-12-17 TA08-352A: Microsoft Internet Explorer Data Binding Vulnerability

2008-12-15 TA08-350A: Apple

2008-12-09 TA08-344A: Microsoft Updates for Multiple Vulnerabilities

2008-12-05 TA08-340A: Sun Java Updates for Multiple Vulnerabilities

2008-11-14 TA08-319A: Mozilla Updates for Multiple Vulnerabilities

2008-11-11 TA08-316A: Microsoft Updates for Multiple Vulnerabilities

2008-11-04 TA08-309A: Adobe Reader and Acrobat Vulnerabilities

2008-10-23 TA08-297A: Microsoft Windows Server Service RPC Vulnerability

Symantec Threatcon Status

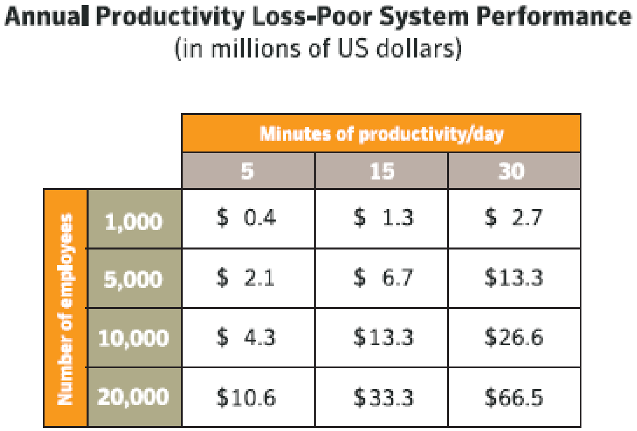
Symantec ThreatCon

Level 1: Normal

❶ **2009-01-28** - Microsoft Security Bulletin MS09-001 was released a week ago, but no public exploits or incidents of active exploitation targeting the vulnerability are known.

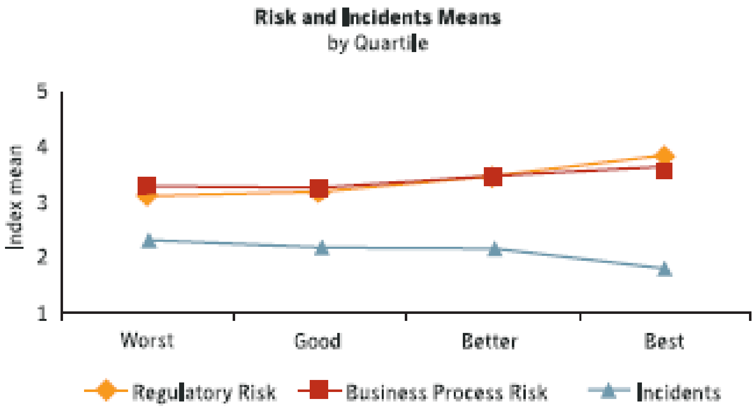
This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under these conditions, only a routine security posture, designed to defeat normal network threats, is warranted. Automated systems and alerting mechanisms should be used.

Emagined Security Dashboard: http://www.emagined.com/security_dashboard.php (2009-01-29)



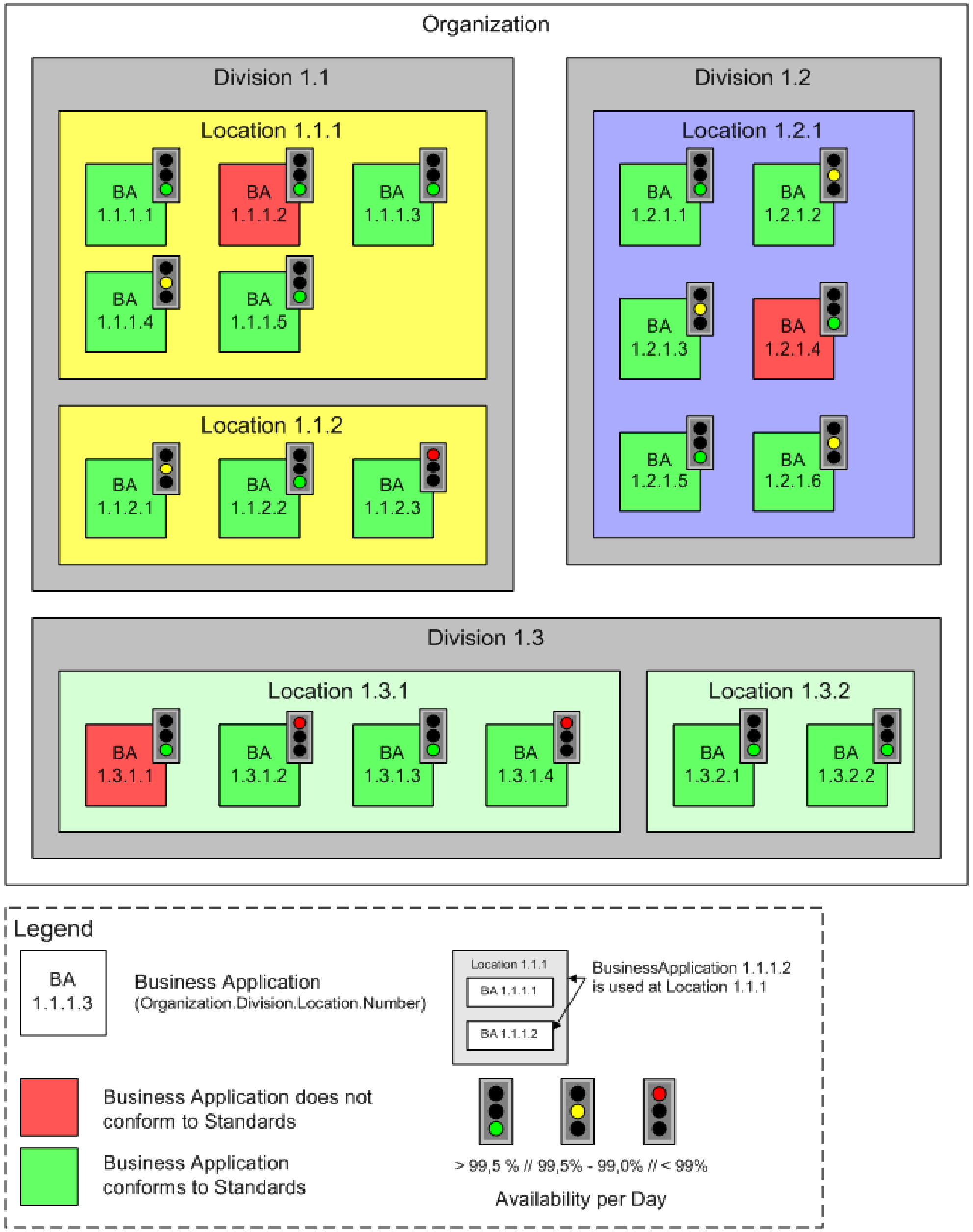
Annual Productivity Loss-Poor System Performance
(in millions of US dollars)

		Minutes of productivity/day		
		5	15	30
Number of employees	1,000	$ 0.4	$ 1.3	$ 2.7
	5,000	$ 2.1	$ 6.7	$13.3
	10,000	$ 4.3	$13.3	$26.6
	20,000	$10.6	$33.3	$66.5



Symantec IT Risk Management Report 2: Myths and Realities
http://eval.symantec.com/mktginfo/enterprise/other_resources/b-it_risk_management_report_2_01-2008_12818026.en-us.pdf

Visualization of risk –
What you could be using



Organization

Division 1.1

Location 1.1.1

BA 1.1.1.1 · BA 1.1.1.2 · BA 1.1.1.3 · BA 1.1.1.4 · BA 1.1.1.5

Location 1.1.2

BA 1.1.2.1 · BA 1.1.2.2 · BA 1.1.2.3

Division 1.2

Location 1.2.1

BA 1.2.1.1 · BA 1.2.1.2 · BA 1.2.1.3 · BA 1.2.1.4 · BA 1.2.1.5 · BA 1.2.1.6

Division 1.3

Location 1.3.1

BA 1.3.1.1 · BA 1.3.1.2 · BA 1.3.1.3 · BA 1.3.1.4

Location 1.3.2

BA 1.3.2.1 · BA 1.3.2.2

Legend

BA 1.1.1.3 — Business Application (Organization.Division.Location.Number)

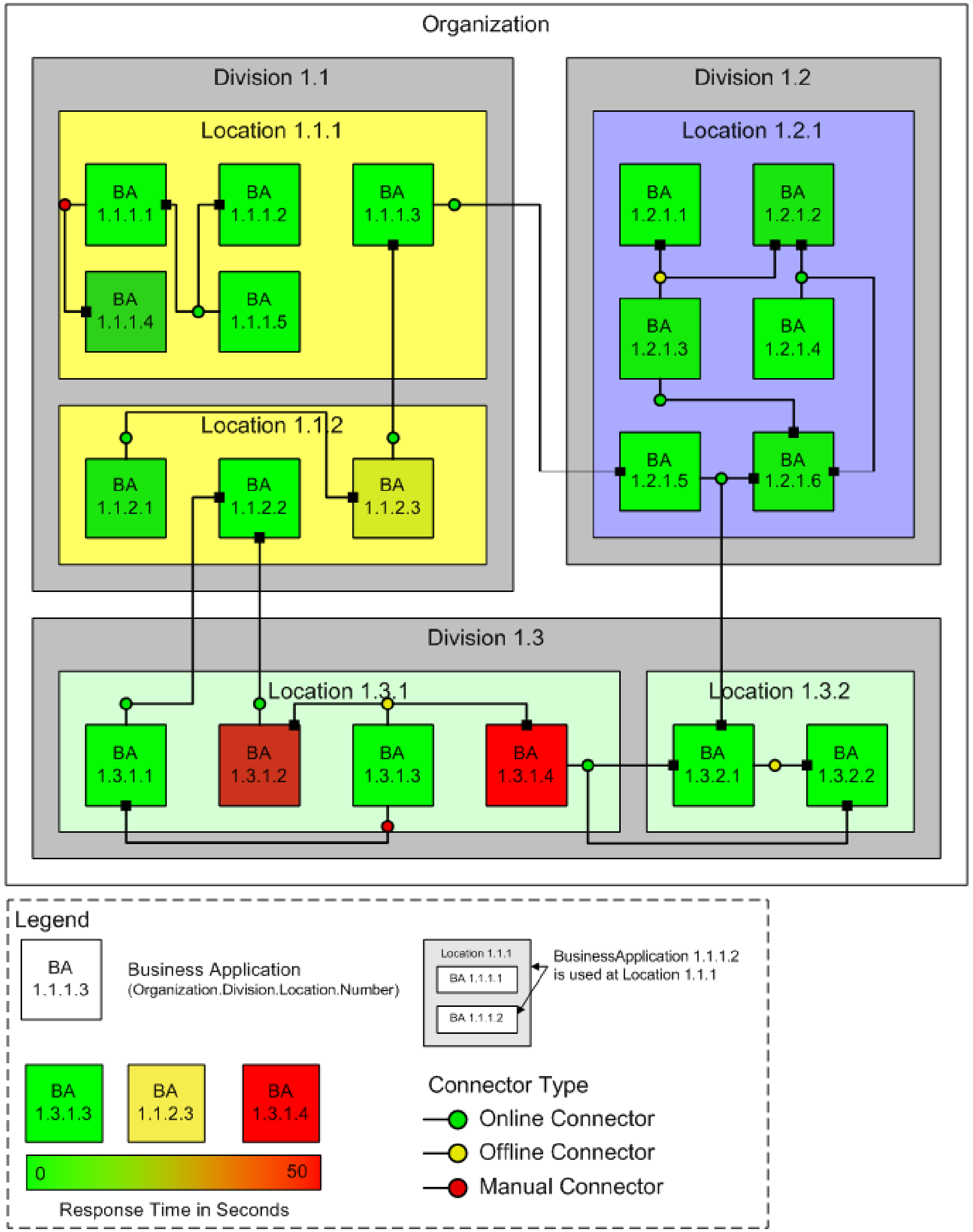
Location 1.1.1 / BA 1.1.1.1 / BA 1.1.1.2 — BusinessApplication 1.1.1.2 is used at Location 1.1.1

🟥 Business Application does not conform to Standards

🟩 Business Application conforms to Standards

> 99,5 % // 99,5% - 99,0% // < 99%

Availability per Day



Organization

Division 1.1

Location 1.1.1

BA 1.1.1.1 · BA 1.1.1.2 · BA 1.1.1.3 · BA 1.1.1.4 · BA 1.1.1.5

Location 1.1.2

BA 1.1.2.1 · BA 1.1.2.2 · BA 1.1.2.3

Division 1.2

Location 1.2.1

BA 1.2.1.1 · BA 1.2.1.2 · BA 1.2.1.3 · BA 1.2.1.4 · BA 1.2.1.5 · BA 1.2.1.6

Division 1.3

Location 1.3.1

BA 1.3.1.1 · BA 1.3.1.2 · BA 1.3.1.3 · BA 1.3.1.4

Location 1.3.2

BA 1.3.2.1 · BA 1.3.2.2

Legend

BA 1.1.1.3 — Business Application (Organization.Division.Location.Number)

Location 1.1.1 / BA 1.1.1.1 / BA 1.1.1.2 — BusinessApplication 1.1.1.2 is used at Location 1.1.1

BA 1.3.1.3 · BA 1.1.2.3 · BA 1.3.1.4

0 — 50

Response Time in Seconds

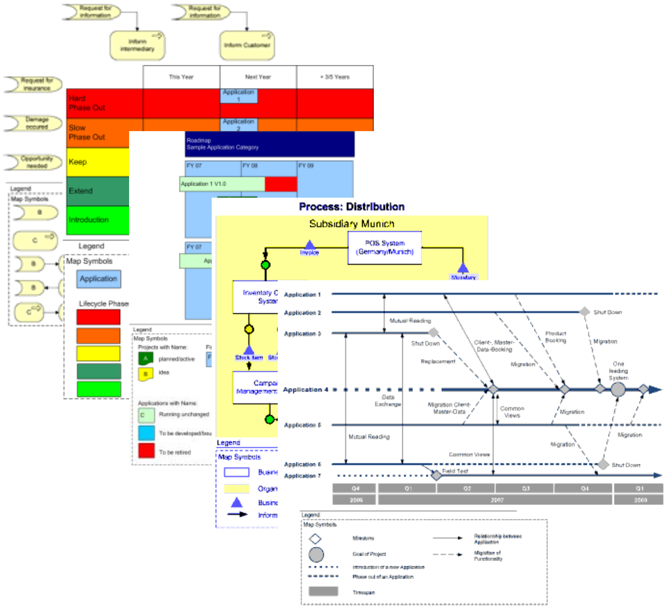
Connector Type

- Online Connector
- Offline Connector
- Manual Connector

Lack of standardized viewpoints for managing the enterprise

Software Engineering: Established viewpoints for recurring and known problems

- modularity, deployment, interaction, …

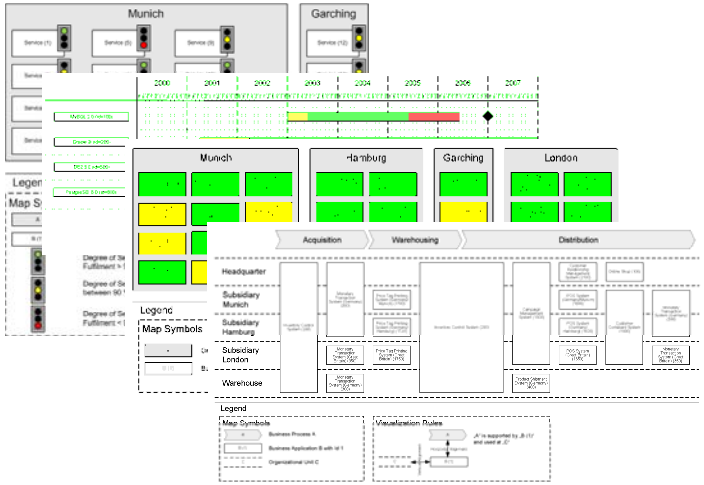


Enterprise Architectures: Emerging modeling languages and viewpoints, e.g.

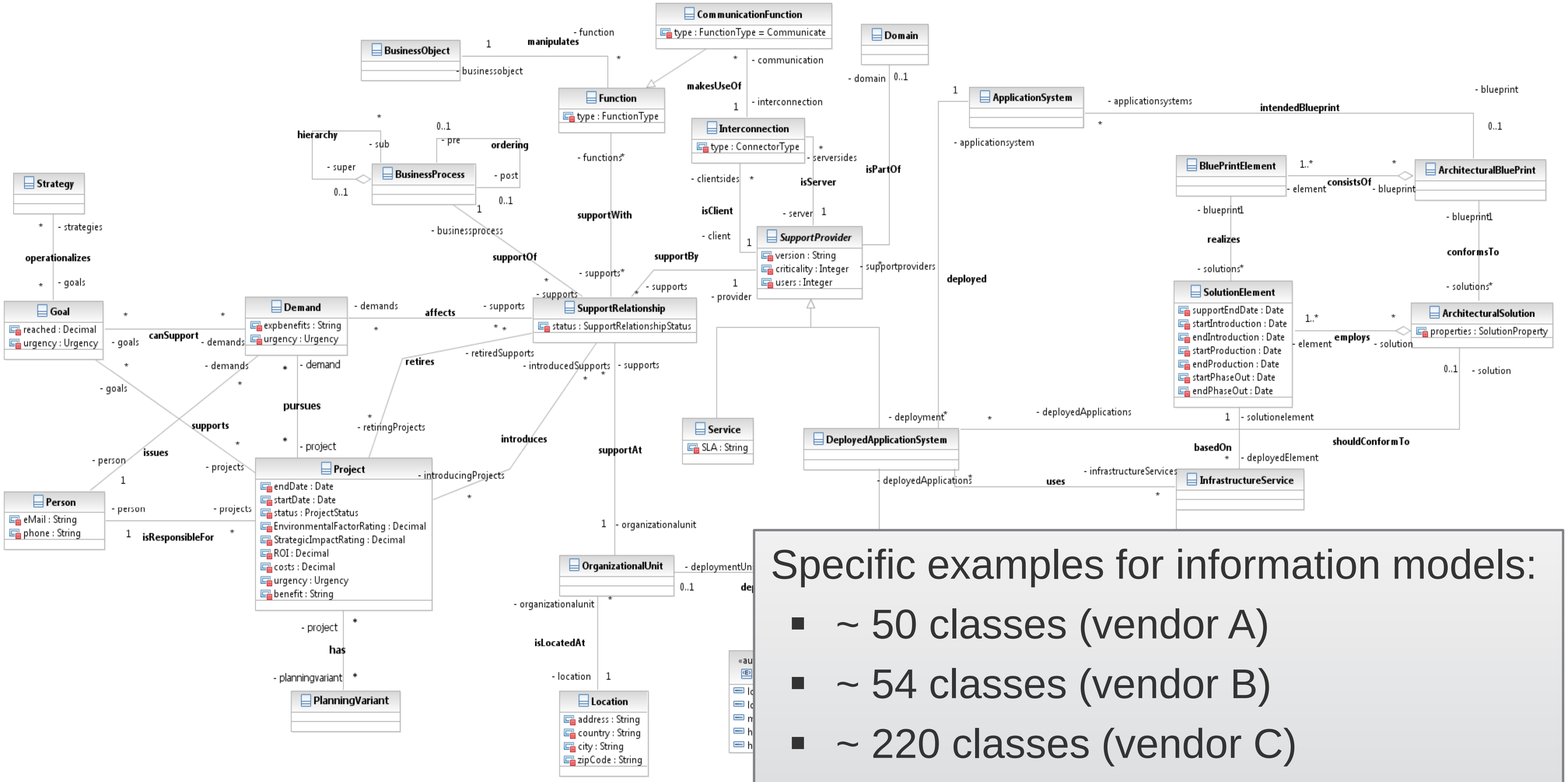
- ArchiMate (http://www.archimate.com)
- System Cartography (http://www.systemcartography.info)

Many organization-specific viewpoints:

- rarely documented
- visibility limited to a single organization



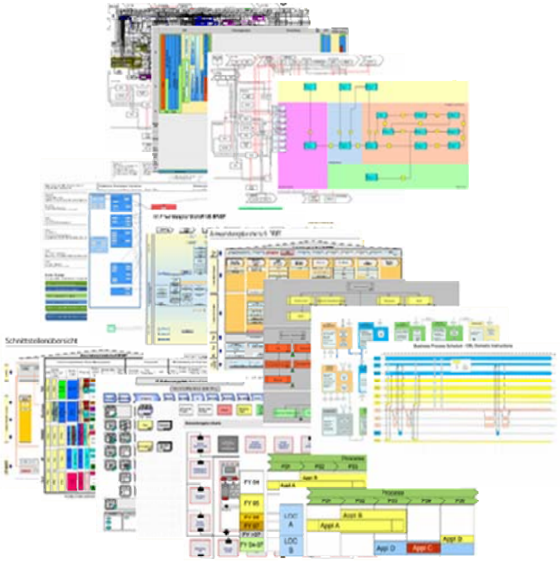
What information is needed to manage the enterprise?



Specific examples for information models:

- ~ 50 classes (vendor A)
- ~ 54 classes (vendor B)
- ~ 220 classes (vendor C)
- ~ 470 classes (vendor D)
- At least twice as many associations
- Numerous attributes per instance

System Cartography – Where we came from, what we achieved and what we will do

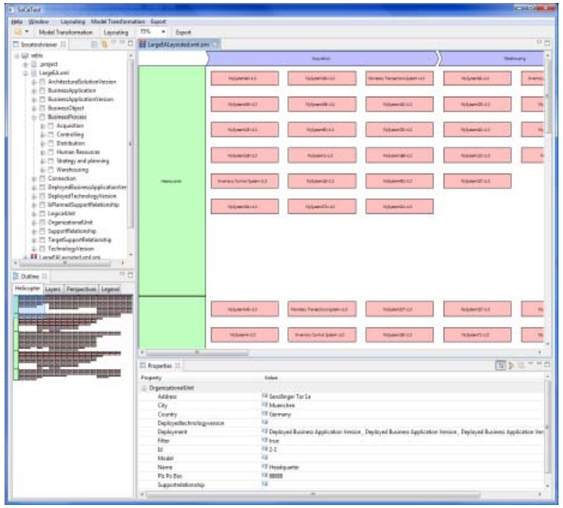


Where we came from

- Software Cartography develops models and methods for describing, evaluating, and constructing application landscapes.

What we achieved

- Development of the SyCaTool
- Enterprise Architecture Management Tool Survey
- Development of the EAM Pattern Catalog



What we will do

- Establish a community for EAM Patterns
- Simulation of enterprise architectures
- Extension of the project scope from Enterprise Architectures to *Systems of Systems*

➔System Cartography

Application of System Cartography to visualize risk

Agenda

- Motivation and Introduction
- Enterprise Architecture Management Patterns
- System Cartography Tool (SyCaTool)
- Visualizing Risks
- Conclusion and Outlook

EAM patterns document proven practice solutions for recurring problems in managing the EA

An enterprise architecture management pattern (**EAM pattern**) is

- a general, reusable solution to a common problem
- in a given context
- identifies driving forces,
- known usages, and
- consequences.

An EAM pattern takes a holistic perspective:

- It addresses concerns at the enterprise (systems of systems) level.
- It considers social, technical, and economic forces in a balanced manner.

- It is discovered in working solutions rather than being invented or hoped for.
- It uses a clear, accessible, and informal language that allows practitioners to describe their knowledge and experience.

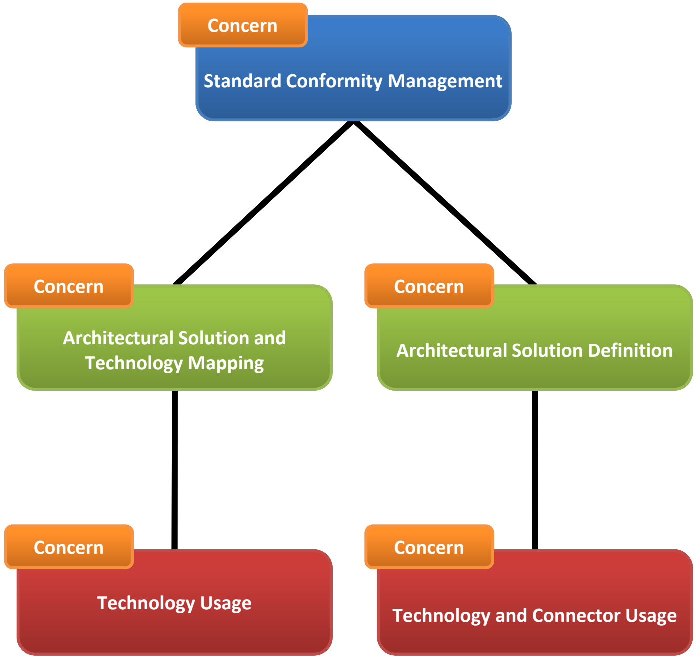
Pattern languages are a proven way to capture best practices and expert knowledge and to socialize it inside a group, department, entire company, or entire design discipline.

The EAM pattern catalog is made up of concerns, M-Patterns, V-Patterns and I-Patterns

Tailor the EAM to the specific situation (*pains*) of the enterprise and follow an incremental strategy based on **EAM patterns** representing proven practices.

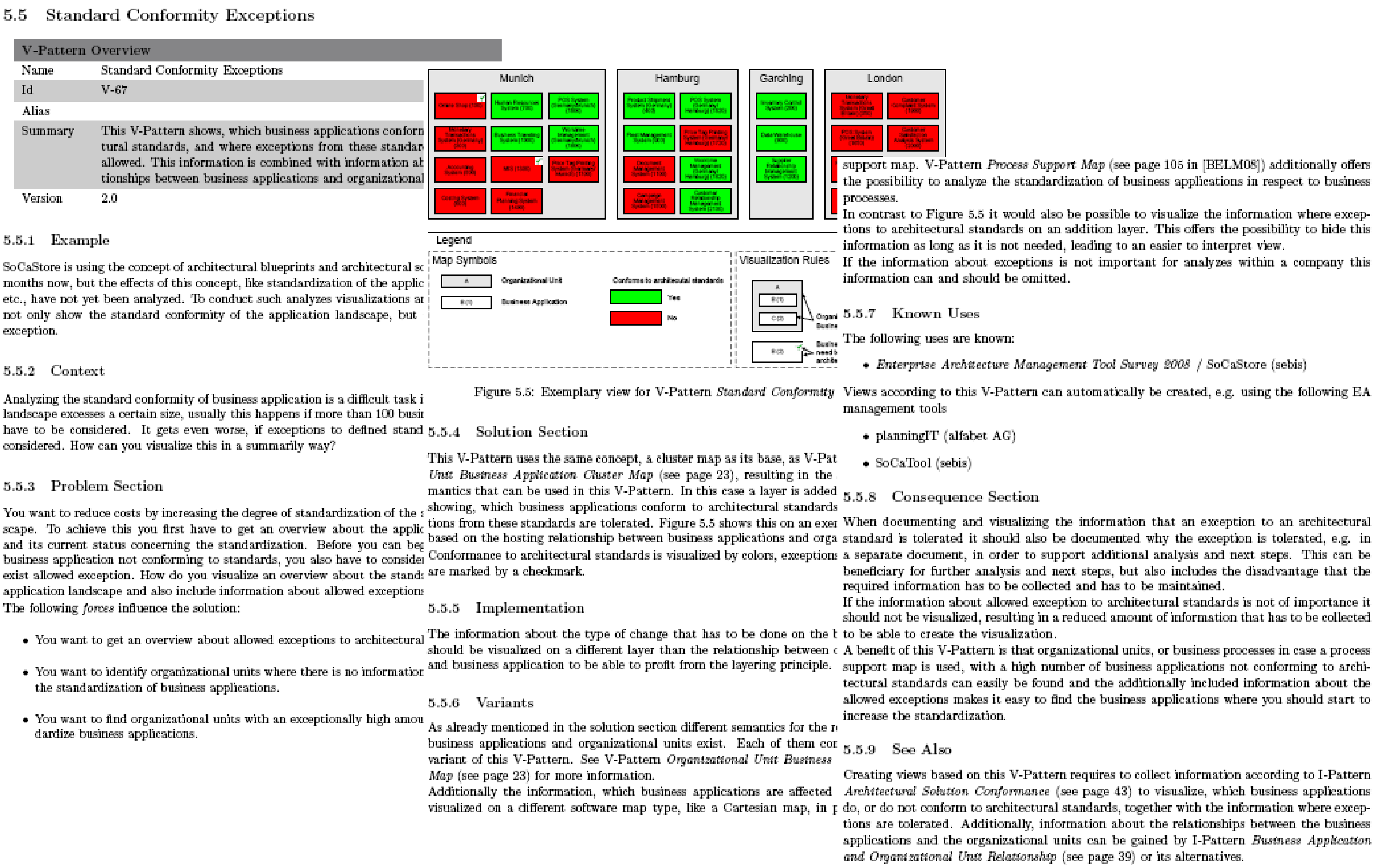
Systematically document the dependencies between

- individual management concerns,
  Which concern is relevant for which stakeholder?
- methodology patterns (M-Pattern),
  Which activities are required to address a concern?
- viewpoint patterns (V-Pattern), and
  Which viewpoints help stakeholders to collaboratively perform the activities?
- information model patterns (I-Pattern)
  Which information has to be available to generate a view?


Concern
Standard Conformity Management
Concern
Architectural Solution and Technology Mapping
Concern
Architectural Solution Definition
Concern
Technology Usage
Concern
Technology and Connector Usage

Draw attention to the consequences implied by a pattern (labor, required information, *political* resistance, …)

Exemplary EAM Pattern for Standard Conformity Management – Standard Conformity Exception



5.5 Standard Conformity Exceptions

V-Pattern Overview	
Name	Standard Conformity Exceptions
Id	V-67
Alias	
Summary	This V-Pattern shows, which business applications conforn tural standards, and where exceptions from these standar allowed. This information is combined with information ab tionships between business applications and organizational
Version	2.0

5.5.1 Example

SoCaStore is using the concept of architectural blueprints and architectural sc months now, but the effects of this concept, like standardization of the applic etc., have not yet been analyzed. To conduct such analyzes visualizations ar not only show the standard conformity of the application landscape, but exception.

5.5.2 Context

Analyzing the standard conformity of business application is a difficult task i landscape excesses a certain size, usually this happens if more than 100 busi have to be considered. It gets even worse, if exceptions to defined stand considered. How can you visualize this in a summarily way?

5.5.3 Problem Section

You want to reduce costs by increasing the degree of standardization of the a scape. To achieve this you first have to get an overview about the applic and its current status concerning the standardization. Before you can beg business application not conforming to standards, you also have to conside exist allowed exception. How do you visualize an overview about the stand application landscape and also include information about allowed exceptions The following *forces* influence the solution:

- You want to get an overview about allowed exceptions to architectural
- You want to identify organizational units where there is no informatio the standardization of business applications.
- You want to find organizational units with an exceptionally high amou dardize business applications.

Munich
Online Shop
Human Resources System
POS System (Germany/Munich)
Monetary Transactions System (Germany)
Business Traveling System
Warehouse Management (Germany/Munich)
Accounting System
MIS
Price Tag Printing System (Germany/Munich)
Costing System
Financial Planning System
Hamburg
Product Shipment System (Germany)
POS System (Germany/ Hamburg)
Fleet Management System
Price Tag Printing System (Germany/ Hamburg)
Document Management System
Warehouse Management (Germany/ Hamburg)
Campaign Management System
Customer Relationship Management System
Garching
Inventory Control System
Data Warehouse
Supplier Relationship Management System
London
Monetary Transactions System (Great Britain)
Customer Complaint System
POS System (Great Britain)
Customer Satisfaction Analysis System
Legend
Map Symbols
A
Organizational Unit
B(1)
Business Application
Conforms to architectural standards
Yes
No
Visualization Rules
A
B(1)
C(2)
Organi
Busine
B(3)
Busine
need t
archite

Figure 5.5: Exemplary view for V-Pattern *Standard Conformity*

5.5.4 Solution Section

This V-Pattern uses the same concept, a cluster map as its base, as V-Pat *Unit Business Application Cluster Map* (see page 23), resulting in the mantics that can be used in this V-Pattern. In this case a layer is added showing, which business applications conform to architectural standards tions from these standards are tolerated. Figure 5.5 shows this on an exa based on the hosting relationship between business applications and orga Conformance to architectural standards is visualized by colors, exceptions are marked by a checkmark.

5.5.5 Implementation

The information about the type of change that has to be done on the b should be visualized on a different layer than the relationship between c and business application to be able to profit from the layering principle.

5.5.6 Variants

As already mentioned in the solution section different semantics for the r business applications and organizational units exist. Each of them co variant of this V-Pattern. See V-Pattern *Organizational Unit Business Map* (see page 23) for more information.

Additionally the information, which business applications are affected visualized on a different software map type, like a Cartesian map, in p support map. V-Pattern *Process Support Map* (see page 105 in [BELM08]) additionally offers the possibility to analyze the standardization of business applications in respect to business processes.

In contrast to Figure 5.5 it would also be possible to visualize the information where exceptions to architectural standards on an addition layer. This offers the possibility to hide this information as long as it is not needed, leading to an easier to interpret view.

If the information about exceptions is not important for analyzes within a company this information can and should be omitted.

5.5.7 Known Uses

The following uses are known:

- *Enterprise Architecture Management Tool Survey 2008* / SoCaStore (sebis)

Views according to this V-Pattern can automatically be created, e.g. using the following EA management tools

- planningIT (alfabet AG)
- SoCaTool (sebis)

5.5.8 Consequence Section

When documenting and visualizing the information that an exception to an architectural standard is tolerated it should also be documented why the exception is tolerated, e.g. in a separate document, in order to support additional analysis and next steps. This can be beneficiary for further analysis and next steps, but also includes the disadvantage that the required information has to be collected and has to be maintained.

If the information about allowed exception to architectural standards is not of importance it should not be visualized, resulting in a reduced amount of information that has to be collected to be able to create the visualization.

A benefit of this V-Pattern is that organizational units, or business processes in case a process support map is used, with a high number of business applications not conforming to architectural standards can easily be found and the additionally included information about the allowed exceptions makes it easy to find the business applications where you should start to increase the standardization.

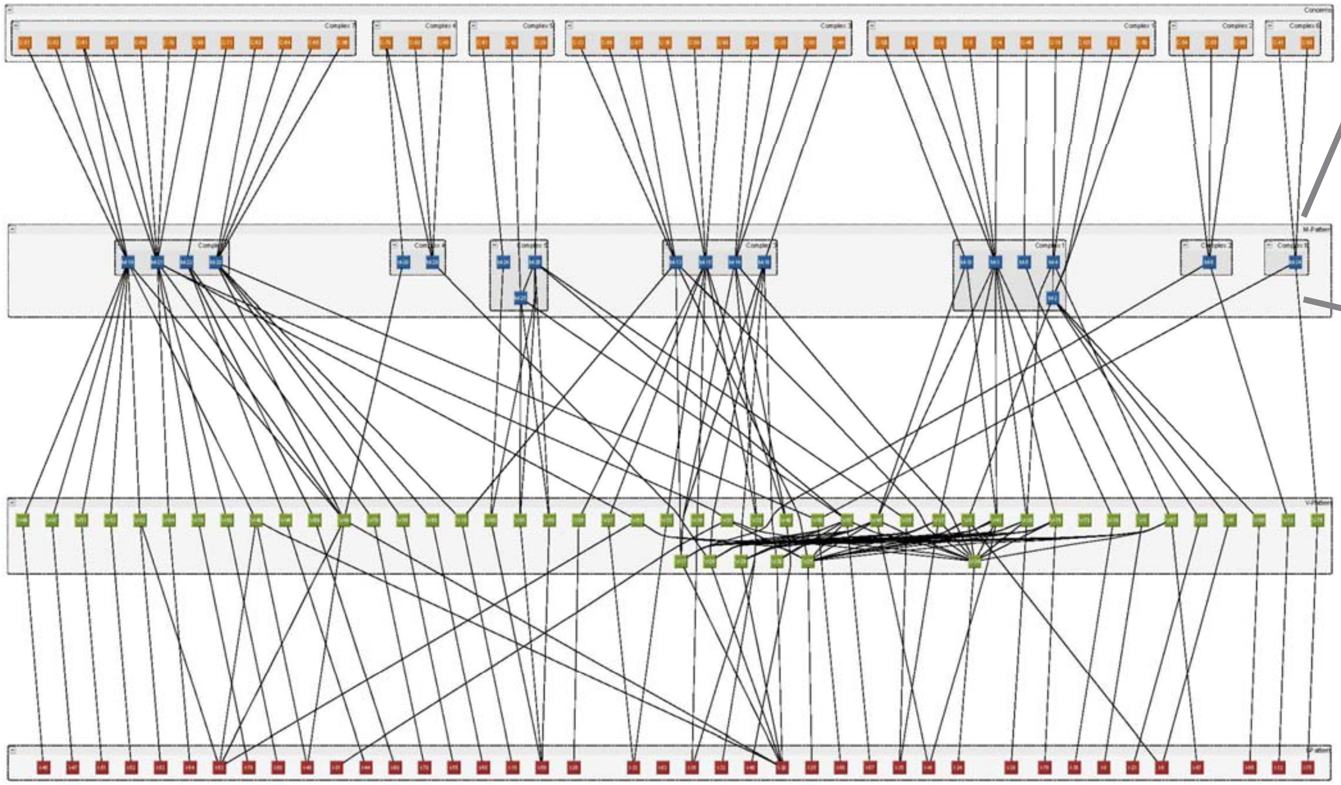
5.5.9 See Also

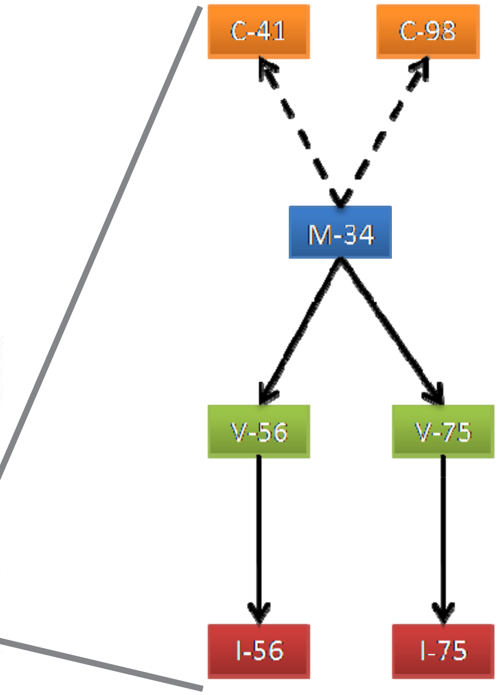
Creating views based on this V-Pattern requires to collect information according to I-Pattern *Architectural Solution Conformance* (see page 43) to visualize, which business applications do, or do not conform to architectural standards, together with the information where exceptions are tolerated. Additionally, information about the relationships between the business applications and the organizational units can be gained by I-Pattern *Business Application and Organizational Unit Relationship* (see page 39) or its alternatives.

Overview about EAM patterns and how they are linked

- Origin: Literature, experience from *sebis* research projects, structured interviews of 25 enterprise architects
- Selection based on relevance and adoption by an extensive online questionnaire

➔ 43 concerns, 20 M-Patterns, 53 V-Patterns, and 47 I-Patterns





http://www.systemcartography.info/eampc-wiki

Agenda

- Motivation and Introduction
- Enterprise Architecture Management Patterns
- System Cartography Tool (SyCaTool)
- Visualizing Risks
- Conclusion and Outlook

Motivation for generating views for risk management

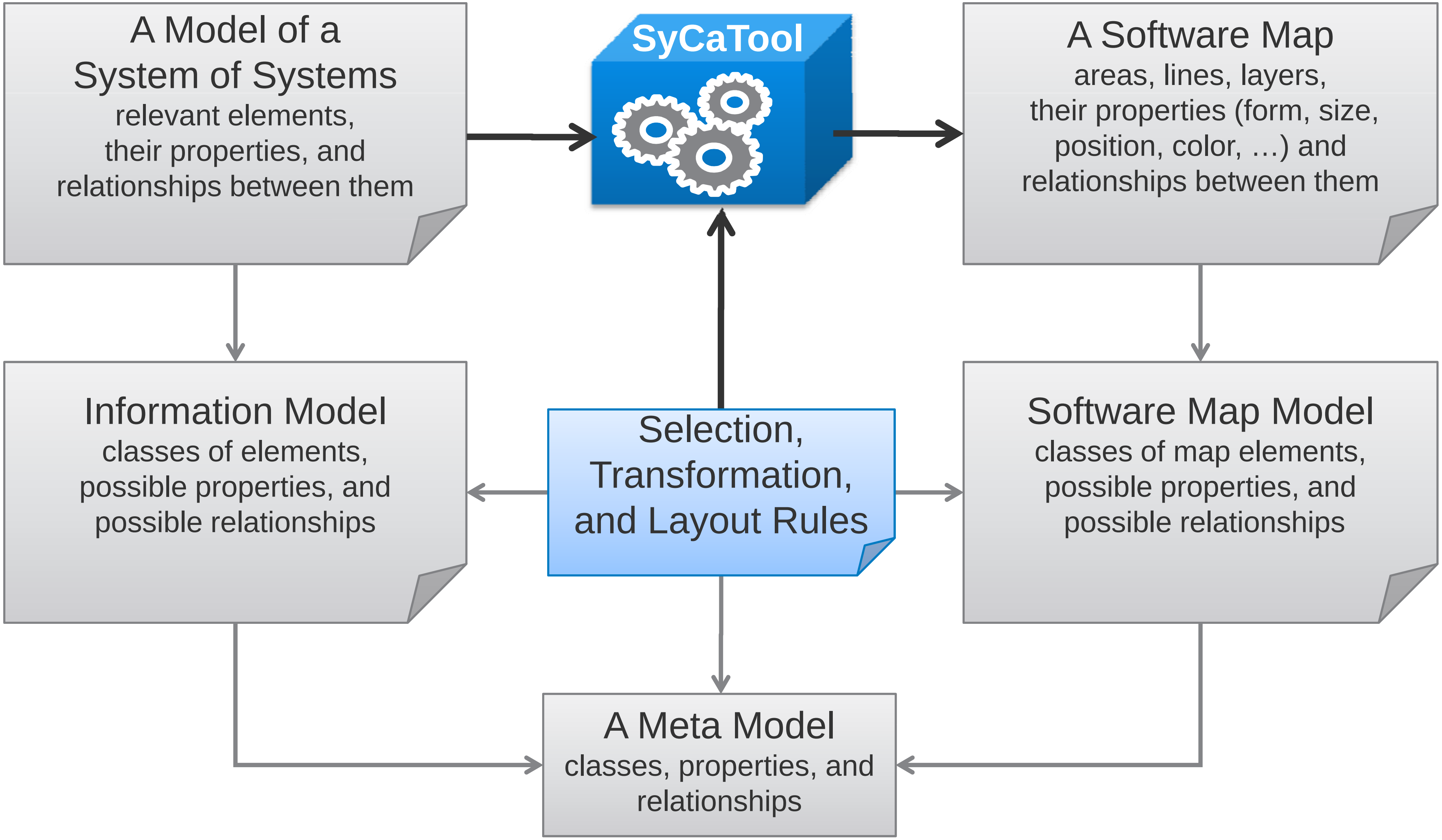
Reasons for generating views for risk management

- Different stakeholder have different concerns
- Causes of risk change fast (real-time)
  - ➔Obsolete before published
  - ➔Information is not available timely
- Inconsistent visualizations based on inconsistent data
- Manual creation of views
  - is error prone and
  - requires high effort

➔View generation for risk management

- must be stakeholder oriented
- address concerns relevant to these stakeholders
- needs to support multiple views of abstraction
- needs to reuse existing information in repositories
  - try to find inconsistencies between different sources
- has to be timely

SyCaTool creates visualizations based on customizable layout rules



A Model of a System of Systems
relevant elements,
their properties, and
relationships between them

SyCaTool

A Software Map
areas, lines, layers,
their properties (form, size, position, color, …) and
relationships between them

Information Model
classes of elements,
possible properties, and
possible relationships

Selection, Transformation, and Layout Rules

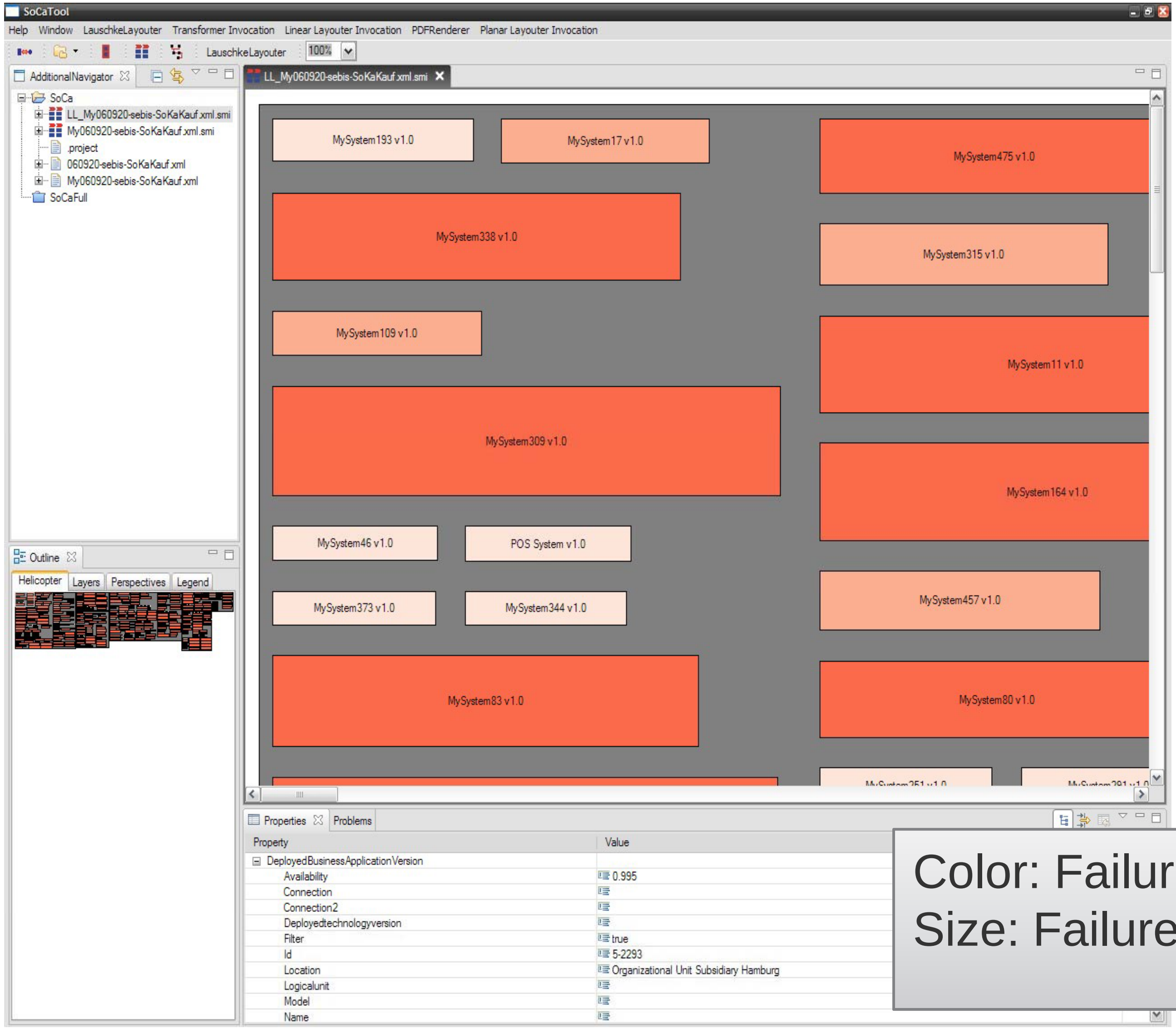
Software Map Model
classes of map elements,
possible properties, and
possible relationships

A Meta Model
classes, properties, and
relationships

A → B A based on B

A → B Data flow from A to B

Screenshot SyCaTool rich client:
Cluster map with two metrics



Property	Value
⊟ DeployedBusinessApplicationVersion	
Availability	0.995
Connection	
Connection2	
Deployedtechnologyversion	
Filter	true
Id	5-2293
Location	Organizational Unit Subsidiary Hamburg
Logicalunit	
Model	
Name	

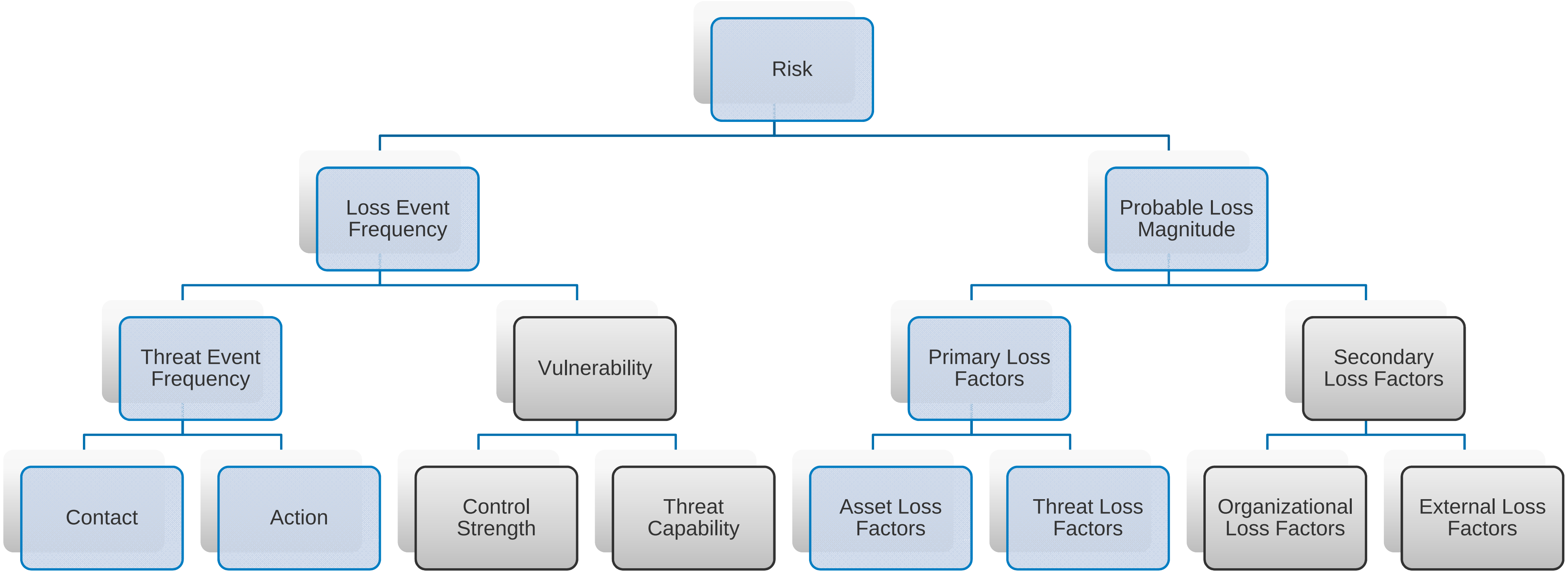
Color: Failure Probability
Size: Failure Propagation

http://www.systemcartography.info/sycatool

Agenda

- Motivation and Introduction
- Enterprise Architecture Management Patterns
- System Cartography Tool (SyCaTool)
- Visualizing Risks
- Conclusion and Outlook

Modeling risks using the Open Group FAIR risk taxonomy



Risk

Loss Event Frequency

Probable Loss Magnitude

Threat Event Frequency

Vulnerability

Primary Loss Factors

Secondary Loss Factors

Contact

Action

Control Strength

Threat Capability

Asset Loss Factors

Threat Loss Factors

Organizational Loss Factors

External Loss Factors

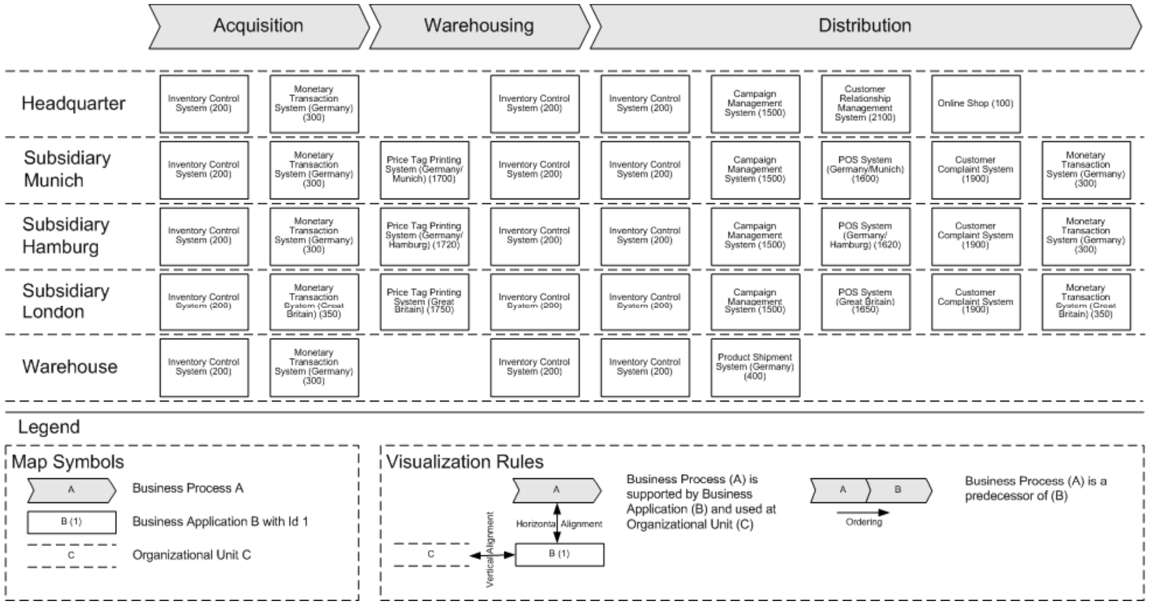
🟦 Included in the demonstration

⬜ **Not** included of the demonstration

Using a *Process Support Map* as a base map for visualizing risk

Two-dimensional space

- **X-Axis** for business processes
  - layer 0 to 3
  - linear process
  - viewed as a value chain
- **Y-Axis** for
  - organizational units
  - plants
  - target markets
  - products
  - …



	Acquisition		Warehousing		Distribution				
Headquarter	Inventory Control System (200)	Monetary Transaction System (Germany) (300)		Inventory Control System (200)	Inventory Control System (200)	Campaign Management System (1500)	Customer Relationship Management System (2100)	Online Shop (100)	
Subsidiary Munich	Inventory Control System (200)	Monetary Transaction System (Germany) (300)	Price Tag Printing System (Germany/ Munich) (1700)	Inventory Control System (200)	Inventory Control System (200)	Campaign Management System (1500)	POS System (Germany/Munich) (1600)	Customer Complaint System (1900)	Monetary Transaction System (Germany) (300)
Subsidiary Hamburg	Inventory Control System (200)	Monetary Transaction System (Germany) (300)	Price Tag Printing System (Germany/ Hamburg) (1720)	Inventory Control System (200)	Inventory Control System (200)	Campaign Management System (1500)	POS System (Germany/ Hamburg) (1620)	Customer Complaint System (1900)	Monetary Transaction System (Germany) (300)
Subsidiary London	Inventory Control System (200)	Monetary Transaction System (Great Britain) (350)	Price Tag Printing System (Great Britain) (1750)	Inventory Control System (200)	Inventory Control System (200)	Campaign Management System (1500)	POS System (Great Britain) (1650)	Customer Complaint System (1900)	Monetary Transaction System (Great Britain) (350)
Warehouse	Inventory Control System (200)	Monetary Transaction System (Germany) (300)		Inventory Control System (200)	Inventory Control System (200)	Product Shipment System (Germany) (400)			

Legend

Map Symbols

A Business Process A

B (1) Business Application B with Id 1

C Organizational Unit C

Visualization Rules

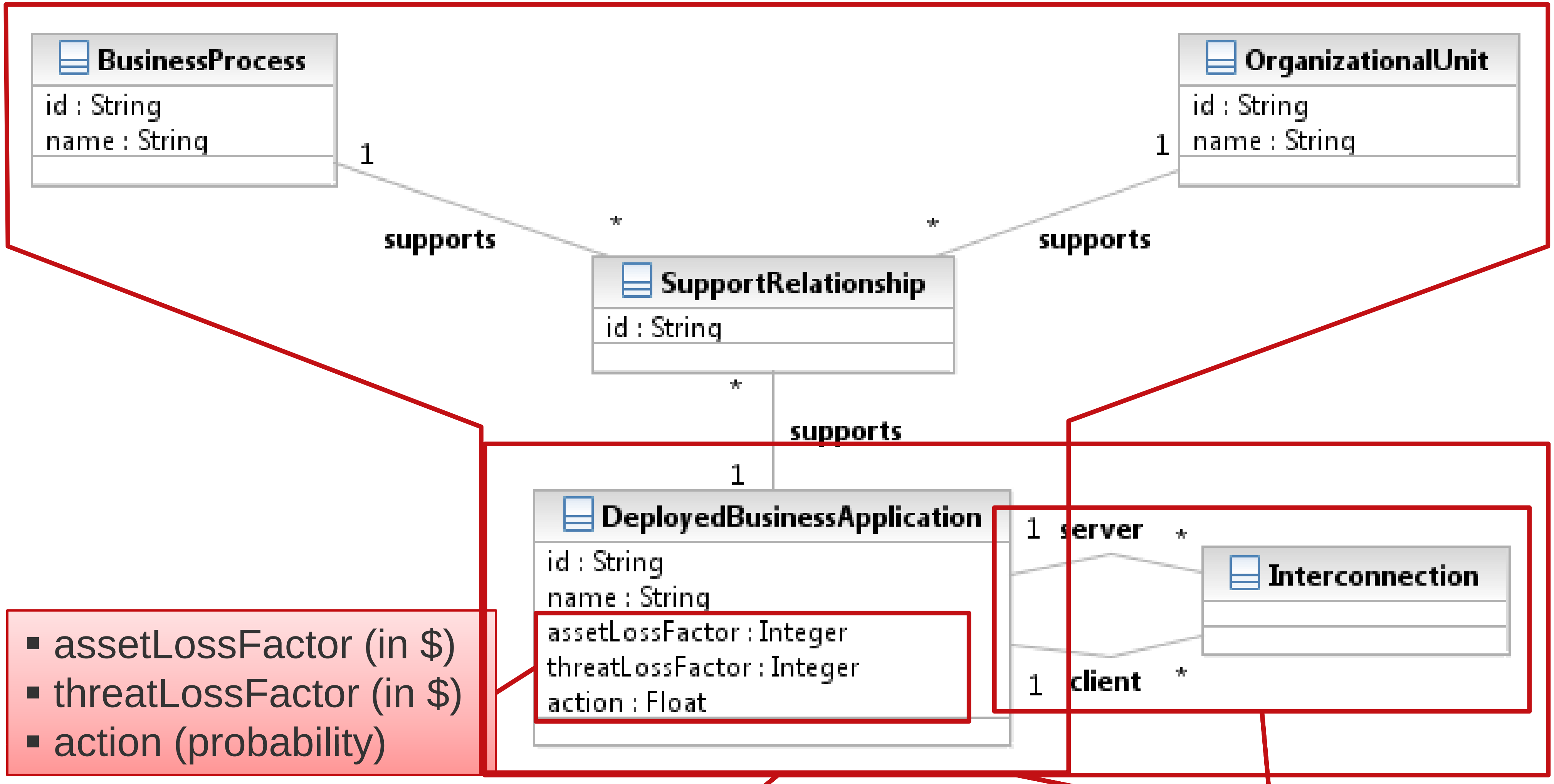
Business Process (A) is supported by Business Application (B) and used at Organizational Unit (C)

Business Process (A) is a predecessor of (B)

Useful for e.g. risk analysis, benchmarks, consolidation projects, etc.

Process Support Map (V-Pattern V-17) is part of the EAM pattern catalog

Information model used in demonstration of view generation for risk management



- assetLossFactor (in $)
- threatLossFactor (in $)
- action (probability)

EAM Pattern Catalog

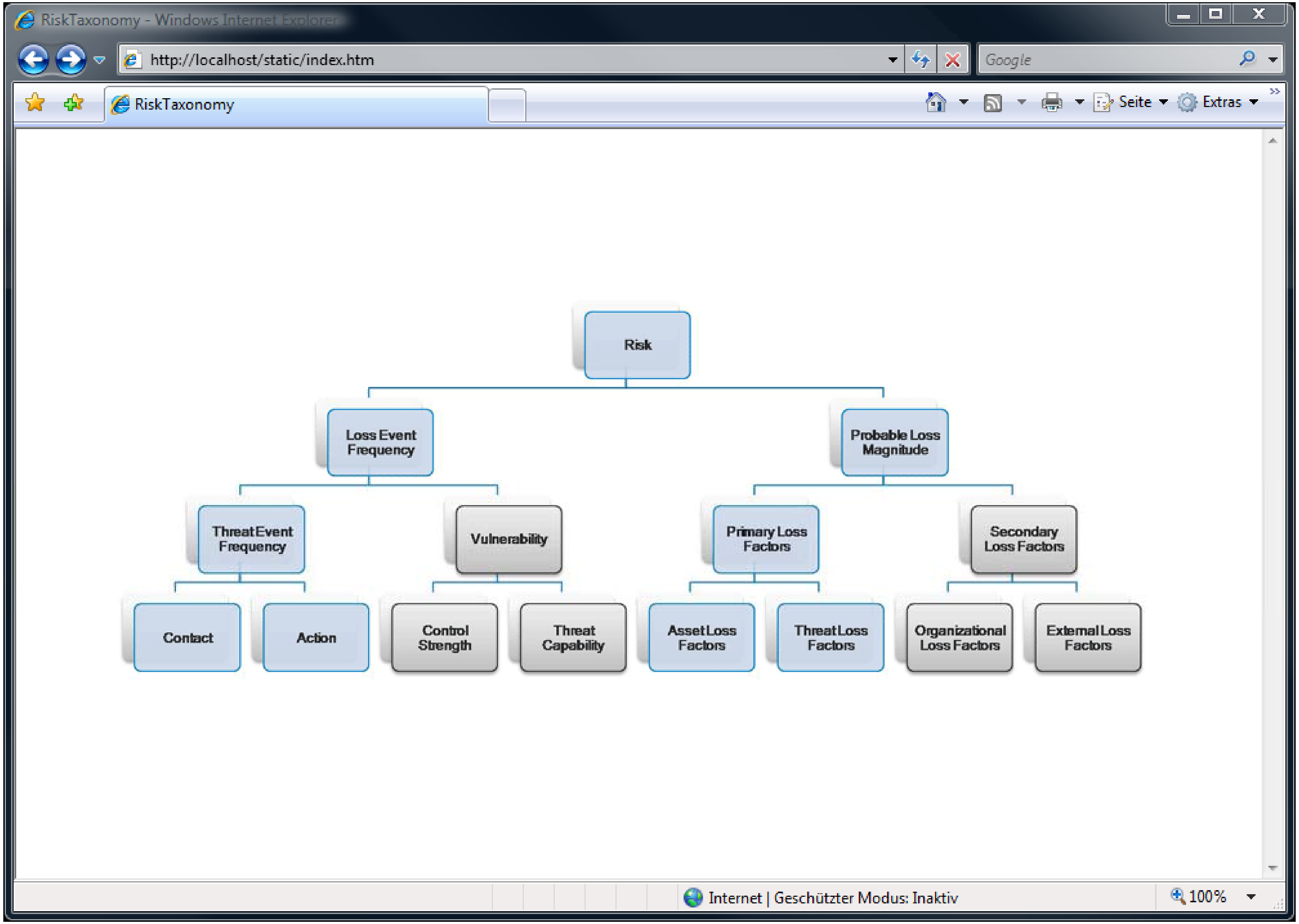
- Business Process Support (I-30)

EAM

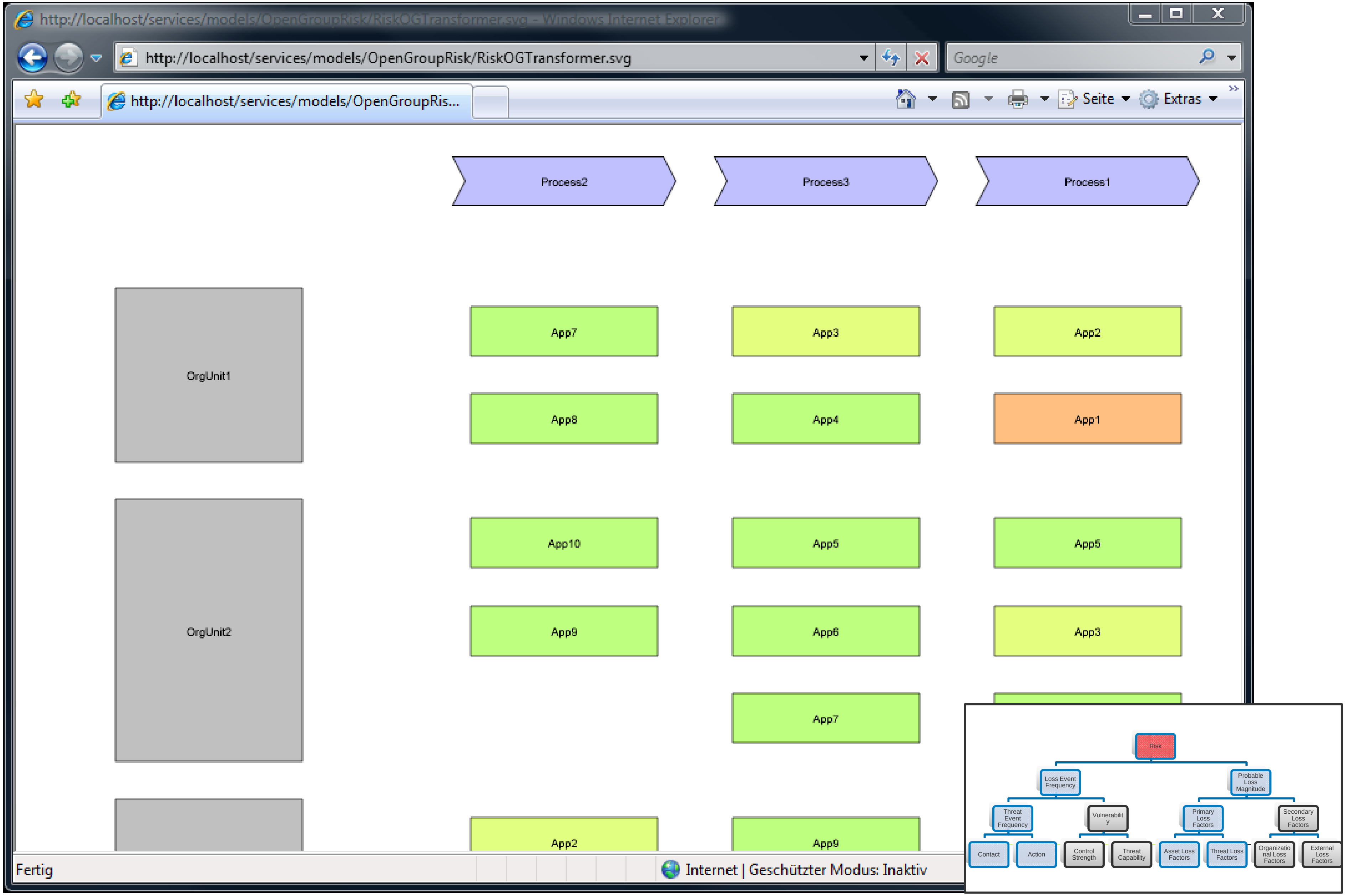
- Int

- contact (number of incoming interconnections)

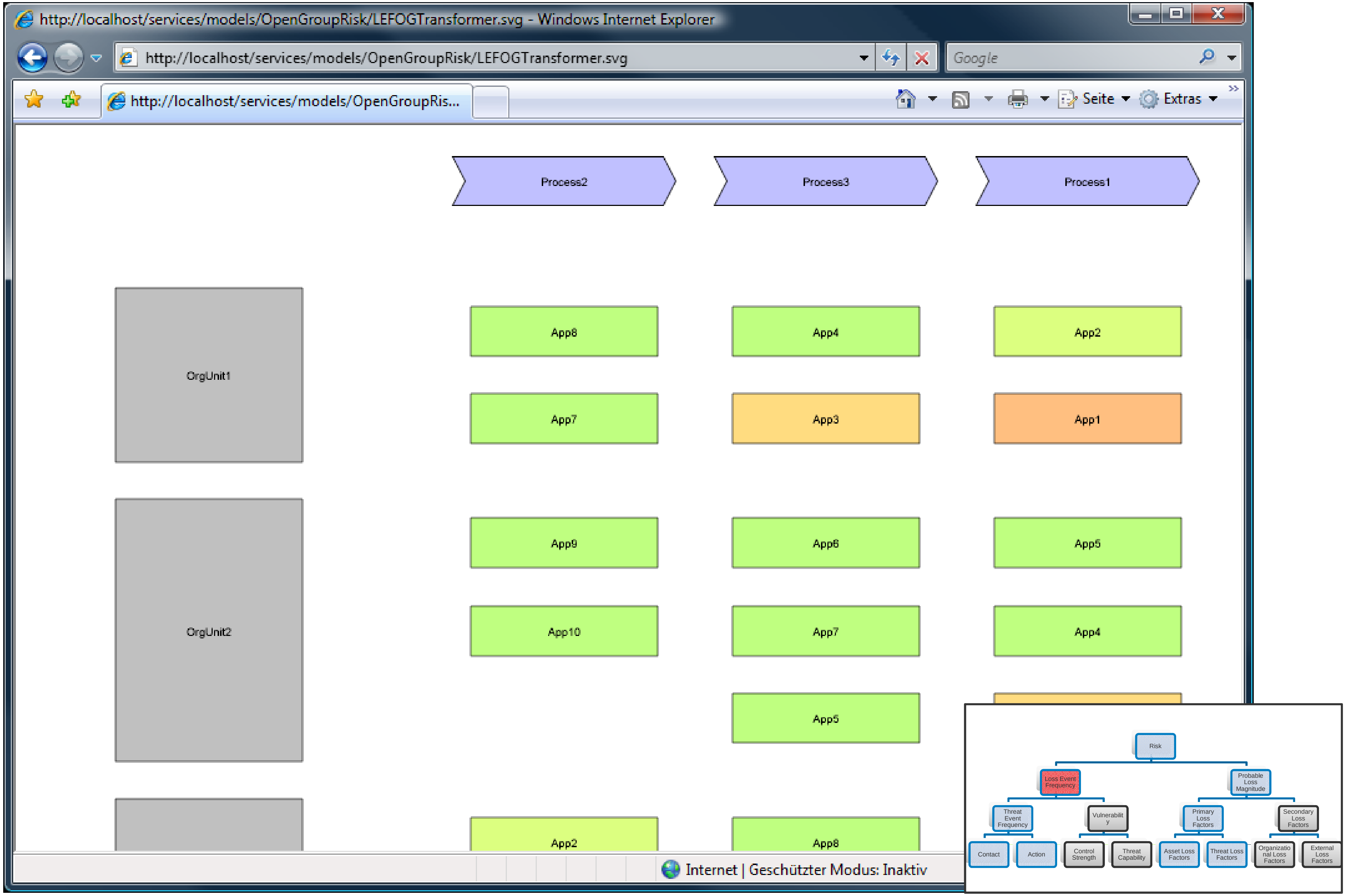
FAIR risk taxonomy – SyCaTool demo



Visualizing *Risk* for applications in respect to organizational units and processes



Visualizing *Loss Event Frequency* for applications in respect to organizational units and processes



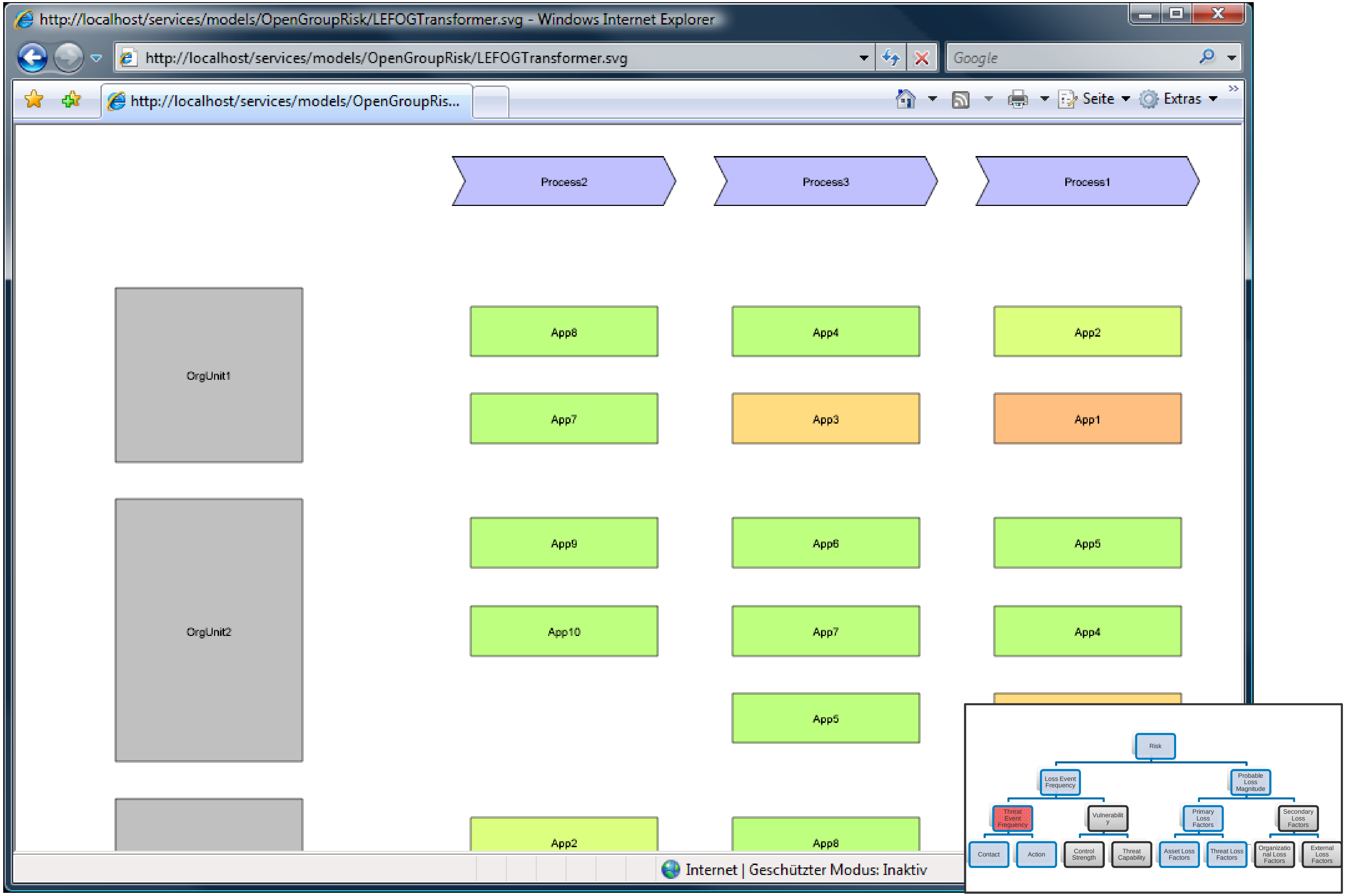
http://localhost/services/models/OpenGroupRisk/LEFOGTransformer.svg - Windows Internet Explorer

http://localhost/services/models/OpenGroupRisk/LEFOGTransformer.svg

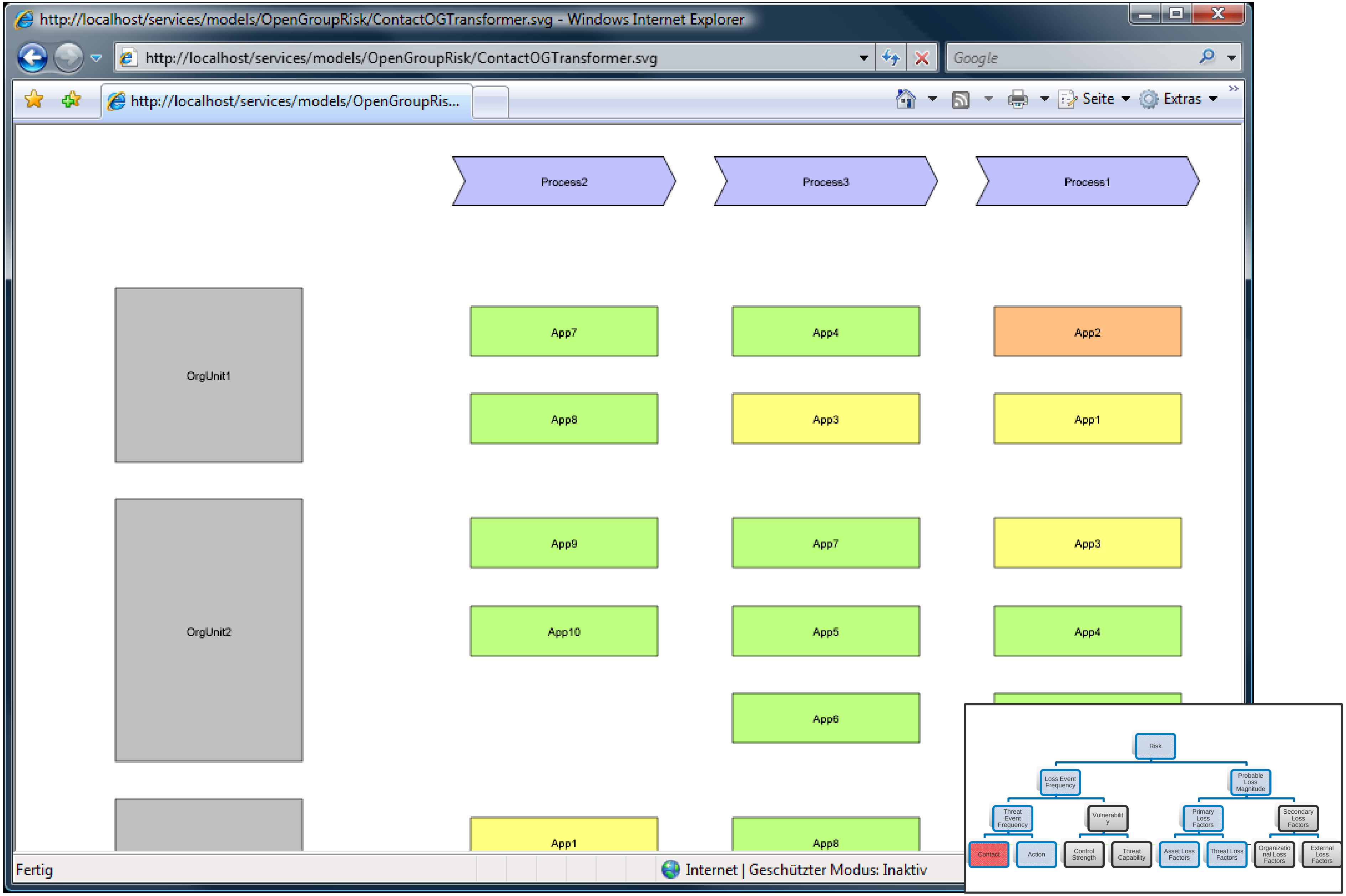
	Process2	Process3	Process1
OrgUnit1	App8 App7	App4 App3	App2 App1
OrgUnit2	App9 App10	App6 App7 App5	App5 App4
	App2	App8	

Internet | Geschützter Modus: Inaktiv

Visualizing *Threat Event Frequency* for applications in respect to organizational units and processes

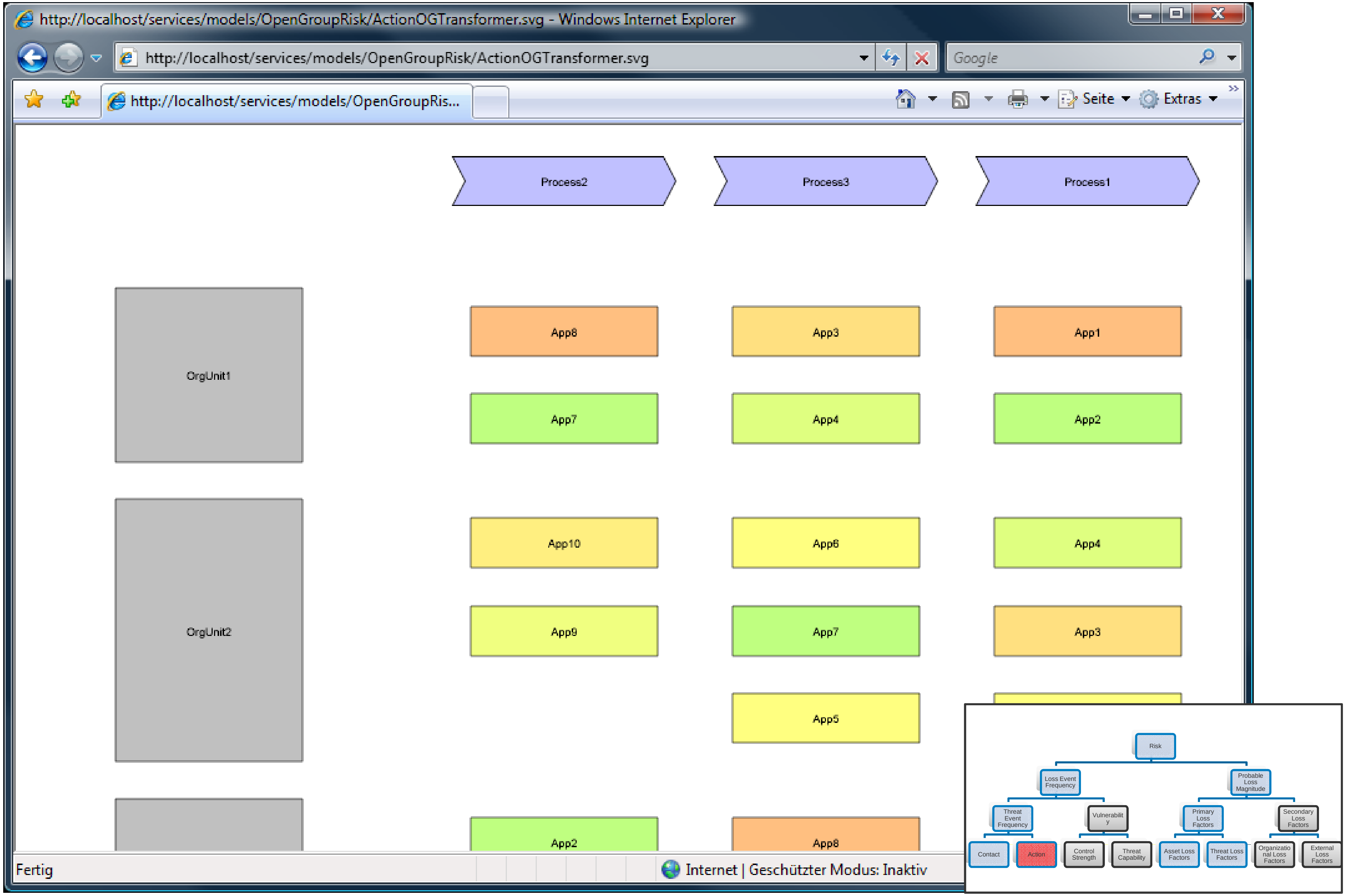


Visualizing *Contact* for applications in respect to organizational units and processes

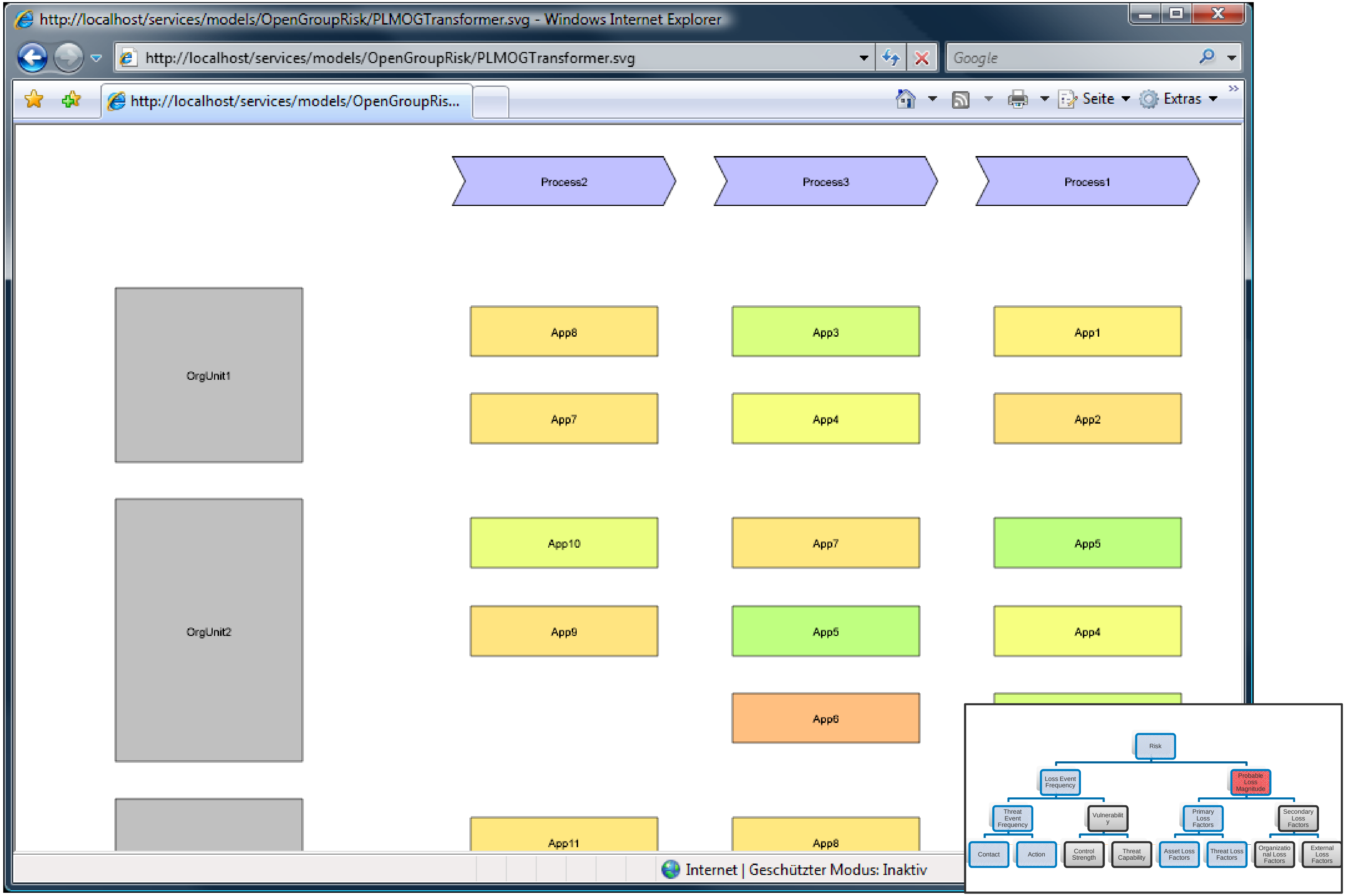

http://localhost/services/models/OpenGroupRisk/ContactOGTransformer.svg - Windows Internet Explorer
http://localhost/services/models/OpenGroupRisk/ContactOGTransformer.svg
Google
http://localhost/services/models/OpenGroupRis...
Seite
Extras
Fertig
Internet | Geschützter Modus: Inaktiv
Risk
Loss Event Frequency
Probable Loss Magnitude
Threat Event Frequency
Vulnerabilit y
Primary Loss Factors
Secondary Loss Factors
Contact
Action
Control Strength
Threat Capability
Asset Loss Factors
Threat Loss Factors
Organizatio nal Loss Factors
External Loss Factors

	Process2	Process3	Process1
OrgUnit1	🟩 App7 🟩 App8	🟩 App4 🟨 App3	🟧 App2 🟨 App1
OrgUnit2	🟩 App9 🟩 App10	🟩 App7 🟩 App5 🟩 App6	🟨 App3 🟩 App4
	🟨 App1	🟩 App8	

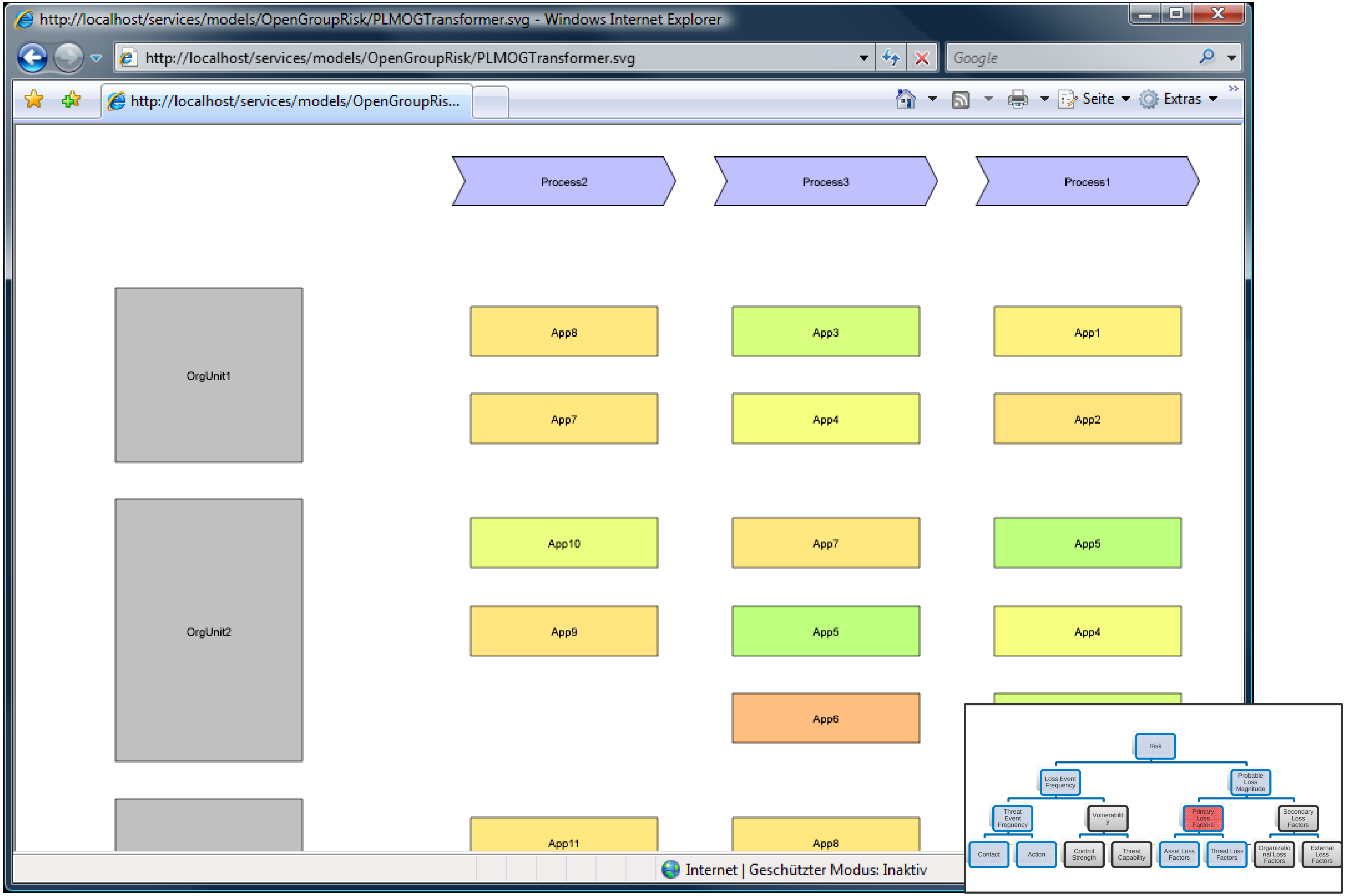
Visualizing *Action* for applications in respect to organizational units and processes



Visualizing *Probable Loss Magnitude* for applications in respect to organizational units and processes

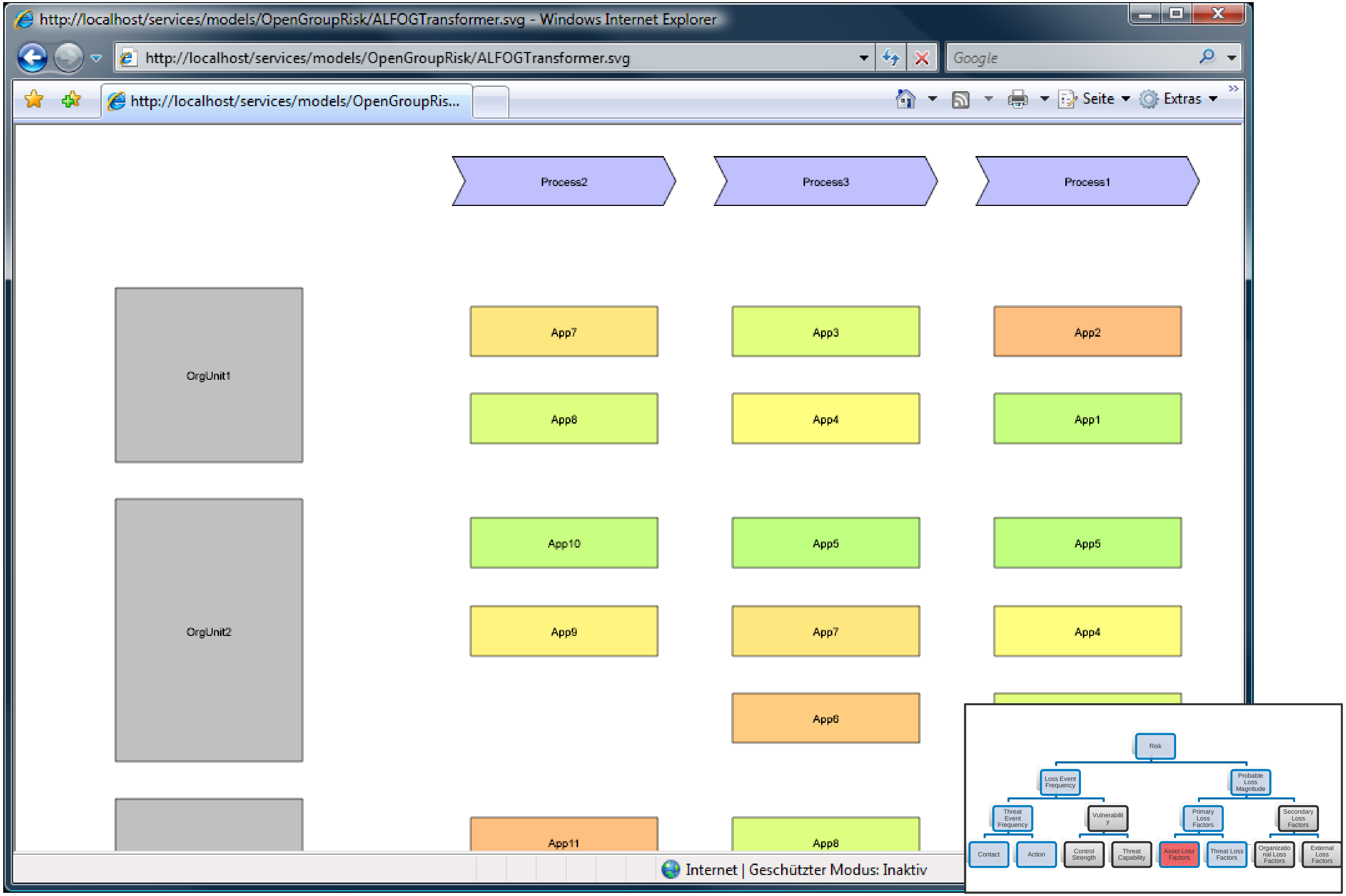


Visualizing *Primary Loss Factors* for applications in respect to organizational units and processes

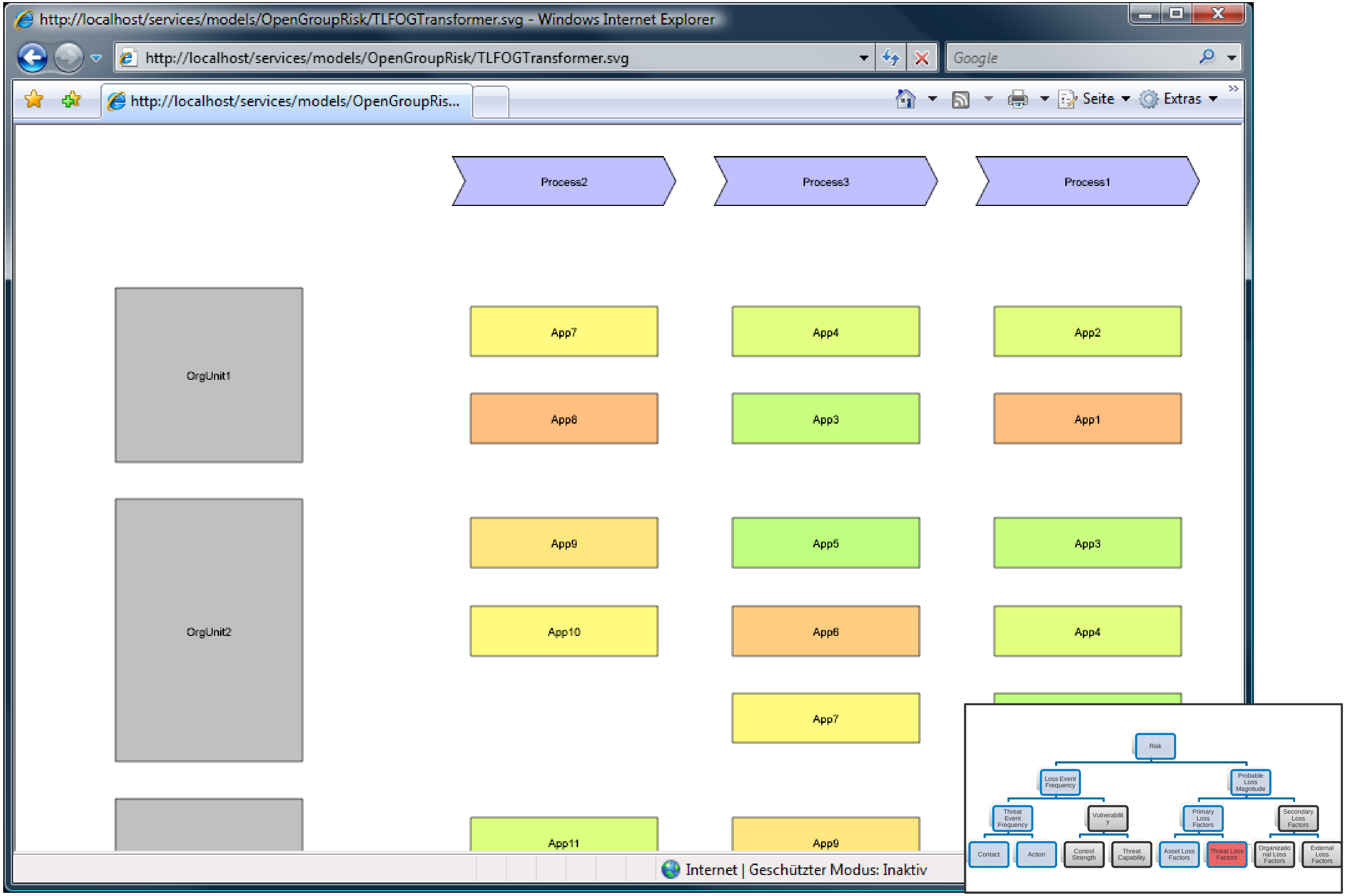


http://localhost/services/models/OpenGroupRisk/PLMOGTransformer.svg - Windows Internet Explorer

Visualizing *Asset Loss Factors* for applications in respect to organizational units and processes



Visualizing *Thread Loss Factors* for applications in respect to organizational units and processes



Agenda

- Motivation and Introduction
- Enterprise Architecture Management Patterns
- System Cartography Tool (SyCaTool)
- Visualizing Risks
- Conclusion and Outlook

Conclusion and outlook

Results of System Cartography project can be used to improve risk analysis described by FAIR risk taxonomy

- SyCaTool generates
  - customized visualizations and
  - supports multiple Stakeholder-oriented abstractions

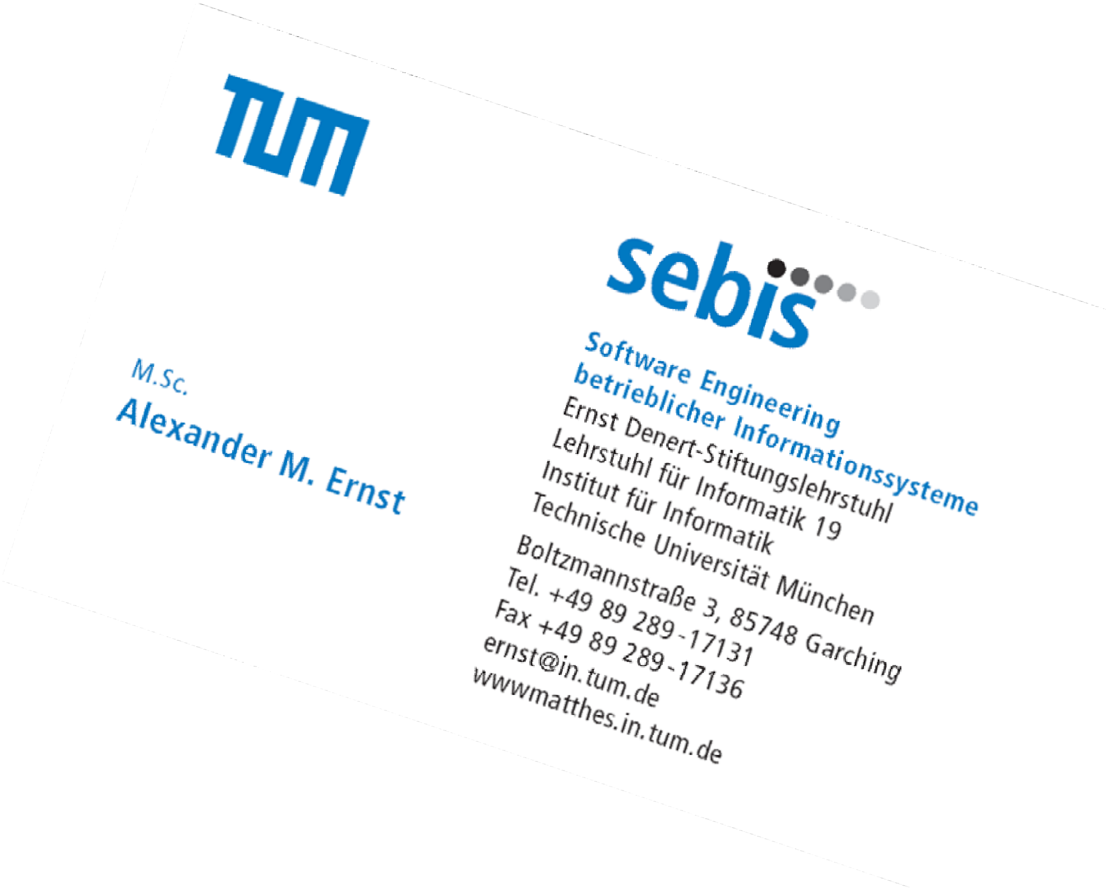
  ➔Prototypic implementation showed the potential for visualizing risks
- EAM patterns are a promising approach to capture, disseminate, and apply EAM knowledge

  ➔Utilization on risk management showed the same benefits

➔SyCaTool and EAM patterns should be used to further advance risk management practice

➔We are looking for people to support us extending the EAM Pattern Catalog concerning risk management

Thank you for your attention!



M.Sc.
Alexander M. Ernst

Software Engineering
betrieblicher Informationssysteme
Ernst Denert-Stiftungslehrstuhl
Lehrstuhl für Informatik 19
Institut für Informatik
Technische Universität München
Boltzmannstraße 3, 85748 Garching
Tel. +49 89 289-17131
Fax +49 89 289-17136
ernst@in.tum.de
wwwmatthes.in.tum.de

More information about

- System Cartography www.systemcartography.info
- EAM Pattern Catalog www.systemcartography.info/eampc-wiki
- SyCaTool www.systemcartography.info/sycatool

Backup

Business Application – Direct Attributes

- assetLossFactor (in $)
- threatLossFactor (in $)
- contact (numer of incomming interconnections)
- action (probability)
- organizationalLossFactor (in $)
- externalLossFactor (in $)
- controlStrength
- threatCapability

Business Application – Derived Attributes

- primaryLossFactor (in $) = assetLossFactor + threatLossFactor
- secondaryLossFactor (in $) = organizationalLossFactor + externalLossFactor
- probableLossMagnitude (in $) = primaryLossFactor + secondaryLossFactor
- contact (count) = number of interconnections associated to the BA
- threatEventFrequency (weighted count) = contact * action
- vulnerability = controlStrength and threatCapability
- lossEventFrequency (weighted count) = threatEventFrequency * vulnerability
- risk ($ per time) = lossEventFrequency * probableLossMagnitude