### D2.1 Draft Ontology Of Financial Risks & Dependencies Within & Outside The Financial Sector
**Vol. 1 - Building Ontologies**

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Parsifal Deliverable 2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Title</td>
<td>Draft ontology of financial risks and dependencies within and outside the financial sector</td>
</tr>
<tr>
<td>Version</td>
<td>2.0</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Work Package</td>
<td>WP 2</td>
</tr>
<tr>
<td>Deliverable Type</td>
<td>Other</td>
</tr>
<tr>
<td>Contractual Date of Delivery</td>
<td>31/01/2010</td>
</tr>
<tr>
<td>Actual Date of Delivery</td>
<td>02/02/2010</td>
</tr>
<tr>
<td>Responsible Unit</td>
<td>EDGE</td>
</tr>
<tr>
<td>Contributors</td>
<td>J.-Yves Gresser, B. Haemmerli, S. Morrow, K.Sullivan, H. Arendt</td>
</tr>
<tr>
<td>Keyword List</td>
<td>Ontology, Model, Glossary, Financial Market, Payment, Credit, Invoice, Risk, Business Continuity, Crisis, Trust, Privacy</td>
</tr>
<tr>
<td>Dissemination level</td>
<td>DD</td>
</tr>
</tbody>
</table>
Executive Summary

Words are important. Even in narrow or highly specialised fields, a common understanding is paramount.

The aim of this document is to contribute to a better, common understanding of the key concepts in risk management and financial infrastructures.

An ontology is a knowledge-sharing tool between persons belonging to a community of interest. A representational language of conceptual graphs or scheme-based systems, may be more familiar to IT professionals. However, as an ontology is often drawn from “story telling” by stakeholders, it will immediately look more familiar to them than any other mode of description.

Formal ontologies are also meant to be the backbone of the Semantic Web. They will be at the core of the next generation of navigation tools. It is not a coincidence that the W3C set up, in 2007, an incubator group (XG) on disaster management ontology: a common ontology based framework seems the only way to respond to the proliferation of participants in building information systems to support the management of emergency operations [1]. Recent advances in crisis management, show that while being primarily a model or an abstraction, an ontology diagram can be used as a “roadmap” in the real world. Some of the diagrams of this document could get a wide distribution in the financial world and beyond.

In PARSIFAL the goal is to work, “on identifying best practices and propagating these to existing or future CFI and CII owners, operators and service providers, that are gradually creating the chain of interconnected services required by large and small corporate customers”.

This advocates for more clarity and visibility i.e. to provide simple tools which contributors could use a) to capitalize on existing knowledge, b) to enable the recording of their own findings in a concise and illustrative way.

A 2008 survey on ontologies in the security area [4] concludes that while ontologies exist mostly on specific subjects, none is fully comprehensive nor able to evolve. SOA type security models are oriented toward IT development, they are either too abstract, or too narrow.

Fewer models exist in the financial sector [2, 13] and until recently there was no model combining security and finance ontologies.

In this document, we present:

— a simple model combining the ground ontologies from both the security and the financial sector (Chapter 3): This is likely pioneering work;

— ontologies in our three work areas (business continuity, control engineering, trusted sharing of sensitive /confidential information). These ontologies lay the ground for further approaches, while one-page roadmaps illustrate the instant benefits of our approach (Chapter 4);

— an extensive structured glossary (Vol. 2). This glossary is based on a compilation of terms, available from public institutions (like the European Central Bank) or known experts. It includes more terms appearing in the other deliverables of the Parsifal project and being especially relevant to our context.

1 DOW (Description Of Work)
The primary aim of the models was to share knowledge within the Parsifal project, inside the project team and with representative stakeholders, in other words to deal with semantic gaps. Using such models is not yet common practice. However it is getting wider acceptance in technical and business circles. It is still difficult to predict what will drive their success:

— immediate benefits from maps or vade mecum like the one pager on crisis, or
— actual improvements in risk mitigation or crisis management?

Likely both will have an impact. Improvements will need to be measured and quantified, thus methods (ontologies) of quantification, starting with “quantistic” risk management, need to be defined, standardized and disseminated.

The models were already instrumental in the gap analysis, from which research directions should emerge, like:

— identifying the role of stakeholders and spotting those who could take the leadership / responsibility of research,
— modelling itself at a degree which should be more comprehensive, evolving, standard and directly usable by the various players.

The attached glossary remains instrumental. The first it is more familiar to most. The second is a component of any ontology. Our pledge would be to maintain such a glossary beyond the life time of the project and to make it the companion of next versions of the CIIP handbook [32].

Acknowledgment

We wish to thank here the persons of the Banque de France who introduced us to the “Joint Forum” and who gave us access to their Structured Glossary on Business Continuity. It is when screening this glossary that some of the models presented in Chapter 4 were created. These persons also contributed to the first validation of these models. This initiative should contribute to the promotion of Business Continuity, a key issue for all sectors
# Table of Contents

1. Introduction: Presentation of the Document ................................................................. 6
2. Why Ontologies? ........................................................................................................... 7
   2.1. Glossaries ............................................................................................................... 7
   2.2. Ontologies ............................................................................................................. 7
   2.3. Ontologies and Glossaries .................................................................................... 7
   2.4. Ontologies as Communication Tools ................................................................. 7
   3.1. How Do Bankers See Themselves: Top Level Concepts In Finance ...................... 9
   3.2. Top Level Concepts In Risk Management .............................................................. 12
   3.3. Merging Risk and Finance Ontologies .................................................................... 13
   3.4. Conclusion to Chapter 3: ..................................................................................... 18
4. Representing Key Challenges & Adding to Current Knowledge .................................... 20
   4.1. Control Engineering ............................................................................................. 21
   4.2. Trusted Sharing of Sensitive Information .............................................................. 28
   4.3. Business Continuity ............................................................................................. 33
   4.4. Conclusion to Chapter 4: Standardization and Interoperability of Ontologies ........ 47
5. Conclusion .................................................................................................................. 48
6. References .................................................................................................................. 49
   Terminology & Ontologies .......................................................................................... 49
   Glossaries & Foundation Documents ........................................................................ 50
   CIIP Documents – Europe & USA ................................................................................ 51
   Regulation .................................................................................................................... 52
   Finance Sector – EU, USA, World ............................................................................... 53
   Supervision .................................................................................................................. 53
   Information Sharing ..................................................................................................... 53
   Identity ......................................................................................................................... 54
   Modelling ..................................................................................................................... 55
   Network & Services, Interdependencies, Dependability, Resilience ............................ 55
Appendix A. Appendix A Ontologies of Security – Citations & Further References .......... 57
Appendix B. Appendix B Diagrams from The EIIF XG Aug 2009 Report ......................... 59
Table of Diagrams

Diagram 1 - Top Level View of the Financial Sector ................................................................. 10
Diagram 2 – Top Level Model of the Financial Markets ............................................................. 11
Diagram 3 - Top Level Concepts of the Common Criteria .......................................................... 12
Diagram 4 - Top Level Concepts of Risk Management ................................................................. 13
Diagram 5 – Infrastructures ......................................................................................................... 14
Diagram 6 – Top Level categorisation of Risks& Related Concepts .......................................... 15
Diagram 7 – Top Level Concepts of Settlement and Risks ............................................................ 17
Diagram 8 - Top & Level 1 Categories of Parsifal Glossary ........................................................ 18
Diagram 9.1 – Concepts of Control Engineering in Financial Trading ......................................... 23
Diagram 9.2 – More on Control Engineering ............................................................................... 24
Diagram 10 – A Simple Ontology of Digital Identity ................................................................. 26
Diagram 11.1 – Trusted Sharing of Information .......................................................................... 30
Diagram 11.2 – Trusted Sharing of Information (from D2.3) ....................................................... 31
Diagram 12 – Scoping: Top Level Concepts of Business Continuity ......................................... 35
Diagram 13 – Concepts for a Business Continuity Strategy ....................................................... 36
Diagram 14 – Content & Outcome of a BCP (simplified) .............................................................. 37
Diagram 15 – A One-page Roadmap for a Crisis (Simplified) ..................................................... 39

Table of Figures

Figure 1 SOA Identity Ontology .................................................................................................. 25
Figure 2 Overview of the data classification process .................................................................. 32
Figure 4 – Top Level Structure for Defining Service Level Agreements (from G Dobson et al.) .... 44
Figure 5- QoSOnt Structure ........................................................................................................ 45
Figure 6 Overview of the Dependability Ontology ...................................................................... 46
Figure A.1 Conceptual Mind Map ................................................................................................ 59
Figure A.2 Phased Framework Model (see [Hackman, 2007], [Roper, 1998]) ............................ 60
Figure A.3 Orchestra Framework Example (see EU-funded ORCHESTRA Project) (See. ISDR Vocabulary and UNISDR Terminology) .............................................................. 60
Figure A.4 Tactical Situation Object Model in Open Advanced System for dISaster .................. 61
Figure A.5 OGC Feature Model - Open Geospatial Consortium (OGC) standards for spatial objects and relations in support of the Framework Concepts and to harmonize these as needed ...................... 61
Figure A.6 W3 Coordination Use Case Information Model based on data schemas from two existing emergency information systems, OCHA and Sahana ......................................................... 62
Figure A.7 W3 Coordination concepts framed under DOLCE-Lite Conceptualization ............... 63
1. Introduction: Presentation of the Document

This document is the second and final version of Parsifal deliverable D2.1. It starts with a short presentation on glossaries and ontologies (Chapter 2).

Our aim is to contribute to a better and common understanding of the key concepts in risk management and financial infrastructures at large. The key chapters, 3 and 4, cover:

Ontologies which lay the ground for further work, i.e. ontologies which can be derived from the description of financial activities, and ontologies which can already be derived from predecessors in the European Program for the protection of critical Infrastructures;

Ontology-based approaches. In this version they are applied to three key areas in our project

Control engineering. Recent stories have shown that lack of control is the heart of problems, which put the very existence of financial institutions or markets at stake. Some of these problems led to the current crisis;

Trust sharing of confidential information. An interpretation of Parsifal deliverable D2.3;

Business continuity. a wide corpus of knowledge is already accessible. However this knowledge applies to either interbank, or intra-bank, systems. A true end-to-end approach is still needed.

In the conclusion (Chapter 5) we try outlining the next steps.
2. Why Ontologies?

Words are important. Even in narrow or much specialised fields, a common understanding is paramount. Nowadays every discussion or technical paper will start with a series of designations (words, expressions) and definitions. Is it the natural bias we got from axiomatics? It could be. The process is so natural that we seldom reflect upon it [6].

2.1. Glossaries

Every new field of knowledge calls for a new vocabulary. As new concepts or artefacts emerge, they call for designations. Designations may come from the laboratories, from the experts, men or women “of the art”, or from “marketers”, sales people, design or media creators. Designations will use an old or a new word.

They will often appear in communication, marketing, sales and technical documents as list of terms. In a glossary, a term appears as a designation plus a definition. It may also include a few explanatory notes on technical, legal and other aspects. Terms usually appear in alphabetical order.

2.2. Ontologies

C. Roche [12] defines an “ontology” as “a shared description of concepts and relationships of a domain expressed in a computer readable language” An ontology deals primarily with (real or virtual) objects as diverse as: the consultation of a doctor, an illness, an engine, an animal, and a species.

An ontology is a representation, from one or more different point of view, of properties or characteristics of an object, conceptualised and bearing one or several names, in one or several languages. Such an object can be found in classical knowledge bases.

A “modern” ontology is “… A conceptualisation of a domain to which one or several vocabularies can be associated and which participates to the meaning of terms”.

Defined for a given objective, an ontology expresses a point of view shared by a community.

An ontology is represented in a language (explicit ontology) whose theory (semantics) guarantees the properties of the ontology in terms of consensus, coherence, sharing and reuse.”

2.3. Ontologies and Glossaries

In most glossaries the alphabetical order puts related terms apart. This is true whichever (alphabetical) language is used. Thus glossaries are good at providing definitions for terms which were already spotted or heard. They are more difficult to use when discovering a new field.

An ontology provides formal ways of assessing the properties of an object. As such, it adds clarity to the definition of concepts and their relationships.

2.4. Ontologies as Communication Tools

An ontology may rely on “well formed” formulas. Syntax and semantics may be precisely defined, thus ensuring almost automatically their formal consistency. An ontology may in itself be used as an exchange format between machines.

In our context an ontology is primarily a knowledge-sharing tool.
Artificial Intelligence (AI) representation languages, conceptual graphs or scheme-based systems may be more familiar to IT professionals. However as an ontology is often drawn from “story telling” [14] by stakeholders it should immediately look more familiar to them than any other description.

Last but not least, formal ontologies are supposed to be the backbone of the Semantic Web. They will be at the core of the next navigation tools.

In 2007 Tim Berners-Lee himself reported on the Semantic Web forum an exciting visit from the students in Sri Lanka who had just received an award for their open source disaster management system²:

“I remembered many conversations about the desirability for wide interoperability³ in emergence and disaster situations. I suggested the Sahana folks provide RDF feeds of, for example, missing persons, found persons, shelters, relieve groups and resources on the ground, and other things they track. I started a wiki page to capture a little of this… A possible next step would be an Incubator Group (XG) for a disaster management ontology development.” The EIIF XG is currently active [1].

Parallel advances in crisis management (see section 4.3) show that while being primarily a model or an abstraction, an ontology diagram can be used as a “roadmap” in the real world.

In one of the French leading financial institution top managers already get a “Structured glossary on business continuity” in their “Crisis briefcase”. The crisis life-cycle diagram of section 4.3.4 will be part of the next update.

---

² The system is downloadable from http://www.sahana.lk
³ A key goal.

Our stakeholders either come from the business side or from the IS/IT side, either from the financial sector and/ or from research. They need to start developing a mutual understanding. Simple diagrams about how they represent knowledge in their field may be the starting point.

In section 3.1 we start with top level diagrams from the finance industry. Section 3.2 is devoted to high level concepts of Risk Management as can be derived from CIIP and others. Section 3.3 describes an attempt to merge ontologies.


Despite several developments [2, 13] there is currently no standard comprehensive ontology for finance and banking. In this respect the initiative of the ECB to launch on September 30, 2008 a public consultation on a GLOSSARY OF TERMS RELATED TO PAYMENT, CLEARING AND SETTLEMENT SYSTEMS [16] was more than highly welcome.

The following relies heavily on this draft as well as categories which may arise from the organisation of standard bodies or documents (ISO, CEN, TWIST etc.).

3.1.1. Top Level Concepts

When describing the financial sector two types of terms are used. They may be:

— specific to finance like payment, securities clearing, derivative, or
— also used in other sector like system, rule, process… infrastructure.

Diagram 1 is a top level view of key concepts. The grouping of these concepts into more abstract notions (Rule, Role, Service, Infrastructure, System, Process, Event) is reflected into the graphics.

The list of relationships is not exhaustive, e.g. an “event or behaviour” may trigger a “process” while the result of a process may be an event or a behaviour (like the transition to another process).

In this diagram the concept of (Business Entity) does not appear. Beyond bank or credit institution, or insurers, entities are designated by their Role (see broker, payment operator). Thus the concept of Role seems more relevant. It is not developed at this stage because it is very much context dependant.

NB The concept of “Insurance” does not appear in the ECB glossary.

Legend

Blue circle or rounded rectangle: regulation, regulation scope
White circle or rounded rectangle: role or players.
Light yellow circle or rounded rectangle: service, service scope.
Dark yellow circle: infrastructure/ platform/ system
Blue rectangle: process, event.
Diagram 1 - Top Level View of the Financial Sector

The concepts appearing in this top level view can be used to regroup terms which will in any glossary fall apart. This is illustrated in the following table on the list of terms from the ECB glossary.

Please take note of the (standard) linguistic bias which makes every term singular, unless only the plural exists.

---

4 NB: Every diagram in this document was build with Ontologos Semantic Network Craftbench.
3.1.2. **A Top Level View Of Terms Related To Financial Markets**

Diagram 2 covers the Financial Markets. It can work in at least two ways:

As a validation tool for the top level diagram, of which it provides a specific view; and

As a top level representation of a specific domain.

**Legend** (see diagram 1, extended with light grey circle or rounded rectangle for customers, different shades of yellow for service activities or financial instruments)

**Diagram 2 – Top Level Model of the Financial Markets**

Other areas / domains could be represented in this way.
3.2. Top Level Concepts In Risk Management

Section 3.2 deals with risk in a general context. The purpose is to extract the concepts which will be merged in section 3.3 with those extracted from the financial sector.

This section seems to imply that the risk and finance worlds evolved separately. This is not true as banks were and are still often at the forefront of security. This is just a working hypothesis.

3.2.1. Extending the top level concepts of the “Common Criteria”

Diagram 3 is a direct transcription of the “top-level concepts” diagram of the “Common Criteria” document [28].

Diagram 4 is the result of the validation of diagram 3 in different contexts. It is a combination of top-down and bottom-up approaches in business continuity and/or crisis management. CIIP terms start appearing as well as broad categories of concepts like

Player/Actor/Stakeholder (owner is just one of them);

Asset, which may designate an infrastructure, a product or a service based on an infrastructure as well as another asset of a stakeholders. In the CIIP terminology this tends to be split between “Infrastructure” and “Service”;

Potential (a category to which “Risk” and “Threat” belong), for which a lighter background colour is used;

Actual (as the opposite to potential, to which “Event” or “Behaviour:, in the UML sense, belong).
The model is supplemented with standard types of countermeasures, which are also called “Measures” later on, and which may appear under Risk Mitigation in the glossary.

“Vulnerability” is taken as an example of a “Risk Factor” (see Parsifal D2.3). “Awareness” appears as a relationship.

### 3.3. Merging Risk and Finance Ontologies

The first idea was to merge only areas which are closely related to CIIP i.e. concepts related to risks, infrastructures, systems and selected processes. This already provides a kind of gap analysis between business and technology terminologies.

This is however not sufficient. Financial actors rely heavily on rule books. These rule books may cover issues as diverse as service domains, schemes for operations in payments or financial trade, interbank exchange systems. A rule may apply to a specific system, platform or infrastructure. It may extend to the end-user of a service. Thus the concept of Rule may include
Processes, Operations and Oversight / Supervision / Control. As such these concepts are relevant to Parsifal.

The difficulty is that a set of rules, e.g. the concept of cap in gross settlement systems, may be both technical and financial: an interesting subject in itself. This bears an inherent risk of overconfidence, to say the least, of the business managers in their technical system. This might be coined as an “Oversight Risk or a “Governance risk”. This is an issue for section 4.2 on Control Engineering.

In any case the common list must include some (not all) of the rules and name of few critical players / participants.

A few terms in the table call for more clarity: infrastructure, risk, system etc. This is illustrated in the following diagrams.

**Diagram 5 – Infrastructures**
The relationships between concepts are either extracted from definitions, or from the original text or … inferred from the authors’ experience. The diagram is drawn in such a way as to minimize the number of these relationships.

In this model we take “criticality” as an attribute.

Diagram 6 – Risks is derived from diagram 2. All concepts derived from merging the security and finance ontologies are not taken into account, as a few of them are taken care of under one heading, e.g. those related to critical staff.

This diagram may already look too complex. It calls for sub-ontologies which are the subject of section 4.
Market risk is actually the combined outcome of risks figuring in the diagram. One may be surprised that resilience appears as a “risk factor”. We take that a factor can work both ways in a positive or a negative way. Also resilience is polysemic: it may be a factor or a goal!

This type of diagram may act as a check list even for our own exercise e.g. Threat Agent does not appear in the initial lists, nor the expression Risk Mitigation. They will need to be added to the glossary.

Diagram 7 – Settlement & Risks is another way of combining risk and sector specific ontologies.

The model is like its predecessors, based on our simple rule – player – service – infrastructure - system – process – risk meta-model. It is a semantic model relying on terms which are specific to settlement, most of them recorded in the Glossary.

The concept Settlement Rule includes items ranging from broad settlement principles (e.g. gross or net settlement), settlement obligations to “components” or “parameters” of a settlement system like the settlement cycle, the finality or the cut-off time.

A special set of rules are the Lamfalussy Standards applying to systematically important payment system (bottom left of the diagram).

As mentioned already, parties involved in a settlement system get special names. These names refer to specific responsibilities, rights and duties which are normally documented in rule books or SLAs. As already noted the way it is done is a key issue.

The other stakeholders are not included in the diagram. Settlement is from the point of view of an end-customer the final process. Thus its duration (Settlement Lag), as well as its termination, will have an impact on other processes. For the latter we just mention “Settlement Failure” which may cover a wide range of issues and “Gridlock”, typically something which systems are designed to avoid. The lag inherent in every settlement system is an important risk factor (see bottom right of the diagram). In this diagram we represent it as a relationship. As we do with risk mitigation. These are just shortcuts.

Two types of concepts are represented around Settlement System: the first type refer to the way the systems are working, the second to the type of set up for these systems to operate.
Diagram 7 – Top Level Concepts of Settlement and Risks
3.4. Conclusion to Chapter 3:

3.4.1. Structuring the Parsifal Glossary

In PARSIFAL one of our goals is to work “on identifying best practices and propagating these to existing or future CFI and CII owners, operators and service providers that are gradually creating the chain of interconnected services required by large and small corporate customers”.

Chapter 3 deals directly with terms from a terminology or an ontology perspective:

Diagram 1 - Top Level View of the Financial Sector- and diagram 2 – Top Level Model of the Financial Markets- are derived from financial glossaries;

Diagram 3 - Top Level Concepts of the Common Criteria- and diagram 4 - Top Level Concepts of Risk Management are derived from known models / glossaries in the security domain.

Diagram 5 –Infrastructures-, diagram 6 – Top Level categorisation of Risks & Related Concepts – and diagram 7 – Top Level Concepts of Settlement and Risks combine these diagrams in such a way as to achieve mutual understanding between stakeholders coming from different horizons with their own specialty language.

The Parsifal Glossary (Vol. 2) is structured along 5 top level concepts - Governance, Stakeholder, Risk, Infrastructure, Technology to which we added Identity as this is a domain requiring special attention.

Diagram 8 - Top & Level 1 Categories of Parsifal Glossary
3.4.2. More on Stakeholders

The first specific goal of the Parsifal project, was to bring together qualified financial industry and R&D stakeholders from the various ICT Security areas. We got a strong representation from all groups whether in the private sector, on the research side, or the suppliers, and an excellent coverage of all required professional areas: column 1 in table 1 lists their profile.

The next challenge was to identify which of these stakeholders could endorse the recommendations and take the leadership in specific research directions. This seems to be more related to their statutory position (columns 2 to 4).

Table 1 – Type and Role of Stakeholders

<table>
<thead>
<tr>
<th>Profile / Position</th>
<th>Regulation / Standards/ Best Practices</th>
<th>Focus group / dedicated entity</th>
<th>Infrastructure / operator / service provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Industry&quot; leaders</td>
<td></td>
<td>s</td>
<td>P</td>
</tr>
<tr>
<td>Large payment processors in Europe</td>
<td></td>
<td>s</td>
<td>P</td>
</tr>
<tr>
<td>Central banks / regulators and their lobbyists</td>
<td></td>
<td>P</td>
<td>s</td>
</tr>
<tr>
<td>Drivers/ influencers of transaction banking, operating within a bank</td>
<td></td>
<td>s</td>
<td>P</td>
</tr>
<tr>
<td>Strong influencers of transaction banking, operating outside banks</td>
<td></td>
<td>P</td>
<td>s</td>
</tr>
<tr>
<td>Specialists/ functional leaders</td>
<td></td>
<td>s</td>
<td>P</td>
</tr>
<tr>
<td>Research/ research consultants/ Academia</td>
<td></td>
<td></td>
<td>P</td>
</tr>
<tr>
<td>Suppliers (security / technology solutions providers?)</td>
<td></td>
<td>s</td>
<td>P</td>
</tr>
<tr>
<td>Strong influencers of security / technology solutions</td>
<td></td>
<td>s</td>
<td>P</td>
</tr>
<tr>
<td>Other candidates</td>
<td></td>
<td>?</td>
<td>?</td>
</tr>
<tr>
<td>European Commission (EC) representative</td>
<td></td>
<td>P</td>
<td>s</td>
</tr>
</tbody>
</table>

Legend: P means primary, S secondary

It should be noted, that standard categories in financial ontologies are more business oriented see diagrams 1, 2, 7 while they serve mostly financial regulatory purposes. A standard correspondence should be established between the traditional categories and those of table 1 related to CIIP.

---

5 D1.1 - Report on ESG Establishment, Bernhard Haemmerli, Michael Freiberg, January 2009
4. Representing Key Challenges & Adding to Current Knowledge

The diagrams presented in chapter 3 lay the ground for building a more complete knowledge base. The purpose of chapter is to illustrate how:

— more sophisticated ontologies could be build from the ground ontologies of chapter 3;
— knowledge can be added to the existing knowledge base(s).

Diagrams of version 1.0 were based on:

— the International Critical Information Infrastructure Protection (CIIP) Handbook, “the product of a joint effort within the CRN partner network”, “an initiative for international dialog on security risks and vulnerabilities, risk analysis and management, emergency preparedness, and crisis management” [32];
— the CI2RCO reports [35];
— TWIST and contributors [17];
— the DOW and the first position papers issued in Parsifal, and
— Proposals for additions to the ECB glossary related to security,
— the Joint Forum [47].

These diagrams were supplemented, or updated, with considerations arising from further developments in Parsifal. Chapter 4 is structured along the three key Parsifal work streams:

Control engineering in Controlling Instant On Demand Business in Critical Financial Infrastructures (CFI): Authentication, Identity Management, Resilience and Denial of Service) (section 4.1);

Trusted sharing of confidential information in Entitlement Management and Securing Content in the Perimeterless Financial Environment: Identity, Policy, Privacy and Audit (section 4.2);

Business continuity in Business Continuity and Control in an Interconnected and Interdependent Service Landscape: Cross Border and Cross Organisations (section 4.3).

“Control engineering” is an emerging field. The current crisis exacerbates the needs for developments in this area.

“Trusted sharing of confidential information” was already identified as a key research area in the programs of the European Commission. For the public it is mostly related to privacy and issues like “identity theft”. There is much more to it while value chains extend and fragment, while the trends towards virtualization accentuates. This is developed in D2.3. Here the specific knowledge of D2.3 is aggregated to other field.

Business continuity is likely the area which adheres most to other CIP projects. It is an area where the bank supervisors did, and are still doing, extensive work. Section 4.3 is building on their current knowledge. Crisis management is at the intersection of business continuity and control engineering.
4.1. Control Engineering

The complexity and volume of today’s financial trade fall beyond current state-of-the-art techniques for Internet connected process protection. The proof is in the repetition and in the acceleration of catastrophic events since 1987. The number of cases was small until the late 2007 but a single of them already incurred huge financial losses, threatening the viability of a bank, whatever its size.

In early 2008 the confidence of in banks and financial markets was already at stake. This should have encouraged key players to test new methods and solutions which can prove their efficiency and security via verifiable protections in an objective fashion. This did not happen!

The rest is NOT history as it led to the worst financial crisis in our times, a crisis which may not have reached its peak yet.

On July 3, 2008 the banking supervision authority (Commission bancaire) decided to issue a reprimand (blâme) and to fine the SG (amount 4 M euros). It is outside of the remit of this document to go into a detailed analysis of the case. We are only interested in enriching our list of problems, incidents, challenges etc.

With a small group of bankers we reached a consensus on the following list:

- Anomalies in book-entry of trade operations seem to be by far the most frequent problem in financial trading rooms,
- Cancelling or amending book-entries. In the case of SG this is how the “rogue” trader was able to hide actual operations,
- Legal safety in a fast moving environment. In financial trading the issue is how to secure a business where products are evolving so fast
- Fragmented environment where multiple players are involved in a single transaction, this makes
- Limit management difficult, as well as

Aggregation of data, while the goal is to give the right information to right person in due time, to have this person read the information and be prepared to take the required decision,

- Following on collateralisation and other guarantee schemes, this relates to
- Counterparty eligibility. Eligible Counterparty is already on the list of ECB terms.

As far as solutions or directions for studies are concerned, we can only make a tentative list of directions to explore:

- Consistency intra and inter applications,
- Ongoing monitoring & control. The ability to track and audit EVERY step of a transaction, or at the very least, accumulate the limits of a financial transaction in real time, is a key aspect. Current measures and actions fall short in this respect. Controls remain very fragmented and are not cognizant of fundamental barriers to verifiable business process: End to End visibility and auditability. A complete vision of risks and solutions is necessary.

When a hacker meets an obstacle, they are not likely to confront it but to circumvent it. Organisations and IT systems always have holes or small “cracks” which attackers can exploit.
Responding individually to a check list of threats, is not sufficient. Complexity is a challenge in itself, which state-of-the-art solutions fail to deal with.

- Delegations & accountability. Every participant in e-business should be certain that “individuals or systems who communicate or transact via the Internet, are truly who they appear to be, and do only those things they are authorized to do.”

A common failure is due to overconfidence in the technologies of governance, identification/authentication and audit. This leads business managers to actually give up their responsibilities to IT personnel in solving the issue.

- Authenticity and Integrity guarantees,
- Tools, models, patterns,
- Deperimeterisation. SG internal survey states that the trader was able to forge e-mail. Again this can only be solved from end-to-end, between ALL participants in a financial transaction. This clearly goes beyond the perimeter of SG and emphasizes the crux of the matter for open Internet communications.

This is another lesson from the SG: most analysts restricted their consideration to problems within the perimeter of the bank. They agree about the possibility of problems extending beyond this perimeter, but they believe these problems are too complex and beyond the reach of current technology. This is an aspect we should consider in this project. It is closely related to the deperimeterization advocated in section 9.0 of D2.3.

Briefly stated, the challenge is two folds:

- first to be able to react in real time to expected or unexpected events,
- second to synchronize with market innovations.

Diagram 9.1 is a derivation of diagram 2. It is a semantic interpretation (the process is called by linguist “semasiology”) of the preceding text. It shows how two lists and one statement can be interpreted in a model where the concepts are assigned to the relevant categories – actors, rules, potentialities etc. and their relationships made explicit. Please take note that:

- detailed definitions can also be extracted from the text and terms added to a glossary,
- it is a top level model. If we were to work further on the case a more detailed model would be needed.
Diagram 9.2 is diagram 9.1 supplemented with notions highlighted in scenarios, challenges and recommendations formulated under work stream 1 during both Frankfurt workshop, including:

— more potential attackers (cybercrime, ex-employee),
— a wider variety of attacks through cyberterrorism or Trojan virus,
— a more detailed list of possible counter measures, like out-of-band, closed-user-groups (CUG), secure storage and dissemination of identities, location and environment sensitive transactions, supported by standard classification of identity attributes, trust (data) indicators on platform managing multiple identities,
— explicit rules or goals related to accountability or compliance, and
— re. technologies a focus on virtualisation (cloud computing).

A few changes are worth noting:

— End to end is definitely a goal,
— Identity management is not just a measure, but is at the heart of systems / applications (to the point where ID infrastructures should be viewed as critical infrastructures see section 4.1.1).
Diagram 9.2 – More on Control Engineering
4.1.1. Identity Management & Protection [57 to 76]

The next figure is an example of the few ontologies related to “identities”.

Figure 1 SOA Identity Ontology

Security Patterns Map

The next paragraph present an attempt to get a more holistic view of the field.

Top Level Concepts

ID records bear information about distinguishable entities (an entity may be a physical person, a (virtual) avatar, a company: ultimately an addressable physical or virtual object).

Keys or ciphers are at the heart of the security mechanisms. They are a list of characters, thus data which can be recorded, duplicated, transmitted (exchanged).

---

6 Source: Securing Service-Oriented Architectures using a Model-driven Approach, Nelly A Delessy, July 2007
Certificates combine keys and information related to entities and a usage context. They can be used as keys.

Data (information, records) are created, updated, revoked (deleted), stored, transmitted (exchanged) (the IDM Cycle) and used in different application contexts. ID data (information, records) may be used for identification, authentication, authorization (validation): this completes the ID Life Cycle.

Data (information, records) have properties. These properties may be represented by attributes. Some of their properties may result from categorization e.g. sensitive vs. non-sensitive, private vs. public. There are currently very few regional or global agreements on categorization. A category is usually specific to a local government or even to an application!

Diagram 10 – A Simple Ontology of Digital Identity

ID Infrastructures
ID data (information, records) reside in directories, repertories, ID token. trace of ID data (information, records) may reside in log data bases of many kinds (AIP, merchants, trade or payment platforms), thus

“IDM becomes a CI in its own right” “Secure storage and dissemination of ID and credentials (is needed)” (WS 1 - Scenarios).

ID data (information, records) circulate via transmission media. Protection of transmission media is also needed (see latest report on the security of TCP/IP).

---

7 Interoperability relies first on common and public codes/ (nomenclatures)
More on identities is to be found in Parsifal deliverable D2.2. These documents includes considerations on:

- Top Threats against privacy, abuse: fraud, denial of service from lack of integrity, data (information, records) theft or counterfeiting, Asset (property incl. data) loss;
- Top Concerns Shared with Other Sectors like interoperability, overall privacy challenges, protection against potential abuse, denial of service;
- Specific Concerns to Finance like actual end-to-end in the context of longer value chains (interdependencies), value driven transactions, volume, speed and fast evolutions in financial markets;
- Determining Technological Trends

Its recommendations cover:

- Data Security in Highly Distributed Environments;
- Key Countermeasure Applications: IDM, Threat/ Fraud Recognition

Approaches need to be defined, established, broadly understood and recognised by all participants in the broader financial, trade and technical domains.

This should be possible while goals/ objectives of stakeholders are not necessarily convergent or synchronized. It must be for a few underlying concepts but may not be achievable when going into very detailed implementations.

Then semantic interoperability between “silos” which actually exist, or may exist, within the financial sector, within financial markets or infrastructures, or between financial and for example, trade infrastructures, becomes the true challenge.
4.2. Trusted Sharing of Sensitive Information

“Players/actors” in the financial sector need to share information which should not be disclosed to other parties.

From a very broad perspective finance is either an exchange or a transformation business: By exchange we mean the flow of money between players. An example of transformation being; from deposit to credit, from assets to shares to derivatives, from debt to securities. In the transformation business, players need to also share information, in fact, more information than in the exchange business.

In addition, daily or field players tax and supervision authorities, need monitoring or reporting information.

4.2.1. Information sharing in payment

A single payment is a rather simple process, which still has to go across several financial and non-financial systems, and sometimes across currencies, or boundaries. In essence this is already a distributed process.

Trading of securities exhibits all the characteristics of payments applied to a basically two-step process: negotiation and settlement.

In a single payment, five types of information (data) are needed; ID of the payer, routing information to the payee, an amount, delivery and charging parameters, reference data for the payer and the payee. There has been numerous discussion re. the standardization of this information. The key issue in Parsifal is whether any given field or field-value is confidential or not, and whether any given confidential data is to be protected or not against undesirable disclosure, for example,

— are IBAN and BIC confidential?
— is the attachment of a bank domiciliation to the pair IBAN / BIC to be taken as confidential?
— is the fact that payer A intends to pay payee B to be taken as confidential? This means that it is not a specific field that is confidential but the result obtained in correlating two fields;
— is a payment failure confidential?
— is the amount of the payment confidential? Etc.

The answer cannot be yes/no in any situation. Disclosure is relative, relative to the data, relative to the players.

In any case undesirable disclosure cannot be excluded, during the payment itself or during reporting. What measures should be taken, beyond publicity, as required by law in a few US States?

Undesirable disclosure is not the only issue. Diversion is another one. It may impact the destination, the origin or the amount of payment.

4.2.2. Information sharing in factoring or trade credit insurance

In this type of business information issues are more complex. Take for example the role of rating agencies or of credit enhancers and the negative impact they had on the current crisis.
Let us take a simpler example like factoring or trade credit (without securitization). The factor or the trade credit company will need to get accurate information about the actual and foreseen exposure of its customer’s customers. The information needs to be as complete as possible. Little of this information is “white”, more of it is “grey” and hopefully not “black”.

Factors, trade credit companies will look for it as well as information companies, big or very small. Factors or trade credit companies will normally not disclose the information they collected. They will just use it to pay bills, or to guarantee customer credit. This is their decision to be taken as public or not.

What about mistakes? Angry companies brought a few cases of wrong ratings to the courts. Are these beyond or within our scope?

Information agencies have different interest. They have to make a living from information disclosure. Risks may arise from:

- the collection or the calculation process (this takes us back to the subprime crisis);
- inappropriate disclosure (theft of information for whichever use);
- diversion or alteration in support of some kind of fraud.

The key concepts mentioned in section 4.2.1 and 4.2.2 and their relationship are represented in diagram 10.1.
The next diagram 10.2 takes into account key aspects of D2.3, including the developments on:

— human touch points (from the Creation of the information resource to End of life policy) which are regrouped into the vulnerabilities,

— the various tools (to Build Intelligence, to Link and Apply Policies, to Enforce Security) upon which countermeasures could rely.

Redundancies or ambiguities e.g. on Rating or Access control are taken care of, while Global scale (or scalability) appears as a key goal.
Diagram 11.2 – Trusted Sharing of Information (from D2.3)
Data or information classification deserves to be formalized. While the following figure is not an ontology, it could be the starting point for modelling.

**Figure 2 Overview of the data classification process**

Source: ISACA Journal (Appendix 6 of D2.3)
4.3. Business Continuity

For the ECB draft glossary “Business Continuity” consists of “arrangements aimed at ensuring that a system meets agreed service levels even if one or more components of the system fail or if it is affected by an abnormal event.”8 The Microsoft storage glossary defines it as “the ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy.”

This latter concept is actually closer to what experts call “Resilience”.

Business continuity may expand as: business continuity plan or planning, business continuity management, business continuity coordinator, business continuity/disaster recovery, business continuity management program, team or group, business continuity institute, business continuity management policy.

In the financial sector one of the leading authorities has been the Joint Forum, a group of IT Experts from Central banks worldwide, who are focussing on prevention and protection issues in the banking sector [47].

The following diagrams started from an internal document of the Banque de France. This document gathers terms related to this domain and presents them in a structured way. Introducing a new formalism led us first to express the relationships between these terms, as these relationships seldom appear in the original document. This in return could lead to a new structure for the Banque’s glossary.

4.3.1. Top Level View

Dealing with business continuity will lead to activities which can progress along the following steps:

⎯ Scoping,
⎯ Outlining the business continuity strategy,
⎯ Developing a business continuity plan,
⎯ Managing problems etc. when they occur,
⎯ Returning to normal operation after a problem etc.

A parallel description was added in D3.5 Report on State of the art, section 4.3.3. It lists as follows:

⎯ BCM Policy
⎯ Current Situation Assessment
⎯ BIA – Critically – Risk Assessments
⎯ Selection of Business Continuity Strategy
⎯ Contingency Plans (Activation, Recovery/Response and Return)
⎯ Test, Maintenance and Auditing Plans
⎯ Training, Awareness and Communication Plans
⎯ Organizational Model
⎯ Continuous Improvement Tasks.

While BCM policy could be equated to scoping, BCM includes the next steps to the (actual) selection of a BC strategy see section 4.3.2, the rest is included in the the BCP of section 4.3.3. However the models derived from Joint Forum pay more attention to the actual operational

8 The final version (December 2009) defines it as “a state of uninterrupted business operations. This term also refers to all of the organisational, technical and staffing measures employed in order to: 1) ensure the continuation of core business activities in the immediate aftermath of a crisis; and 2) gradually ensure the continued operation of all business activities in the event of sustained and severe disruption”.

PARSIFAL version 2.0 p.33/63
aspects when unfortunate events occur and the practical steps for recovery (not developed in this document) or for crisis management from the premises to stand back (see section 4.3.4). It illustrates that a) even at the surface there is no standard on the description of methods/approaches.; b) completion is not an easy ask. On the positive side there seems to be a consensus one level down, like on the content of:

— a BC policy,
— a BC strategy,
— a BC plan or its declinations.

This may give hints for scoping the definition of standards in this area.

Diagram 12 covers the first step: scoping (policy). Its purpose is to present the “playing field” of business continuity. Most terms used there should now sound familiar to the reader. Most of them are already included in our Glossary.

The diagram shows where the emphasis is to be put: operational risk, i.e. the continuity in case of a major operational disruption.

Here we find the first indication of a business continuity plan and some of its content. The concept of “Physical Infrastructure” remains schematic.
4.3.2. **Outlining a Business Continuity Strategy.**

The next step covers the business continuity strategy. Diagram 12 outlines the content of such a strategy. This version adds two considerations to the diagram of Version 1.0:

The role of a business entity / company cannot be restricted to its economical aspects. A disruption of financial services may have consequences which may go further,

By definition critical infrastructures are those on which vital activities depend. As an afterthought it seems surprising that infrastructure did not appear at this level in the original glossary.

The word “scenario” carries two different meanings: one restricted to how threats could materialize, the other one covering the consequences and the response to a threat scenario. This latter we name “Scenario (II)”. 

This diagram takes the point of view of a business entity, whichever it is. Its generality goes far beyond financial institutions.

Diagram 13 – Concepts for a Business Continuity Strategy

4.3.3. A Model for Planning and Oversight.

What is in a BCP – a business continuity plan and what is the outcome. Diagram 12 provides schematic answers. A more detailed model could be derived from a more complete formalization of the referenced glossary [18]

Legend

Blue circle or ellipse: information (in essence the plan and its subdivisions or variants)
White circle or rounded rectangle: goal (for BC or higher level)
Blue rectangle: process
Orange rounded rectangles: resource/infrastructure.
4.3.4. **A Roadmap to Live Through a Crisis.**

Diagram 14 goes one step further in model sophistication. A key issue for any person in a crisis situation is first to know where they stand, then what to do next. Thus a simple diagram which a person can refer back as the situation evolves may be extremely useful.

In the BDF glossary “status marks” (jalons) were already there, but it was difficult to articulate in terms of the other concepts. The key idea was to introduce the concept of “Crisis Life-Cycle” to identify and to designate every major turn in a crisis, *i.e.*:

<table>
<thead>
<tr>
<th>Status Mark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before crisis</td>
</tr>
<tr>
<td>Emergency Situation</td>
</tr>
<tr>
<td>Crisis Start</td>
</tr>
<tr>
<td>Crisis Height</td>
</tr>
</tbody>
</table>
— Crisis Resumption
— Stand down.

In line with this approach, decision points are also shown with elements that will trigger, or contribute to, a decision, as well as the consequences – actions, communication etc. Other concepts are taken from BCP ontologies.

A detailed “crisis on a page” scheme should be added to the “crisis case” of the Banque’s managers.

Legend

White circle or ellipse: key concept, step and status marks
Blue rectangle: process
Blues ellipses: information
Violet ellipses: events
Orange circle or ellipse: resource/infrastructure.
Diagram 15 – A One-page Roadmap for a Crisis (Simplified)
4.3.5. **SOA/SOI, Dependability, Interdependencies**

In the context of service centric businesses, future competitiveness in the Financial Sector implies new security challenges at the network and application layer. In this section, Critical Financial Infrastructures (CFI) are supposed to include all components and elements (communication infrastructure, but also software, processes, etc). If insufficiently protected against risk, disruption within it, could trigger or transmit further disruptions amongst participants or systemic disruptions in the financial area more widely.

**An Infrastructure model (again)**

The MASTER’s project\(^9\) model, categorizes the computing infrastructure into four layers\(^11\):

1. Communication infrastructure
2. Host infrastructure
3. Middleware infrastructure
4. Service infrastructure

The word ‘service’ in ‘financial services’ is often confused with the same word in ‘service oriented architecture’ (SOA), which may be used to denominate application functionalities (e.g. get payment data) or infrastructure elements (e.g. computing resources) that are provided as a service through Internet or other communications media. In this context service architecture may include:

- Service component
- Software service
- Service Framework:
- Service Description:
- Service Repository:

Typically, architecture for services must be deployed so as to support properties that will be required to enable service-level security.

This “enabling” layer includes traditional basic security technologies such as firewalls for perimeter protection and access control, link-level encryption for confidentiality, or message authentication codes to ensure the integrity of communications.

A current trend in financial institutions is to move towards shared infrastructure services, and with this centralised security operation centres (SOC’s) dealing with network intrusions, threats, security policy enforcement and configuration.

Services also imply a further move to dynamically managed infrastructure. This is perhaps exemplified in models that use virtualization and GRID/utility/cloud computing.

Other changes in the financial industry (as discussed during the workshop in Frankfurt in 2006, include:

- Concentration of many applications on a few technical system platforms

---

\(^9\) The introduction to this section owes largely to ALP position paper on networks and systems.

\(^10\) http://www.master-fp7.eu/

\(^11\) Detailed definitions in the Glossary.
End-to-end requirements for confidentiality, integrity, authenticity and non-repudiation of certain data elements will be end-to-end (from consumer to ultimate service provider).

Distribution, location independency and loose coupling, are new features that will lead to a higher dependability/resilience of web services: Are they really measurable and testable?

**Dependability – Definition & Ontologies**

IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance defines dependability as:

"... the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers."

IEC TC 56 comments:

“The standards provide systematic methods and tools for dependability assessment and management of equipment, services and systems throughout their life cycles.”

Wikipedia adds:

“The wider use of this noun is in Systems engineering... Dependability can be thought of as being composed of three elements:

- **Attributes** - A way to assess the Dependability of a system,
- **Threats** - An understanding of the things that can affect the Dependability of a system,
- **Means** - Ways to increase the Dependability of a system.”

“Attributes” unfortunately bears several meanings which might cause ambiguities in modelling., properties or characteristics would be more appropriate. Threats, Means (Measures) are on our list.

A first list extracted from the Semantical Atlas of CNRS Institute of Knowledge Sciences gives:

<table>
<thead>
<tr>
<th>Cluster 1</th>
<th>Cluster 2</th>
<th>Cluster 3</th>
<th>Cluster 4</th>
<th>Cluster 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>dependability</td>
<td>infallibility</td>
<td>duplicability</td>
<td>trustworthiness</td>
<td>soundness</td>
</tr>
<tr>
<td>reliability</td>
<td>dependableness</td>
<td>reproducibility</td>
<td>responsibility</td>
<td>firmness</td>
</tr>
<tr>
<td></td>
<td>reliableness</td>
<td></td>
<td>responsibleness</td>
<td>solidity</td>
</tr>
</tbody>
</table>

A second listing provides a single word: “permanence”!

Dependability is very much related to the trustworthiness in a sense that allows “reliance to be justifiably placed on the service it delivers” (see IFIP WG10.4 on Dependable Computing and Fault Tolerance). Dependability is also related to availability, reliability and safety of software systems.

The type and level of interdependency among parts of E2E financial process, change over time and the actual status should be continuously monitored during their lifespan, in order to avoid an unwanted and unnoticed increase in the interdependency.

---

12 More definition of dependability can be found in the Glossary (Vol. 2)
Payment services, for example, such as funds transfer, differ considerably across European countries in terms of type, ownership, participants, processing method, settlement system, membership rules, and degree of centralization, pricing and closing time for same day transactions.

For example, some funds transfer systems involve only direct participants, while others include both direct and indirect participants. From the resilience point of view it is also important to stress that currently the most systems are centralized, i.e., one processing centre only.

In his presentation on “Modelling and Transformations- an Engineering View”, András Pataricza (Budapest University of Technology and Economics), states that “Dependability:... is dangerous if users rely on systems without justification of correctness’, which is a typical situation.

Helvik’s ontology [92] is straightforward and simple (see table 2).
**Table 2. Dependability Ontology (After Helvik)**

<table>
<thead>
<tr>
<th>Threats</th>
<th>Faults</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Design Faults</td>
</tr>
<tr>
<td></td>
<td>Physical Faults</td>
</tr>
<tr>
<td></td>
<td>Permanent</td>
</tr>
<tr>
<td></td>
<td>Transient</td>
</tr>
<tr>
<td></td>
<td>Interaction Faults</td>
</tr>
<tr>
<td></td>
<td>Environment</td>
</tr>
<tr>
<td></td>
<td>Detection</td>
</tr>
<tr>
<td></td>
<td>Multiplicity</td>
</tr>
<tr>
<td></td>
<td>Symptoms</td>
</tr>
<tr>
<td></td>
<td>Severities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Attributes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>Reliability</td>
</tr>
<tr>
<td></td>
<td>Reliability Function</td>
</tr>
<tr>
<td></td>
<td>MTFF</td>
</tr>
<tr>
<td></td>
<td>MTTFF</td>
</tr>
<tr>
<td></td>
<td>MTBF – Failure Intensity</td>
</tr>
<tr>
<td></td>
<td>Mean Active Repair Time (MART)</td>
</tr>
<tr>
<td></td>
<td>Mean Automatic Restauration Time</td>
</tr>
<tr>
<td></td>
<td>Safety</td>
</tr>
<tr>
<td></td>
<td>Safety Function</td>
</tr>
<tr>
<td></td>
<td>Catastrophic Failure Intensity</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Fault Prevention</td>
</tr>
<tr>
<td></td>
<td>Quality Assurance</td>
</tr>
<tr>
<td></td>
<td>Derating</td>
</tr>
<tr>
<td></td>
<td>Conservative Design</td>
</tr>
<tr>
<td></td>
<td>Formal Methods</td>
</tr>
<tr>
<td></td>
<td>Fault Tolerance</td>
</tr>
<tr>
<td></td>
<td>Error Detection</td>
</tr>
<tr>
<td></td>
<td>Recovery</td>
</tr>
<tr>
<td></td>
<td>Fault Removal</td>
</tr>
<tr>
<td></td>
<td>Verification</td>
</tr>
<tr>
<td></td>
<td>Diagnosis</td>
</tr>
<tr>
<td></td>
<td>Correction</td>
</tr>
<tr>
<td></td>
<td>Fault Forecasting</td>
</tr>
<tr>
<td></td>
<td>Ordinal Evaluation</td>
</tr>
<tr>
<td></td>
<td>Probabilistic Evaluation</td>
</tr>
</tbody>
</table>

**Dependence (Dependency), Interdependence (Interdependency)**

Wikipedia defines interdependence as “a dynamic of being mutually and physically responsible to, and sharing a common set of principles with, others. “

Commenting: “this concept differs distinctly from "dependence" in that an interdependent relationship implies that all participants are emotionally, economically, ecologically and or morally "interdependent”... Interdependence recognizes the truth in each position and weaves them together. Two states that cooperate with each other are said to be interdependent. It can
also be defined as the interconnectedness and the reliance on one another socially, economically, environmentally and politically.” One could add financially and technically.

These concepts describe relations between players / systems more than intrinsic properties of “objects” while Helvik’s entities (threats and countermeasures) are indeed objects. Helvik model is not a linguistic model. It should be integrated to our models of chapter 3.

One application of ontologies in this field is the formalization of requirements specification, capabilities specification and to Service Level Agreements [10].

Figure 4 – Top Level Structure for Defining Service Level Agreements (from G Dobson et al.)

As the authors of the diagram quote “the useful (and therefore difficult) part is the Expression and the Metric”. They go one step further in [11] aiming at a “shared conceptualisation... to promote consensus on QoS concepts, by providing a model which is generic enough for reuse across domains... (and to facilitate) intercommunication regarding QoS in a heterogeneous environment.
Other examples:

— The ReSIST Ontology [5],

— UMD (Unified Model of Dependability) is another important development in this area.”

See the following figure.
This framework includes major classes in the ‘core’ accreditation and DBSy ontology, major classes in the dependability ontology, and major classes in the trust ontology.

Algirdas Avizienis et al [91] provide representation of dependability tree, failure modes, Elementary fault classes, and combined fault classes.

Bjørne Helvik [92] presents a dependability ontology based on concepts and terms from IFIP WG10.4, approaches to dependable systems, The organization and properties of various network fault handling strategies.

Last but not least the publication of the first report on the security of TCP/IP in February 2009, should be acknowledged.

The latest developments are directly applicable to the finance sector but how far are they relevant? They may be at the same time:

— too detailed because the financial sector needs to concentrate on actual vulnerabilities. For example, in the SWIFT environment they seem to concentrate at both ends of the network (user connection and messaging servers) while the backbone network is taken a highly resilient, or

— insufficient, for example, how could a model predict a country-wide card-application breakdown from a trivial software error like reading a date in the wrong format?

4.4. Conclusion to Chapter 4: Standardization and Interoperability of Ontologies.

Terms and concepts coming from different areas of expertise, or from different areas of concern, may differ slightly and lead to different ontologies. This has been obvious in the healthcare sector for many years is become apparent in the financial sector. This was spotted by the W3C incubator group on disaster management. The consequences on communication between stakeholders may be devastating in a crisis situation.

However the ability to bring together parts of security and financial ontologies should bring some optimism:

it seems that a common (meta)model is within reach. The “who does what” advocated by the W3C could be supplemented by “where, when, why, with”. Subcategories of this model like “what/ supervision” could also be common to several areas,

there are many commonalities between ontologies which presently lay side by side, like those related to security/ finance/ business analysis/ business process management, to risk/ disaster/ crisis management or to business continuity/ interdependencies/ dependability/ resilience.

Bringing together these ontologies cannot be a single team approach. It needs a consensus from several stakeholders groups on detailed issues.

14 Add references to diagrams of chapter 4
5. Conclusion

The primary aim of the models was to share knowledge within the Parsifal project, inside the project team and with representative stakeholders, in other words to deal with semantic gaps. Using such models is not common practice yet. However, it is getting a wider acceptance in technical and business circles. However, it is still difficult to predict what will drive success:

— immediate benefits from maps or “vade mecum” like the one pager on crisis, or
— actual improvements in risk mitigation or crisis management?

It is likely that both will have an impact. Improvements will need to be measured and quantified, thus methods (ontologies) of quantification, starting with “quantistic” risk management, need to be defined, standardized and disseminated.

The models were already instrumental in the gap analysis, from which research directions should emerge, like:

— identifying the role of stakeholders and spotting those who could take the leadership / responsibility of research,
— modelling itself at a degree which could be more comprehensive, evolving, standard and directly usable by the various players.

The attached glossary remains also instrumental. First it is more familiar to most. Second it is actually a part of any ontologies. Our pledge would be to maintain such a glossary beyond the life time of the project and to make it the companion of next versions of the CIIP handbook [32].
6. References

The references are sorted by the following categories:

— Terminology & Ontologies
— Glossaries & Foundation Documents
— CIIP Documents – Europe & USA
— Regulation
— Finance Sector – EU, USA, World
— Supervision
— Information Sharing
— Identity
— Modelling
— Network & Services, Interdependencies, Dependability, Resilience

Terminology & Ontologies


[8] Vuong Xuan Tran, Hidekazu Tsuji (Graduate School of Science and Technology, Tokai University, Japan), Semantics in QoS for Web Services: A Survey, 2008 (?)

[9] Paola Di Maio, Mae Fa Luang University, Chiang Rai, Thailand, AN OPEN ONTOLOGY FOR OPEN SOURCE EMERGENCY RESPONSE SYSTEM, 2007 (?)

15 A European Network of Excellence, 16 Citer en annexe?
Neil Briscombe, Peter Goillau, Tim Sheppard, Graeme Watson (QinetiQ Ltd.), D3C: a coherent, socio-technical framework for identifying, modelling and managing risks in coalition C2, 11TH ICCRTS (International Command and Control Research and Technology Symposium) COALITION COMMAND AND CONTROL IN THE NETWORKED ERA, September 2006,

Glen Dobson, Russell Lock, Ian Sommerville (Computing Department, Lancaster University), QoSOnt: an Ontology for QoS in Service-Centric Systems, 2005 (?)

Glen Dobson, Peter Sawyer Computing Department, Lancaster University, Revisiting Ontology-Based Requirements Engineering in the age of the Semantic Web, 2005 (?)

Christophe Roche, Ontology- A survey, University of Savoie, Equipe Condillac - Campus Scientifique, 2003


FEF supports the conceptual model proposed in Financial Exchange Theory (FET). Financial Exchange Theory provides a basis for the definition of financial entities such as international financial products, financial transactions, financial services and monitoring positions. Financial components, relating to generic functions within international financial markets, are put together following a simple set of rules to create all the above financial entities.


Glossaries & Foundation Documents


European Central Bank (ECB), GLOSSARY OF TERMS RELATED TO PAYMENT, CLEARING AND SETTLEMENT SYSTEMS, Draft for consultation September 2008, December 2009

This glossary presents “definitions of terms as they are used by market participants, not legal definitions. The objective is for the glossary to have a broad, general scope, rather than being system or infrastructure-specific. The use of these terms and definitions may be subject to limitations on account of the diversity of European infrastructure and legal systems”. The ECB also offers an online glossary http://www.ecb.int/home/glossary/html/glossa.en.html which entries may be sorted according to specific ECB, Statistics, Monetary policy, Payments & markets matters.

Antonio De Nicola, Michele Missikoff (Istituto di Analisi dei Sistemi ed Informatica, Consiglio Nazionale delle Ricerche, Roberto Navigli (Dipartimento di Informatica, Universita’ di Roma ‘‘La Sapienza’’), A software engineering approach to ontology building, In Information Systems, Elsevier, April 2009

Vocabulaire du Forum tripartite, vocabulaire de la Banque de France relatifs à la continuité d’activité , Lexiques structurés, Version 1, June 2008

Khaled M. Khalil, M. Abdel-Aziz, Taymour T. Nazmy & Abdel-Badeeh M. Salem (Faculty of Computer and Information Science, Ain Shams University Cairo), THE ROLE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN CRISIS RESPONSE, 2008 (?)

17 Voir def of accountability?
[23] European System of Central Banks (ESCB)\textsuperscript{18}, or definitions of major business continuity terms in relation to payment and securities settlement systems, June 2007

[24] Institut d’Etudes et de Recherche pour la Sécurité des Entreprises (IERSE), ANALYSE ET GESTION DES RISQUES DANS LES GRANDES ENTREPRISES, Impacts et rôle pour la DSI, Club informatique des grandes entreprises françaises (CIGREF), 2007

[25] Committee on Payment and Settlement Systems (CPSS), Bank for International Settlements (BIS), A glossary of terms used in payments and settlement systems, March 2003


[29] Comité consultatif du secteur financier (CCSF), Glossaire des opérations bancaires courantes, September 2005


[31] The Paper proposes a way for work to be carried out by the CPC in this field, and contains a road map detailing immediate to long-term actions, a scenario to further explain the concept and a glossary of frequently-used CIP terms.


**CIP Documents – Europe & USA**


\textsuperscript{18} The ESCB comprises the ECB and the national central banks (NCBs) of all EU Member States whether they have adopted the euro or not.

\textsuperscript{19} Voir la def de CI ou CII
Policy options on how the Commission could establish EPCIP. In all these documents, European dimension has been clearly identified, both regarding the weaknesses …vulnerabilities… integrated EU-wide approach … complement and add value to the national programmes re critical infrastructures.


European Commission, Communication on Critical Infrastructure Protection in the Fight against Terrorism, 20 October 2004

Suggestions on what would enhance European prevention, preparedness and response to terrorist attacks involving critical Infrastructures (CI).

Regulation

COUNCIL DIRECTIVE 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, 8 December 2008 [CIP Dir].


European eInvoicing Directive,

The authenticity of the origin and the integrity of the information need to be guaranteed until the financial transaction is finalized and duly recorded.


on the taking up, pursuit of and prudential supervision of the business of electronic money institutions

Deliverable 2.1 – DraftOntology Of Financial Risks & Dependencies Within & Outside The Financial Sector

[54] on Settlement Finality.

Finance Sector – EU, USA, World

[55] Yvon Lucas (Editor-in-Chief), Oversight of Means of Payment and Transfer systems, Banque de France (Eurosystème), December 2006 [BDF 2006]

[56] Joint Forum of the Basel Committee on Banking Supervision, the International Organization of Securities Commissions and the International Association of Insurance Supervisors, the Bank of International Settlement (BIS), High-level principles for business continuity, August 2006


[60] building on previous papers that identified e-security as a key component to the delivery of e-finance services. This paper and its technical annexes identify and discuss eight key pillars for secure financial infrastructures

[61] Oversight standards for euro retail payment systems adopted in June 2003 by the governing Council of the European Central Bank (ECB)


Supervision

[64] Bruno DELETRÉ ( Inspection générale des Finances, RAPPORT DE LA MISSION DE REFLEXION ET DE PROPOSITIONS SUR L’ORGANISATION ET LE FONCTIONNEMENT DE LA SUPERVISION DES ACTIVITES FINANCIERES EN FRANCE, January 2009

[65] This report includes appendices comparing the organization of supervisory activities in France Germany, Spain, the Netherlands and UK

Information Sharing


[67] This deliverable summarizes the updates performed during 2006 in the Knowledge Web portal and provides different statistics such as content and access statistics.

[68] Tamer E. El-Diraby (University of Toronto), A SEMANTIC COLLABORATIVE PORTAL FOR THE EXCHANGE OF INFRASTRUCTURE INTERDEPENDENCIES INFORMATION, 2005 (?)

Identity

[70] Jim Rapoza, Predictable insecurity, ‘rfid-tagged credit cards and devices can be read and cloned from a distance.’ No one should be surprised at the problems surrounding RFID, eWeek November 2009

[71] Giles Hogben, Privacy, Security and Identity in the Cloud, ENISA, July 2009


[74] National Institute of Standards and Technology (NIST) Special Publication 800-73, Interfaces for Personal Identity Verification, May 2009

[75] Specifies the interface and data elements of the PIV card

[76] NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification

[77] Specifies the technical acquisition and formatting requirements for biometric data of the PIV system

[78] NIST Special Publication 800-78, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification

[79] Specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

[80] Matthew Rowe (The OAK Group, Department of Computer Science, University of Sheffield), Mapping between Digital Identity Ontologies through SISM, 2009


[85] This post includes interesting considerations on identity ontologies.

[86] Personal Identity Verification (PIV) of Federal Employees and Contractors, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION FIPS PUB 201-1, Computer Security

20 Voir commentaire de SWIFT sur Authorization à propos du glossaire de la BCE.

Business & Technical Requirements for Identity Management in an Interoperable & Electronic Environment, Jan 2007


William MacGregor, William Dutcher, Jamil Khant An Ontology of Identity Credentials Part 1: Background and Formulation, NIST Special Publication 800-103 Draft, October 2006

Liberty Alliance Glossary: Identity Theft Primer, December 5, 2005


A blog attempting at capturing observations of the on-going evolution of digital identity.


“Bridging and harmonizing the identity community with actions that will help ensure secure, identity-based, online interactions while preventing misuse of personal information so that networks will become privacy protecting and more natively trustworthy environments.”

**Modelling**


**Network & Services, Interdependencies, Dependability, Resilience**


FIX Protocol Ltd, Financial Information eXchange (FIX) Protocol

A messaging standard developed specifically for the real-time electronic exchange of securities transactions. FIX is a public-domain specification.

---

22 Restricted to Parsifal Team
Denis Beau (chairman of the CPSS working group on system interdependencies) The interdependencies of payment and settlement systems, Joint Banque de France / European Central Bank conference on "Liquidity in interdependent transfer systems" Paris, 9-10 June 2008 [ECB 2008]


... requirements and drivers including service oriented architectures, high mobility requirements for uninterrupted geographical coverage and high degree of interdependencies, which are national, trans-national and international.

In addition to this, it was deemed necessary that the implementation of the CIIP framework would be supported by collaboration of all the relevant players in the design, set-up, testing and maintenance of the framework.

David Barroso (S21sec, Spain), Botnets – The Silent Threat, ENISA Position Paper No. 3, November 2007


IST FP6 ESFORS12 project, Joint Workshop on Software and Services Development, Security & Dependability13, September 2006,


Algirdas Avizienis UCLA Computer Science Dept, Jean-Claude Laprie, LAAS-CNRS, Toulouse, Brian Randell Dept. of Computing Science, Univ. of Newcastle upon Tyne, Fundamental Concepts of Dependability, April 2001

Bjárne E. Helvik (Norwegian University of Science and Technology), Perspectives on the dependability of networks, and services, Telektronik, March 2004
Appendix A. Ontologies of Security – Citations & Further References

Extracted from [4].
Any Kim, Jim Luo, Myong Kang, Security Ontology for Annotating Resources, 4th International Conference on Ontologies, Databases, and Applications of Semantics (ODBASE’05). 2005
A short description of a network of subontologies

The citation includes the following diagram, which is close from ours.
Appendix B. Appendix B Diagrams from The EIIF XG Aug 2009 Report

Figure A.1 Conceptual Mind Map
Figure A.2 Phased Framework Model (see [Hackman, 2007], [Roper, 1998])

Figure A.3 Orchestra Framework Example (see EU-funded ORCHESTRA Project) (See. ISDR vocabulary and UNISDR Terminology)
Figure A.4 Tactical Situation Object Model in Open Advanced System for dISaster

Figure A.5 OGC Feature Model - Open Geospatial Consortium (OGC) standards for spatial objects and relations in support of the Framework Concepts and to harmonize these as needed.
Figure A.6 W3 Coordination Use Case Information Model based on data schemas from two existing emergency information systems, OCHA and Sahana.
Figure A.7 W3 Coordination concepts framed under DOLCE-Lite Conceptualization