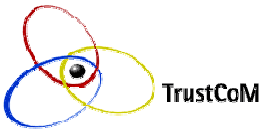

Deliverable

15

Report on Legal Issues Appendix A

Legal Risk Analysis with respect to IPR in the CE Scenario

WP9 Legal Issues

Fredrik Vraalsen, Sintef

Tobias Mahler, NRCCL (eds.)

31/7/2005

Version 1.0

TrustCoM

A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.9

Prepared for the European Commission under FP6 Contract No. 01945 as a deliverable form

Deliverable datasheet D 15 Appendix A

Project acronym: TrustCoM

Project full title: *A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations*

Action Line:	**6**
Activity:	**6.2**
Work Package:	**9**
Task:	**6.2.2**

Document title:	D 15 Report on Legal Issues Appendix A
Version:	1.0
Document reference:	N/A
Official delivery date:	31 July 2005
Actual publication date:	N/A
File name:	
Type of document:	Report
Nature:	Public

Authors:	Dana Irina Cojocarasu[1], Mass Soldal Lund[2], Tobias Mahler[2], Xavier Parent[3], Ketil Stølen[2], Fredrik Vraalsen[2]
Reviewers:	CCLRC, Heather Weaver and Judy Beck
Approved by:	

[1] NRCCL

[2] SINTEF

[3] KCL

Version	Date	Sections Affected
1.0	31.07.2005	Based on work included in TrustCoM internal deliverable ID6.2.2

Table of Content

1 Introduction

This appendix to ID6.2.2 documents the results from the risk analysis of legal issues related to Intellectual Property Rights (IPR) in the TrustCoM Collaborative Engineering scenario.[4]

The analysis is based on the CORAS model-based risk analysis methods and tools.[5] The CORAS risk analysis process is divided into the following 5 sub-processes:

- Context Identification
- Risk Identification
- Consequence and Frequency Analysis
- Risk Evaluation
- Risk Treatment

The results from each sub-process are detailed in the following chapters.

[4] TrustCoM Internal Report ID 2.2.1, Requirements for the Collaborative Engineering Test Bed, dated 9th September 2004, Version 2 Draft D.

[5] Folker den Braber, Theo Dimitrakos, Bjørn Axel Gran, Mass Soldal Lund, Ketil Stølen, Jan Øyvind Aagedal. The CORAS methodology: model-based risk management using UML and UP. Chapter in book titled UML and the Unified Process. Liliana Favre (ed), pages 332-357, IRM Press, 2003.

2 Context Description

The main goals of the context identification sub-process are:

- Identify areas of relevance:
  - Risk management context
  - Target of evaluation
  - Organisational context
  - SWOT analysis
  - System description
- Identify and value assets
- Identify (security) policies and risk evaluation criteria
- Approval of risk analysis background documentation

2.1 Risk Management Context

The goal of the risk analysis documented in this report was to analyse legal risks related to IPR in the TrustCoM Collaborative Engineering (CE) scenario. This work was performed as part of the TrustCoM WP9 – Legal Issues – for internal deliverable ID6.2.2.

The activity plan for the risk analysis is listed in Table 1.

Date	Task Type	Participating Roles
18 November 2004	Target identification, asset identification, threat identification	Vraalsen, Lund, Mahler
29 November 2004	Target identification, asset identification, threat identification	Vraalsen, Lund, Mahler
11 January 2005	Threat identification, asset identification	Vraalsen, Lund, Mahler
27 January 2005	Approval	Vraalsen, Mahler, Lund, Parent, Golby, Keser
28 January 2005	Threat identification cleanup/identification of unwanted incidents	Vraalsen, Mahler, Lund, Parent
28 January 2005	Frequency and consequence identification	Vraalsen, Mahler, Lund, Parent, Golby, Keser
28 January 2005	Treatment identification	Vraalsen, Mahler, Lund, Parent, Golby, Keser
2 February 2005	Cleanup of results	Vraalsen, Lund
3 February 2005	Cleanup of results	Vraalsen, Mahler

Table 1 Assessment plan

Due to the lack of historical or statistical background data, we chose to use qualitative rather than quantitative values for risk consequences and frequencies. The value categories used for consequences and frequencies and their interpretations are shown in Table 2 and Table 3. Frequency probability values are defined based on the chance of occurring within a single design project.

Consequence Value	Description
Insignificant	No impact on business. Minor delays.
Minor	Loss of profits. Lost project phases.
Moderate	Loss of project/client.
Major	Loss of business sector. Close department.
Catastrophic	Out of business.

Table 2 Consequence value definitions

Frequency Value	Description (probability)
Rare	Less than once per ten years (0.00 – 0.01)
Unlikely	Less than once a year (0.01 – 0.05)
Possible	About once a year (0.05 – 0.20)
Likely	2-5 times per year (0.20 – 0.50)
Certain	More than 5 times per year (0.50 – 1.00)

Table 3 Frequency value definitions

The risk matrix in Table 4 shows how to map the frequency and consequence values to risk values.

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Frequency	Rare	Low	Low	Low	Moderate	Major
	Unlikely	Low	Low	Moderate	Major	Major
	Possible	Low	Moderate	Major	Major	Extreme
	Likely	Moderate	Major	Major	Extreme	Extreme
	Certain	Moderate	Major	Extreme	Extreme	Extreme

Table 4 Risk matrix

Table 5 defines the main roles of the participants of the risk analysis. The main part of the risk analysis work was performed by the WP9 partners from SINTEF, NRCCL and KCL. BAE Systems was the author of the scenario under analysis and played the role of the target owner during the risk analysis sessions. To facilitate integration of the socio-economic and legal strands of TrustCoM AL6, IBM also participated in the risk analysis in the capacity of being experts on the socio-economic aspects.

Role	Name	Organisation	Background/Expertise
RA leader	Fredrik Vraalsen	SINTEF	Risk analysis
RA secretary	Mass Soldal Lund	SINTEF	Risk analysis, security
Target owner	Dave Golby	BAE	Aerospace industry
Field expert	Tobias Mahler	NRCCL	Law
Field expert	Claudia Keser	IBM	Socio-economic
Observer	Xavier Parent	KCL	Logic

Table 5 Assessment roles

2.2 Target of Evaluation

The target of evaluation for this analysis is the System Integrator (SI) partner of the Collaborative Engineering Virtual Organisation (CE VO). This actor is responsible for integrating the various aircraft subsystem components into a complete aircraft design.

The focus of the legal analysis during this phase of the TrustCoM project was on Intellectual Property Rights (IPR), so it was decided to restrict the risk analysis to IPR issues. More specifically, the focus would be on trade secrets, refining the following risks identified on page 77 of ID2.2.1:

- Loss of intellectual property such as product design data to competitors by 'leakage', the unintended disclosure of data within a collaboration possibly via intermediaries
- Industrial espionage - competitors accessing company intellectual property by illicit means.

We assume in this analysis that the CE VO is already formed and operational. Furthermore, we assume that the in-flight entertainment systems provider has already been included as a member of the CE VO.

The analysis focuses on the agreements that need to be created during the formation of the larger VO shown in Figure 1. These agreements control the activities and information flow during the operation and dissolution phases, and we focus in our analysis on legal risks and treatments during the operational phase. We have decided to categorise contracts/agreements as risk treatments rather than assets.

The restrictions on the target of evaluation are listed in Table 6.

Task ID	Restriction	Description
Target of evaluation	IPR	Focus on IPR
Target of Evaluation	Focus on SI of CE VO	I.e. Airframe Ltd.
Target of evaluation	CE VO already extended	Entertainment system provider, MyInterLink Ltd., is already integrated in the VO
Threat identification	Leakage, industrial espionage	Main focus of threat identification
Target of Evaluation	Assume Airframe Ltd. Is responsible for system integration	Fitting to the scenario
Target of Evaluation	Assume product design is co-owned	
Target of Evaluation	Assume intention to upgrade aircraft design with entertainment system is already public knowledge	

Table 6 Assessment restrictions

2.3 Organisational context

The organisational context described in this section is based on TrustCoM internal Report ID2.2.1, page 23. The TrustCoM Collaborative Engineering scenario contains three VOs:

- An airliner VO (AirVO) consisting of the carrier, support and maintenance teams;
- A Collaborative Engineering VO (CE VO) which has the technical expertise to support the specification and integration of systems into complex products, and which may take the decision to manufacture the solution for the customer;
- A number of engineering analysis consultancies that form a VO to support design activities within engineering companies. The Analysis VO (AVO) supports general analysis work across engineering and scientific sectors. In this scenario two teams for CFD and CEM work together to analyse the design.

Figure 1 depicts the actors and their relationships within the test bed. The storage provider exists outside these VOs: its status is that of an ‘external supplier’ who connects with these and other VOs (possibly facilitating collaborative working). Its business model is one of deriving revenue by supplying services to many diverse

companies and not being aligned strategically with any particular VO or other organisation that is relevant to the CE sector.

The CE VO is a consortium of aerospace companies with a new member (3). It includes teams of designers working on various parts of the airliner, and consists of the following partners:

1. System integrator (Airframe Ltd.)
2. Avionics manufacturer (MyAvio Ltd.)
3. In-flight entertainment system provider (MyInterlink Ltd.)

The business goal of the CE VO is to win a contract with a major airline to upgrade its fleet with an in-flight entertainment system. This involves demonstrating to the customer, by using predictions of in-service performance, a design that can meet the customer's requirements.

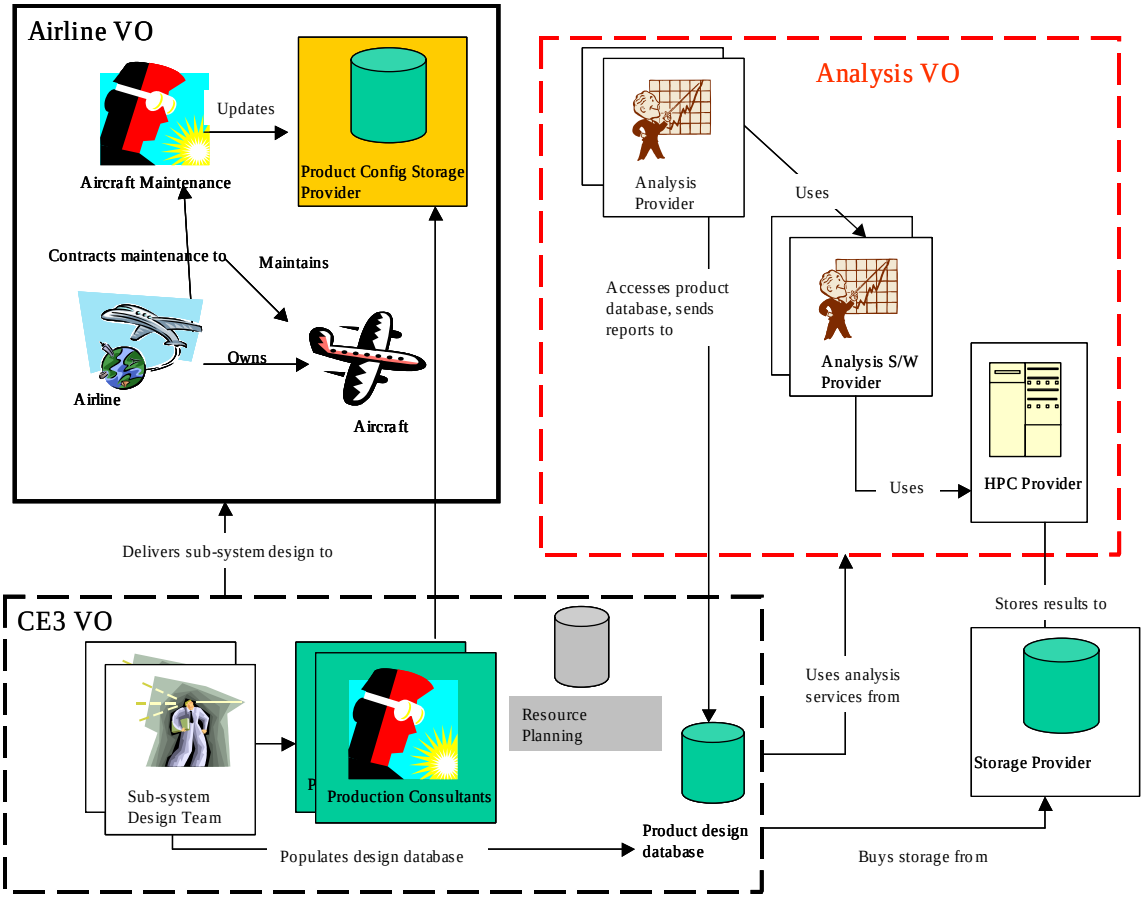

Figure 1 Virtual Organisations within the CE testbed

2.4 Stakeholders

A stakeholder is a person or organisation which has interest in the target that is being assessed. This analysis is performed on behalf of the system integrator (SI), and SI is the only stakeholder. Table 7 contains the stakeholder information.

Stakeholder ID	Stakeholder Role	Stakeholder Name	Description
SI	System Integrator	Airframe Ltd.	System integrator in the CE VO - a consortium of aerospace companies with a new member (in-flight entertainment systems provider). Responsible for integration of the various subsystem designs into a complete aircraft design.

Table 7 Stakeholder Table

2.5 System description

This section describes the analyzed system.

Figure 2 shows a high-level overview of the various VOs and the information access patterns involved in this scenario. This does not go into any detail on "ownership"[6] of the information – as we assume the VOs themselves are not legal entities they cannot own anything, the information has to be owned by one or more of the VO partners.[7]

[6] Since information is only conferred a partial and rather limited legal protection, the use of the term "ownership" should not be understood as referring to a full ownership like it is possible with material goods. The person entitled to a particular IPR may also be referred to as a rights-holder. Hence, the term ownership in this report refers to the position of the rights-holder.

[7] However, the VO members may be considered as collectively responsible in some jurisdictions. This will be the subject of future work of the TrustCoM WP 9.

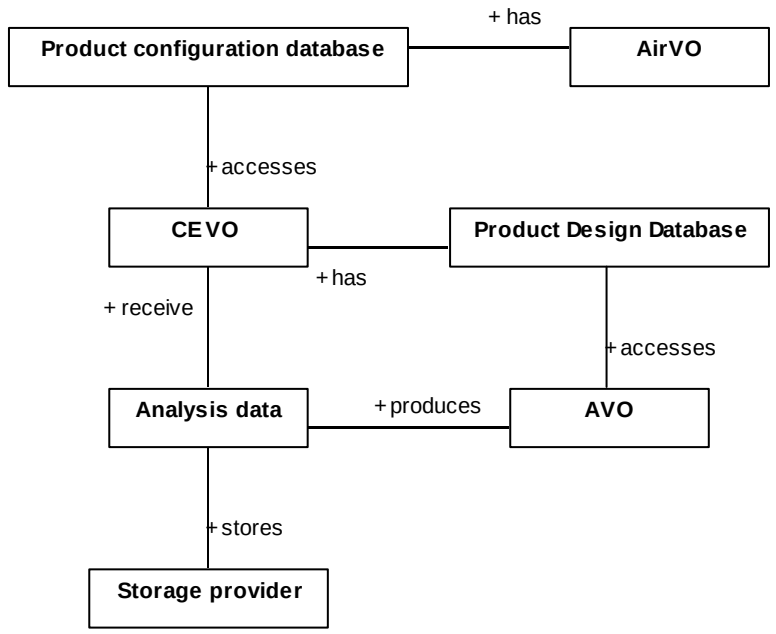

Figure 2 High-level view of VOs and information access

Ownership is however very important from a legal perspective. The owner of the information generally has all rights to the use of that information, but may transfer those rights to others in various forms of limited rights, e.g. the right to read or distribute.

Figure 3 goes into more detail on the CE VO and the relevant IP, i.e. product designs, including ownership relationships. Partners in the CE VO are the systems integrator the sub-system design teams and the in-flight entertainment system provider (see section 2.3). Each partner has a database containing their product designs.

We assume that each sub-system designer owns the designs of their subsystem. Furthermore, we assume that the integrated design is special, in that it is co-owned by all the partners of the VO but produced by the systems integrator.[8]

[8] We assume a rule with this content was included in the VO agreement which governed the original design of the airplane. However, in practice there will not be one right to the integrated design, but a number of different IPR rights, including copyrights, patents, design rights etc. See further below section 2.6.1.

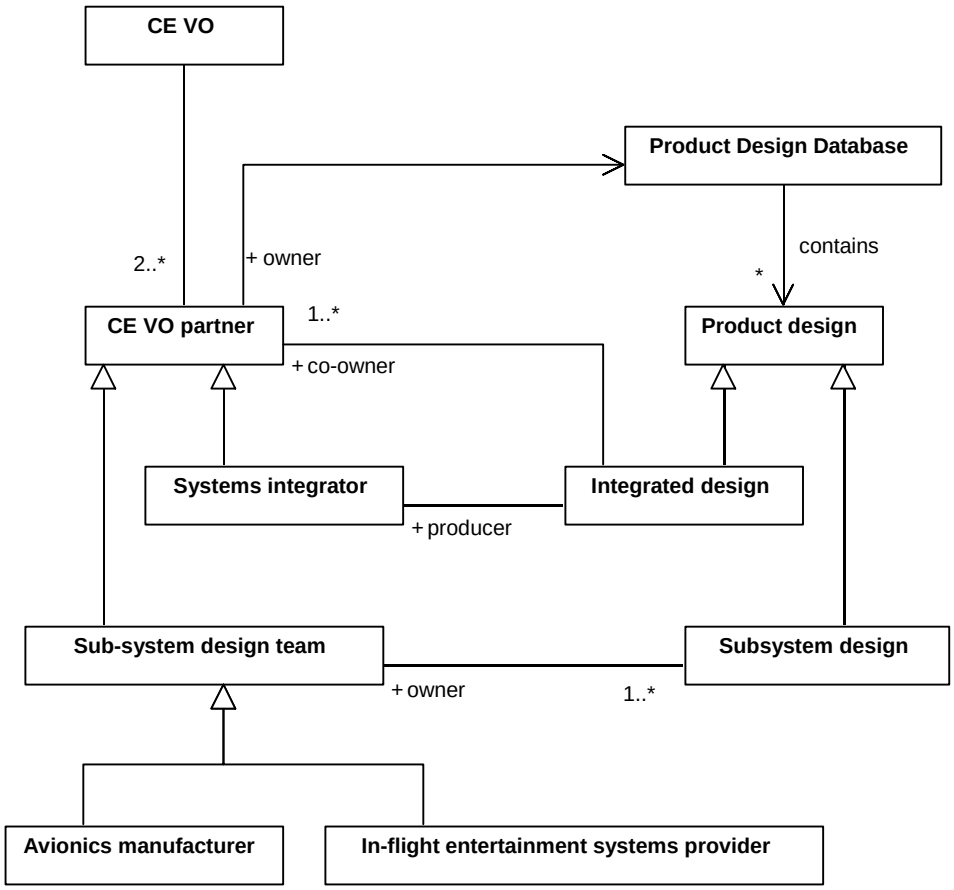

Figure 3 CE VO partners and IP

Figure 4 attempts to illustrate how a partner of one of the VO(s) may be involved with a competitor of the system integrator, possibly through intermediaries (a 'chain' of business partners). This relates to the first risk listed above, disclosure of information to competitors through 'leakage'[9].

[9] It is not relevant at this point of the analysis to refer also to the second risk listed above (industrial espionage) since we're describing the interactions within the business system, focusing most on the consequences of possible business relations between the VO members and third parties, and not on possible unauthorised and unlawful intrusions in their communication systems

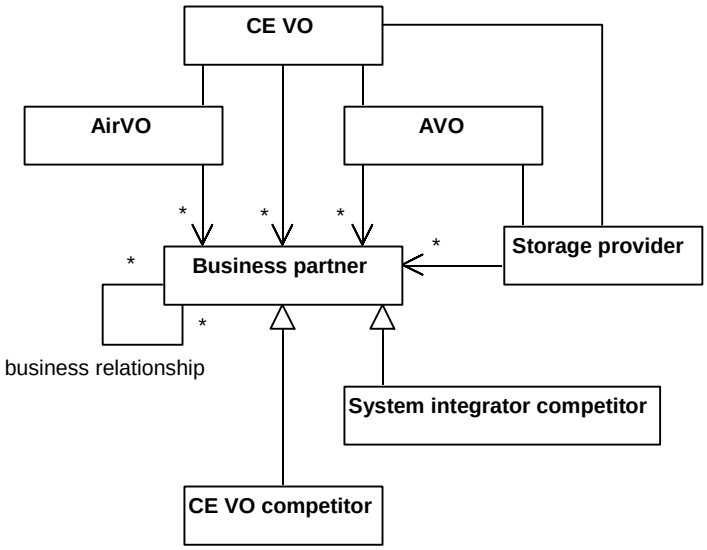

Figure 4 Relation to competitor of system integrator and CE VO

The following figures show various use cases which involve flow of intellectual property (IP) between the systems integrator and 1) other partners in the CE VO, 2) the AirVO, and 3) the AVO and via this to the HPC provider and storage provider. The CE VO acts as an intermediary in the indirect flow of IP from the AirVO to the AVO, e.g. product configuration data.

Figure 5 shows a model of the activities related to requirements negotiations between the CE VO and AirVO.

Similarly, Figure 6 shows a model of the contract negotiations between the CE VO and the AVO. An important part missing from this model is the legal risk analysis performed by the CE VO during the creation of the contract (it is only shown for the AVO). An alternative partial model of the process incorporating legal risk analysis is shown in Figure 7.

Figure 8 shows and overview of the design process, which involves flow of IP between the various partners in the CE VO as well as to the AVO (and via this to third parties). This raises confidentiality issues when a designer accesses the Product Design Database (PDD) of another partner in the CE VO.

The question of how access rights to the PDDs are administered is not covered in ID2.2.1. This relates to power and permission – who has the power to assign permissions to others? Can this power be delegated, and if so, by whom? How is the power shared within the VO, e.g. does a single VO partner represent the others in contract negotiation/agreement? How is access to the PDD limited (e.g. to only this project)?

We assume that the CE VO partners have established long-term relations and are not themselves competitors. This may not be the case for the new partner (in-flight entertainment system provider) however. The process of adding or removing

partners is not described in detail in the scenario. Furthermore, do partners cooperate with competitors of the system integrator in other projects?

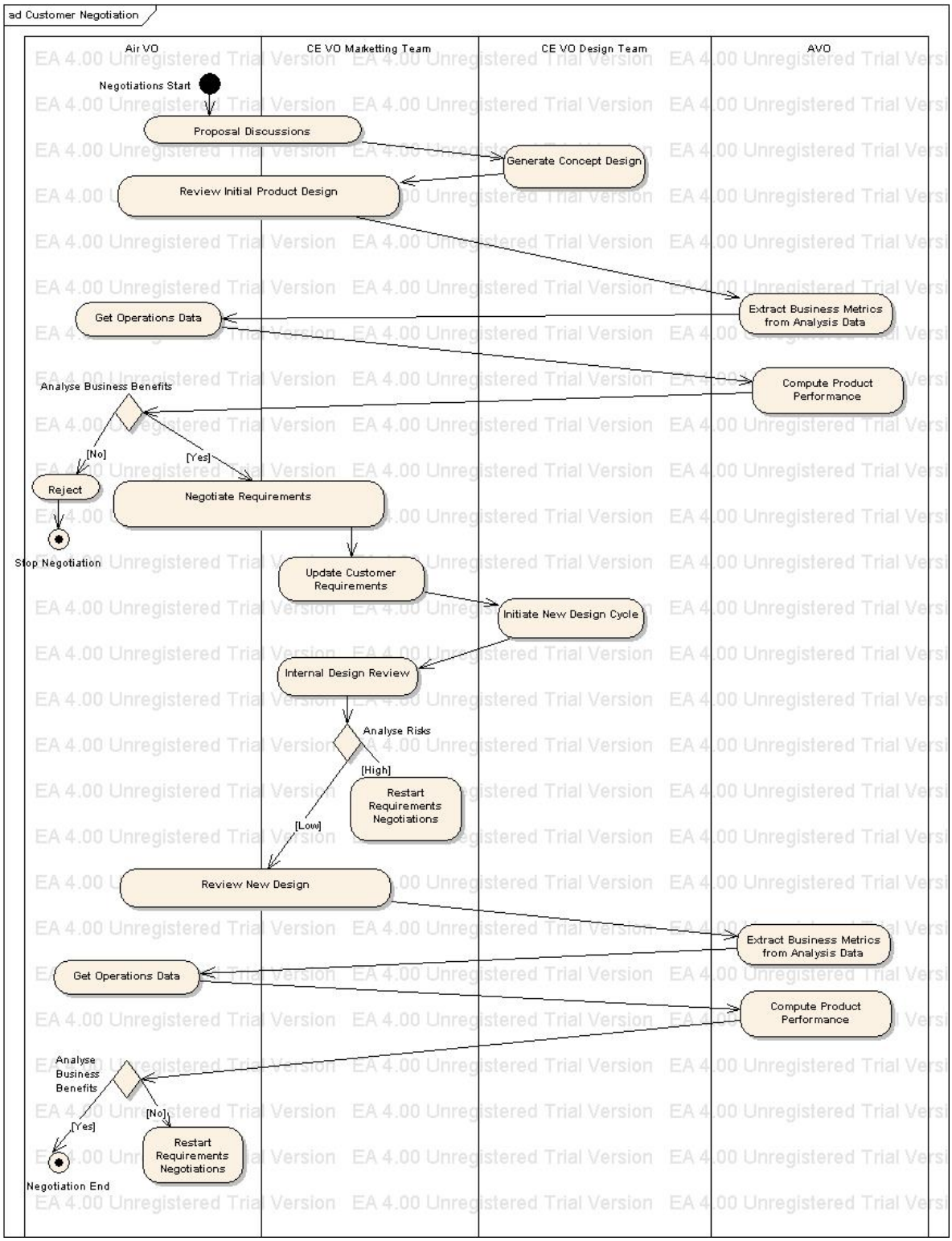

Figure 5 Customer Requirements Negotiations with AirVO

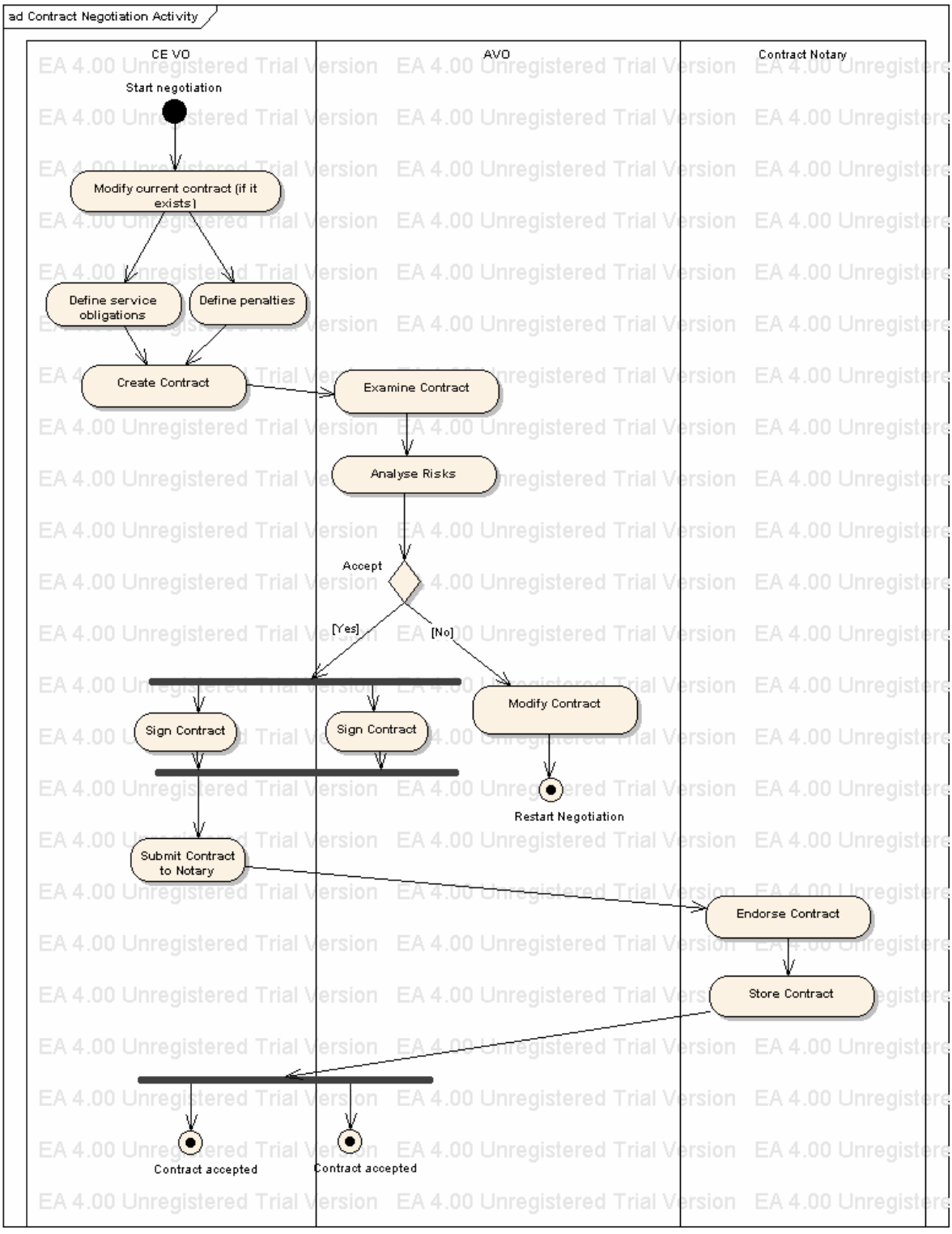

Figure 6 CE VO and AVO negotiations

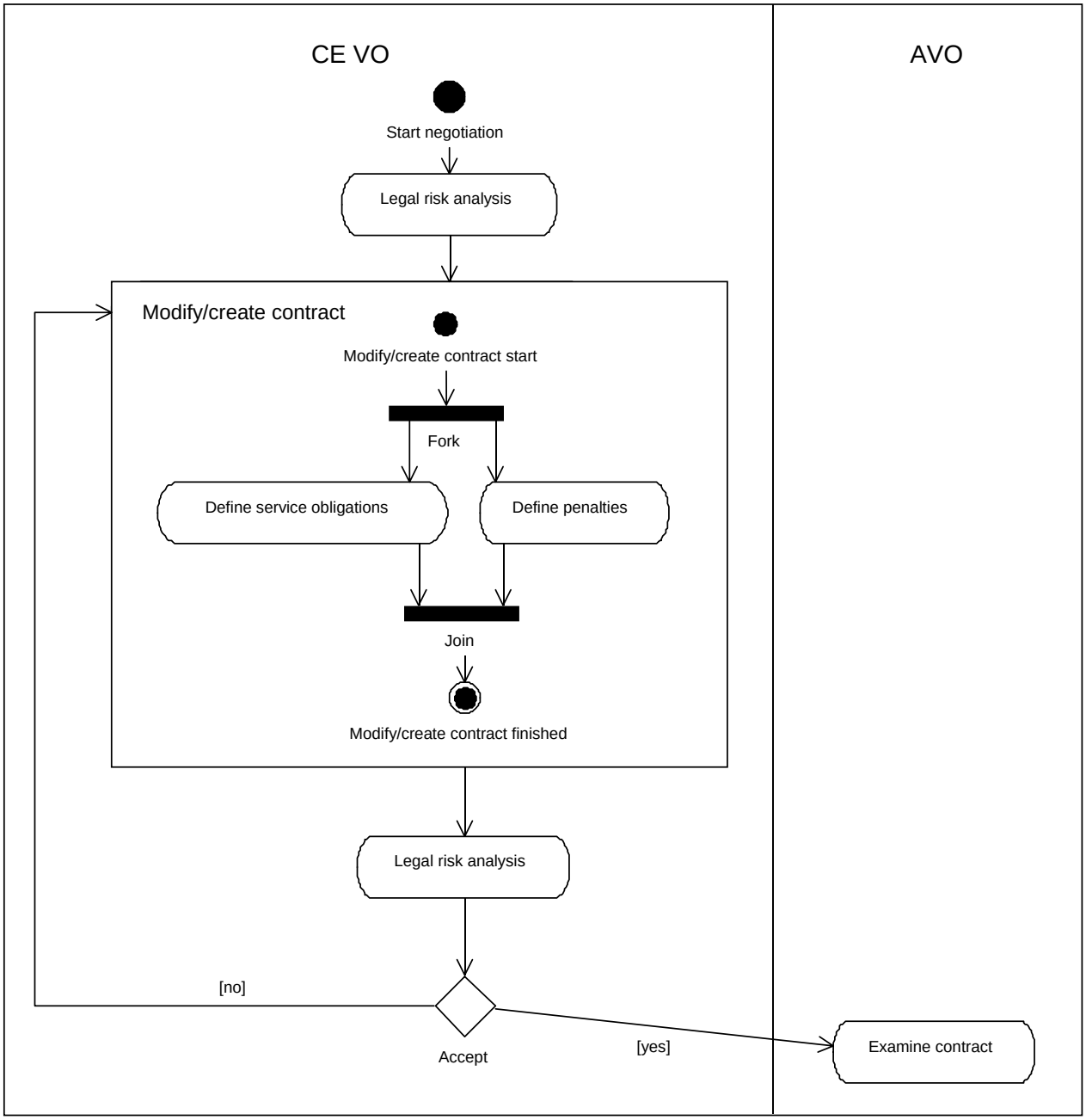

Figure 7 Alternative start of contract negotiation process

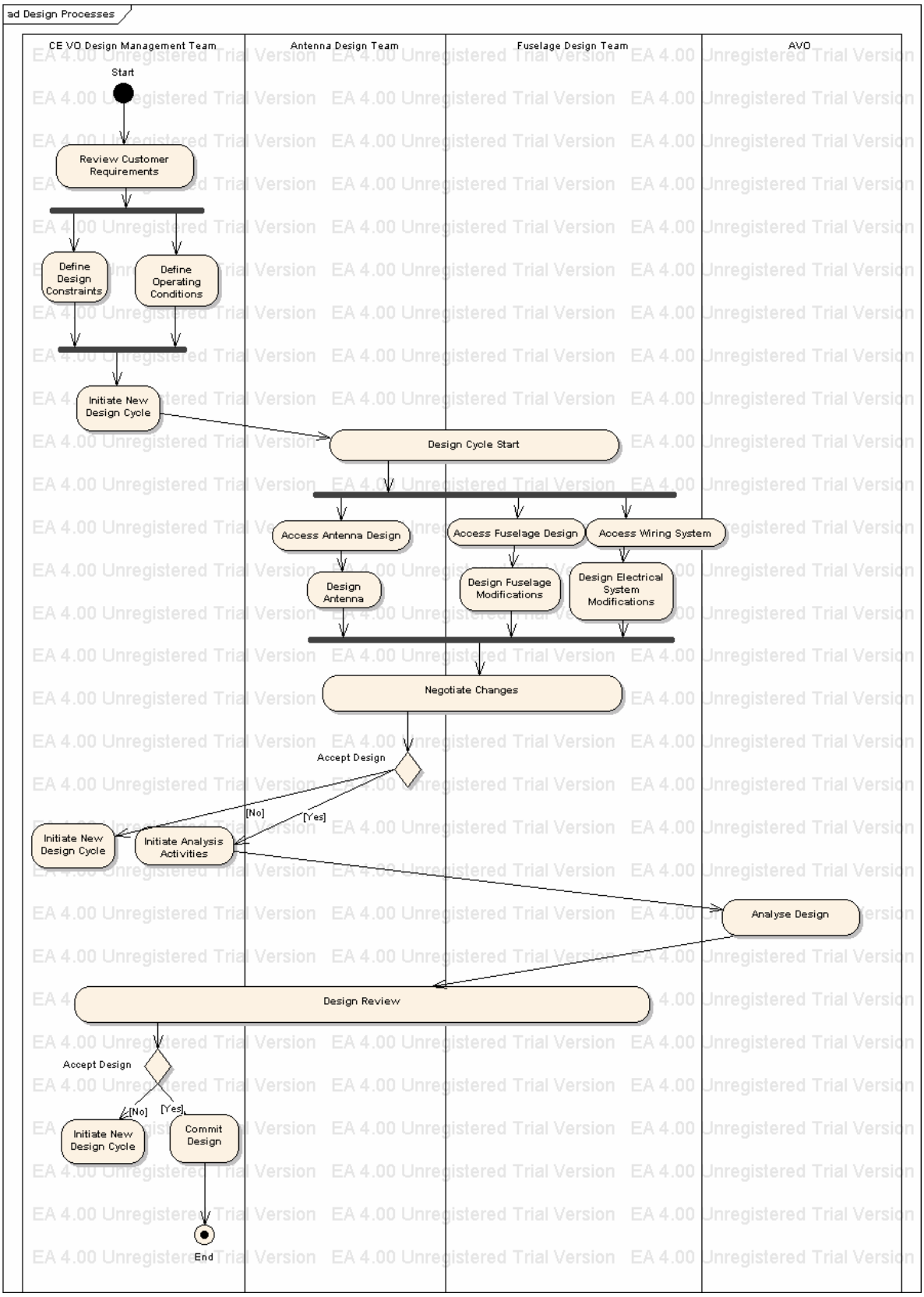

Figure 8 Design Process

2.5.1 Contracts in the CE scenario

It can be assumed that a number of different contracts will govern the internal and external relations in the CE scenario. These will most probably include at least three types of contracts:

- Consortium agreements, which establish a consortium of organizations with a common goal. In the TrustCoM conceptual models, this type of contract is referred to as the legal level of General VO Agreements (GVOA)[10].
- Services or goods related contracts, which govern the provision of services or the purchase of goods without establishing a consortium. [11]
- Service Level Agreements (SLAs), i.e. (electronic) contracts that deal with the specific rules that partners in an operational business process are bound to. These can be included in, or related to, both consortium agreements and services related contracts.

2.5.1.1 CE VO General VO Agreement

Since the CE VO has existed for a longer time, the partners will most probably have established a contract to govern the internal relations between the CE VO partners.[12] The required content of the contract will to a large extent depend on rules and traditions in the chosen jurisdiction and applicable national law. This contract could e.g. consist of the following elements illustrated in Table 8:[13]

Table 8 Possible content of a General VO Agreement (GVOA)

Definitions	Definition of terms used in the GVOA
Agreements	Relation between the GOVA and other agreements among VO members (i.e. the GVOA supersedes and prevails)
Steering Committee	Rules for and role of the steering committee/other committees
Exclusivity	Exclusivity regarding the scope and object of the co-operation
Subcontracting	Subcontracting to third parties (is it allowed?)
Confidentiality	Limiting disclosure and/or use of information disclosed as confidential
Ownership IPR	Ownership of knowledge and IPR
Access Rights	Access to knowledge which is necessary to carry out the

[10] Cf. TrustCoM D 16, Conceptual Models, Section on Contracts and Service Level Agreements.

[11] This type of external contractual relation between the VO and third parties does not seem to be covered in the TrustCoM conceptual model so far.

[12] The VO may even have been set up by establishing a legal entity, e.g. a limited company.

[13] Amended from ALIVE IST Project *VE Model Contracts, Deliverable D 17a* (2002). This contract template seems to be based on English law, where contracts tend to be rather detailed. In other countries, some of the clauses would probably not be included in the contract, since many of the addressed issues already are solved similarly in statutory law.

	project
Liability	E.g. each party is liable to the extent of this party's fault
3rd Party Claims	Handling of third party claims
Insurance	Insurance issues regarding the operation of the VO
Costs & Revenues	E.g. each party bears its own costs, revenues are divided in proportion to the contribution of a party, to be decided by Steering Committee ex ante
Dispute Settlement	E.g. mediation, arbitration, court settlement
Governing Law & Jurisdiction	Defines the governing law and jurisdiction (e.g. English law and exclusive jurisdiction of the English courts)
VO Lifecycle and Termination	Duration and termination of the VO, including • Start and end date • Rules for decisions about expulsion of a party, both procedural and material aspects • Right to terminate the agreement • Effects of termination e.g.: • How to treat other parties' information (e.g. destroy) • Continued confidentiality obligation • Continuation of obligations undertaken during VO lifetime
Amendments	Rules about amending the agreement (e.g. in writing)
"Boilerplate clauses"	These are standard clauses included in most contracts. E.g. the "no partnership" clause makes it clear that the parties are not intending to create a different type of legal relationship such as a partnership. However, the importance of such boilerplate clauses depends on the law governing the agreement. Examples include: • no agency • headings in agreement only for convenience • no waiver (a delay in enforcing a right is not to be understood as a waiver)
"*Force Majeure*"	Effect of "*force majeure",* i.e. circumstances beyond the control of a party, like war, flood, power shortage etc.
Severability	Rule for a situation in which a provision of the agreement is held invalid or unenforceable.
Notice	How do contractual or other notices have to be communicated, e.g. by email or registered post.
Communication and data exchange	E.g. valid and enforceable obligations may be created by a specified use of communication and data exchange. This rule links the GVOA to SLAs and other electronic contracts.

As mentioned above, the CE VO General VO Agreement will cover a number of IPR issues, including ownership, maintenance and sharing of IPR.

- Ownership: The CE VO seems to be a more stable group of enterprises, who have been co-operating for a long time and who will continue to co-operate for a considerable time into the future. The design, construction and maintenance of an aircraft (or its update) involve a long-term commitment and responsibility. Consequently the IPR created during the upgrade of the aircraft with an in-flight entertainment system should be owned by all VO members collectively, unless it is created independently by just one of the VO partners.
- Maintenance: If the *project IPR* is held by all of its members collectively, as is the case for the CE VO, the GVOA should specify the responsibility for maintenance and protection, and how the related costs should be shared.
- Sharing: With respect to the CE VO, the GVOA should include a provision about the compulsory sharing of *pre-existing independent IPR* that is necessary for achieving the objective of the VO (upgrade of the aircraft).

This kind of contract is rather complex in shape and will most probably not be formalized. Instead, its content will be conventional text and its drafting will need to involve humans. In this contract, the parties will need to deal with issues such as the sharing of responsibilities and risks for the overall project. This collaboration agreement will probably only include the permanent members of the VO, while the non-permanent members (the AVO) will not be a contractual partner but a third party to this agreement. Hence, the contractual rules on e.g. confidentiality will not be binding upon the members of the AVO. This doesn't mean hat the AVO will not have the obligation to keep the information confidential, but only that this obligation will be established in a separate agreement between the CE VO and AVO, and not in the General VO Agreement.

The general VO agreement also functions as a framework agreement for SLAs established between the CE VO partners. It can hence refer some of the more specific issues to the SLAs.

2.5.1.2 AVO General VO Agreement

Similar to the GVOA between the members of the CE VO, there will be a general VO agreement in place between the members of the Analysis VO to determine the rules for collaboration and to constitute a framework for SLAs between the AVO members.

2.5.1.3 Air VO General VO Agreement

Given that also the Air VO is a virtual organization of airlines, there will most likely also be a GVOA in place between these parties.

2.5.1.4 Contract CE VO – AVO on Analysis Services

A contract between the CEVO and the AVO should describe the analysis services to be delivered by the AVO and the remuneration for these services to be paid by the CEVO. It is likely that this will not be a collaborative kind of contract, since the AVO members are not supposed to be sharing the risks related to the design (and possible future manufacturing) of the aircraft update. Nevertheless, the issues to be

addressed in this contract are comprehensive, since the AVO members will have access to know-how and trade secrets belonging to the CE VO members. Hence, this contract should also address issues like confidentiality and necessary information security requirements.

In practice the contract can not be concluded between the VOs themselves, since these are not legal entities. Instead, the contract must either be concluded between on the one hand the members of the CE VO and on the other hand the members of the AVO. Alternatively, the contract could be concluded by one member of each VO who represents the other VO members.

This contract may also govern the SLAs to be established between the members of the CE VO and members of the AVO.

2.5.1.5 Contracts Air VO – CE VO on Aircraft Sale and Maintenance

The CE VO has earlier designed and manufactured a number of aircrafts and sold a number of planes to the Air VO or members of the Air VO. There will be different contracts in place, which may cover the maintenance and possible future update of the aircraft. The contracts that regard the maintenance of the aircrafts will most likely also include provisions on mutual information. These contracts will also govern the CE VO's access to the product configuration database held by the Air VO.

2.5.1.6 Service Level Agreements

Service Level Agreements can in addition be established between any of the involved partners (including the members of the AVO) in order to deal with IT service provision. The SLAs are much less complex compared to the collaboration agreements and the agreement between the CE VO and the AVO. Consequently, they can be established as electronic contracts that are established, executed and monitored in an electronic way.

In principle, the SLAs could be established between the collective members of the CE VO and the collective members of the AVO. However, it is also possible that some SLAs could be established between single partners of the respective VOs.

Figure 9 illustrates a possible contract structure for the CE scenario.

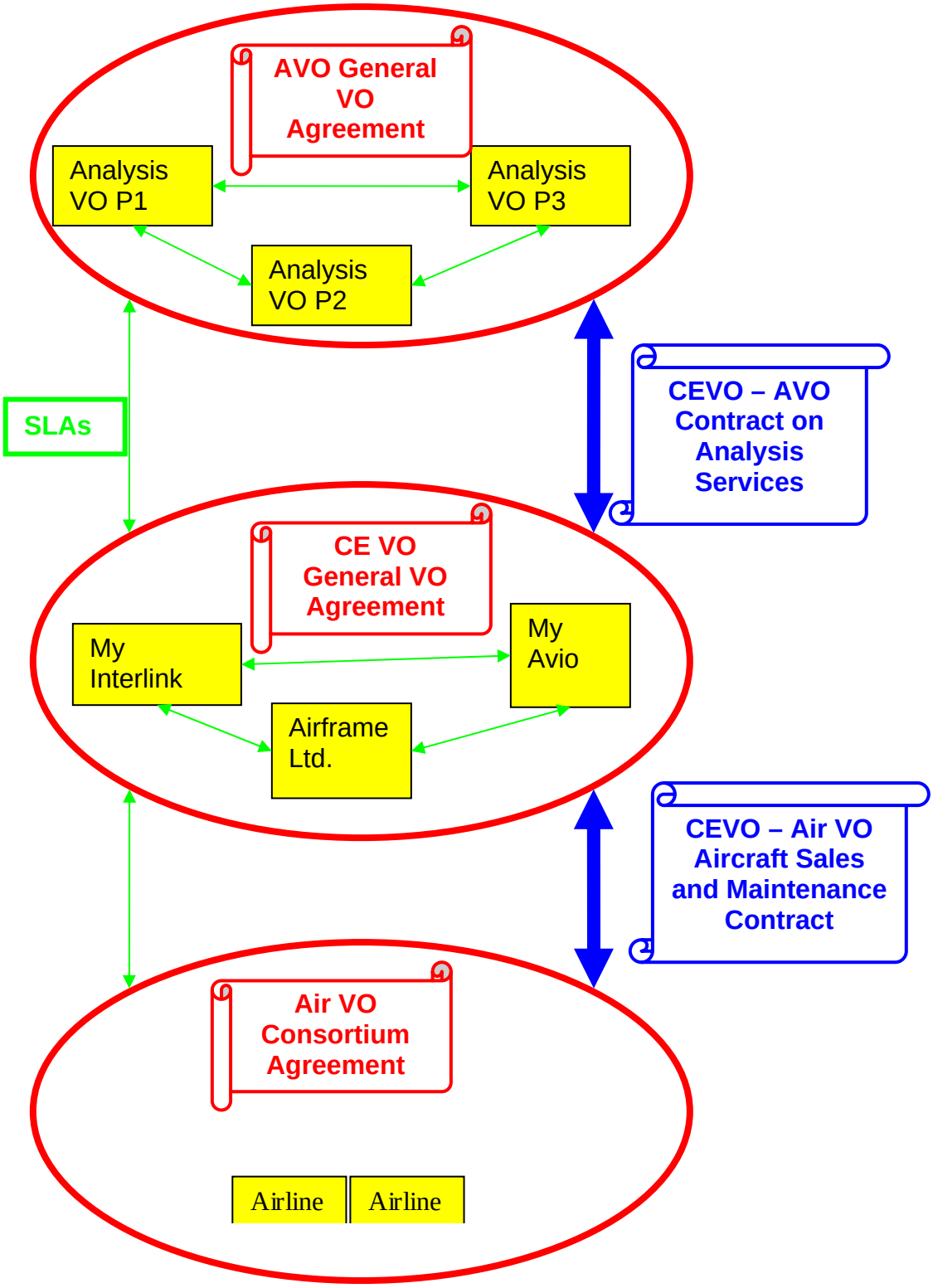

Figure 9 Contractual relations in the CE VO scenario

2.6 Assets

Before identifying the assets, we need to decide on what kind of asset values to use. Given the lack of concrete information about the (monetary) value of assets in the scenario, we decided to assign qualitative values to the assets. The value categories and their interpretations are listed in Table 9.

Asset Value	Description
Very Low	~10 K€
Low	Analysis report. Customer requirements. ~100 K€
Medium	3D model. ~1 M€
High	Complete subsystem design. ~10 M€
Very High	Complete aircraft design. Upgrade contract. Aircraft. ~100 M€

Table 9 Asset value definitions

Assets were identified from the viewpoint of the system integrator stakeholder based on the CE scenario description. The assets were each assigned a value from the categories defined above. The complete list of assets is shown in Table 10. This also includes an initial set of links to relevant IPR mechanisms which may be used to protect the various assets. This is expanded upon in section 2.6.1 below.

Asset ID	Description	IPR protection	Value
PDD	The Product Design Database (PDD) stores all the product design models created by SI	- Copyright? - Database - Design? - Patent? - Trade secret/know-how	Low
Concept design	Share in high-level concept design of passenger aircraft with communication system	- Trade Secret	High
Integrated design	Share in design showing integration of subsystems into a complete passenger aircraft	- Designs? - Patents? - Trade secret/know-how	Very High
Requirements	Customer requirements	- Trade secret/know-how - Copyright?	High
Analysis report	Analysis report from the AVO	- Copyright?	Medium
Know-how/ trade secret	SI's internal knowledge on system integration	- Trade secret/know-how	High

Asset ID	Description	IPR protection	Value
Market share	SI's market share in system integration market		Very High
VO participation	SI is partner in CE VO		Very High
Revenue	SI's revenue from projects, licensing, etc.		High
Partner trust	The CE VO partners' trust in the SI		High
Client trust	The clients' trust in the SI		Very High
AirVO project	Project to upgrade AirVO airplane design with in-flight entertainment system		High
Analysis data	Raw analysis results	- Trade secret/know-how	Medium
Subsystem design	Subsystem design models, owned by other CE VO partners	- Design? - Patent? - Trade secret/know-how	High

Table 10 Asset table

The following asset diagrams show the assets listed in Table 10. Figure 10 shows intellectual property assets, some of which may be owned in whole or part by the system integrator while others originate from the other actors but are still of value to the system integrator, Figure 11 shows other assets related to e.g. business or financial aspects.

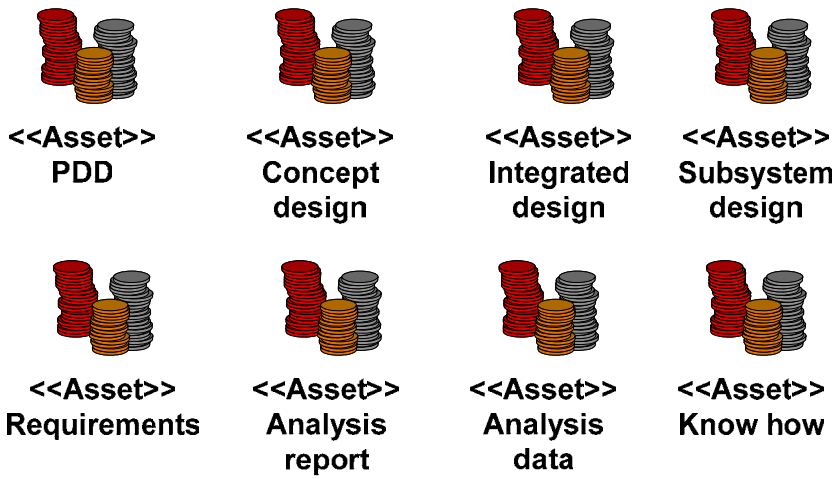

Figure 10 Intellectual property assets

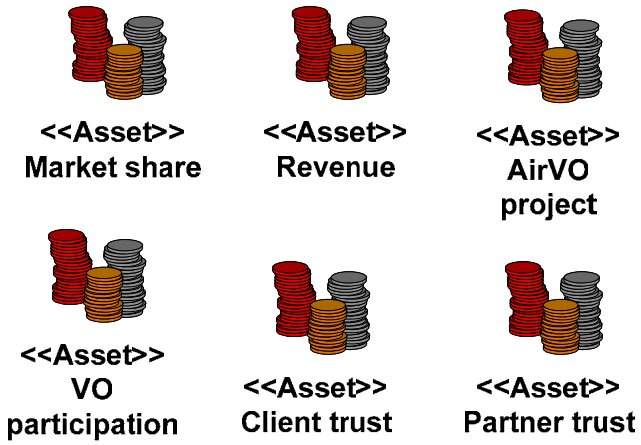

Figure 11 Other assets

2.6.1 IPR Protection of Assets in the Scenario

As indicated in the asset table above, many of the relevant assets are or can be protected by intellectual or industrial property rights.

2.6.1.1 Copyright

Copyright refers to the protection of works resulting from the author's own intellectual creation.[14] The work can be literary, dramatic, musical, artistic or of other kind. In order to be protected, the work must be original. Copyright protection does not require registration, although it may be possible to register the work in e.g. a public register. Such registration merely has a declarative function, since the protection emerges simultaneously with the creation of the intellectual work. The ease of copying digitalized information has led to the development of digital rights management (DRM) systems. Following a harmonization by the EU, national laws now provide protection against the circumvention of DRM systems.[15]

All phases of the life cycle of a virtual organization may involve legal issues relevant to copyright protection. When identifying potential VO partners, the existence of relevant copyrights may be one of the relevant factors. When forming a VO, the GVOA should include rules about ownership and sharing of IPR including copyrights. When operating a VO, partners will have to take other partners' and third parties' copyrights into account. To the degree new copyright is created by the VO, all rights relating to this copyright should be expressed. In particular, the

[14] See further JAL Sterling *World copyright law: protection of authors' works, performances, phonograms, films, video, broadcasts and published editions in national, international and regional law: with a glossary of legal and technical terms, and a reference list of copyright and related rights laws throughout the world* (2nd Sweet & Maxwell London 2003),section 1.01.

[15] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society

customer requirements and the analysis report (produced by the AVO) may be protected by copyright. Finally, the dissolution phase will be influenced by the allocation of intellectual property rights.[16]

In this context, reference should also be made to the protection of computer programmes and databases according to EC law. Computer programmes are protected by copyright as literary works[17] (note also that patent protection may be available in some cases). Thus, the protection of computer programmes follows most of the generally applicable rules on copyright law.

The development of the in-flight entertainment system in the CE scenario could also involve the development of software, legally protected by the rules mentioned above. However, the scenario does not provide details on this. In case computer programmes are developed within the context of the scenario, national laws corresponding to this directive will be applicable.

2.6.1.2 Database Protection

In contrast to traditional copyright, the protection of databases originates not primarily from general copyright law, but from the *sui generis* protection of databases[18]. According to general copyright rules, databases are protected by copyright to the extent that they are original. If this was the only protection, many databases –which typically are systematic (i.e. not intellectually original) collections of items, e.g. phone books – would lack protection regardless of the fact that their creation required a considerable investment. Therefore, such databases are protected in a particular way through the EC database directive. The creator ("maker") of a database is protected from extraction or re-utilization of (parts of) the database, if there has been a substantive investment in obtaining, verifying or presenting the information. In a VO context, many partners will have their own databases, which will be protected by these rules. A database collectively created by (some of) the VO partners would also be protected. Note however that this protection only refers to the database as a whole or to a substantial part of it. The owner of a database is not protected by the sui-generis rights against the extraction and re-utilization of a non-substantial part of the database. Still, since the material this database includes is most probably protected in themselves by copyright or by other intellectual property rights, this will act as an intrinsic protection against any type of extraction and utilisation. Thus, even though it might be seen as "unsubstantial" extraction by comparison to the amount of material that the database includes, that activity will be regarded as copyright (or other IP right) infringement .

Legal risks in the context of the protection of copyrights and databases relate to the ownership and sharing of rights as mentioned in ID 6.2.2, section 3.

---

[16] The ALIVE IST project has produced an overview of possible copyright issues relevant to the different phases of the VO life cycle, see *Report D 13, ALIVE Project, Intellectual & Industrial Property Rights Legal Issue Subgroup* (2002) http://www.vive-ig.net/projects/alive/docs.html.

[17] Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs

[18] A protection of its own kind, see Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

With respect to the product design database, the CE VO has a major interest in protecting itself against the extraction or re-utilization of any part of the database. If a third party copied and reused elements of the product design database, this would constitute a very high loss. However, this loss does not mainly refer to the investment of having organized the items in a database, but rather to the investment that was necessary to create the items stored in the database. As mentioned above, the database right does not protect against the extraction or reuse of non-substantial parts of the database.

2.6.1.3 Patent

Patents may play an important role for the work of a VO, particularly if the VO wants to use a patented invention or if the work within the VO leads to a patentable invention. A patent is an exclusive right to exploit a new technical invention, e.g. a product, the use of a product or a method. In order to obtain a patent, the inventor is required to apply to a patent office. If the patent is granted, the applicant has the right to exclude others from producing, selling or using the invention. This right is granted for a limited time (normally 20 years).

The patent system in Europe consists of national patents and the European patent. In the future there may also be a new community patent, which currently is subject of intergovernmental discussion.

Some criteria can be seen as common requirements for the patentability of inventions, despite existing differences between the various national patent rules and between national and European patent rules. Generally speaking, an invention must fulfil the following criteria in order to be patentable:

- Novelty: The invention must be new with respect to the prior state of the art.
- Inventive step: The invention must be based on an inventive step, i.e. it must not only be a routine development that can be foreseen as obviously following from the state of the art.
- Industrial application: The invention needs to be industrially applicable, regardless of the type of industry.

The collaboration in a VO may require that one partner needs to exploit a patented invention where another VO partner is the patent owner. In such cases, the patent owner typically issues a non-exclusive or exclusive license enabling this. Depending on the business objective and the context of the VO, the license may be granted royalty-free (e.g. based on cross-licensing) or at a lower rate. If the business objective of the VO requires this, the licensing of all necessary patents can also made compulsory in the General VO Agreement.

Alternatively, one could also consider the total transfer of patent rights to a VO partner or to the VO, if the VO is a separate legal entity. However, this would imply that the patent owner loses his rights. In addition, it would have to be registered with the respective authorities. Hence, this option is not desirable for the co-operation within a VO, which often will be limited in time.

Legal risks with respect to patent protection in VOs also include ownership, protection and sharing of rights, all of which are discussed in in ID 6.2.2, section 3.

It is likely that the upgrade of the airplane will involve the use of patented inventions. The development work may also lead to a patentable invention. However, no details are provided in the scenario on any patent issues.

2.6.1.4 Trademark

Trademarks protect brands. It is possible that a trademark of the CE VO is relevant for the asset “client trust”. However, no details are given in the scenario about any trademark issues.

2.6.1.5 Design Protection

The protection of designs refers to three-dimensional and two-dimensional features that are new and either original or have an individual character. In many countries the design must also have a useful function. A design can be registered, which will lead to a more comprehensive protection. However, even unregistered designs may be protected, both as a copyrighted work of art and/or due to the protection conferred in laws prohibiting unfair competition.

While it is possible that the collaboration in the CE VO scenario involves registered designs or the development of new designs that can be registered, no details are available. In any case, the general issues discussed in ID 6.2.2, section 3. will apply also to design protection.

2.6.1.6 Confidential Information (Know-how and Trade Secrets)

When a VO pools resources in order to exploit a business opportunity, there is an inherent risk that this can lead to the loss of control over information a VO partner wants to keep secret. Such secrets can include business plans such as pricing schemes or products under development as well as business methods or techniques not generally known. This information can be represented in different ways, including written or electronic representation and/or the simple fact that the employees have acquired certain knowledge (know-how). The principal reason why a business entity would want to keep this information secret is that the information results in an advantage compared to competitors who do not have access to the information. The safest option to protect such information would be not to disclose it to anybody. However, this may in many cases lead to a situation where the entity is unable to co-operate with others, constantly fearing that secret information could be disclosed. Therefore, if there are compelling business reasons for disclosure, the confidentiality of such information can be protected through a contract between the discloser and the entity to which the information is disclosed. However, this legal protection is rather weak and it has to be integrated with a strategy to protect secret information. This includes ensuring that confidential information is only disclosed to a trustworthy partner and that there are appropriate information security mechanisms in place to protect the information.

2.6.1.6.1 Requirements for Protection

On the international level, a protection of secret information is included in Article 39 (2) of the TRIPS agreement.[19] This article provides a protection for information

- which is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known or accessible to persons within the circles that normally deal with the kind of information in question;
- which has commercial value because it is secret;
- and which has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Hence, trade secrets are protected without any need for registration or other formal procedures, as long as they are sufficiently secret. The above mentioned elements are central also for the protection of confidential information according to national laws, even though there may be some differences in national laws.[20]

2.6.1.6.2 Consequences for Infringements

Some consequences for infringements will depend on the applicable national law. Most countries' laws provide the possibility of criminal consequences for theft of confidential data. Moreover, the owner of the trade secret may be entitled to damages and/or injunctive relief[21]. For parties to a confidentiality agreement, there may also be contractual consequences.

2.6.1.6.3 Confidential Information and VOs

Virtual organisations depend on the ability of the involved partners to collaborate, which may involve the sharing of confidential information. Hence, there is an inherent conflict between the business need to share confidential information and the importance of the same information. The TrustCoM framework could assist in balancing these two requirements. This is the case for all parts of the framework, i.e. trust management, security management and contract management.

2.6.1.6.4 Trust Management

The aim for trust management in the context of confidential business information is to make sure that confidential information does not reach the public domain or the sphere of e.g. a competitor. This risk can be reduced through limiting the collaboration to trustworthy parties. The trustworthiness assessment may to take into account factors such as how close the potential trustee is to a competitor. For example, the trustee may himself compete with the trustor in a market segment where the confidential information is relevant. Furthermore, the potential trustee

---

[19] Agreement on Trade-Related Aspects of Intellectual Property Rights, http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm

[20] For a brief overview on trade secret protection in various countries cf. IPR helpdesk project, The legal Protection of trade secrets, available at www.ipr-helpdesk.org.

[21] Injunction: A prohibitive remedy issued or granted by a court, forbidding to do some act which the defendant is attempting to commit, or restraining the continuance thereof; (Black's Law Dictionary, 5th ed.).

may be allied with a competitor in a strategic alliance, another VO, or other business relation. If the potential collaborator has a close relation to a competitor, this may indicate that one should be more careful with entrusting this entity with confidential information.

2.6.1.6.5 Security Management

The aim for security management in this context is to provide effective measures to ensure that the confidential information is kept secret. The required level of protection cannot be determined in the abstract; laws usually require that reasonable steps are taken under the circumstances. The circumstances will in this context relate to the collaboration of different entities in a virtual organisation. This involves that a distinction will have to be made between (1) short-term and long term VOs, (2) VOs which involve a large number of partners vs. minor VOs, (3) VOs that heavily involve the sharing, exchange and dissemination of confidential information, (4) VOs that deal with confidential information that requires a high level of protection vs. VOs dealing with information which is confidential, but where the misappropriation or dissemination would cause less damage. Hence, VOs handling different levels of confidential information should be able to choose different levels of security protection.

2.6.1.6.6 Contract Management

One of the most useful possibilities of protecting confidential information is the use of confidentiality agreements/non-disclosure agreements. These agreements can be consented upon on a case-by case basis, or confidentiality rules can be included in other contracts, e.g. a general VO agreement.

The aim of the confidentiality agreement is to state explicitly the conditions and the circumstances in which one party(*the discloser*) agrees to disclose information that he regards as *CONFIDENTIAL* to its business partner(*the recipient*), so as to prevent others from accessing and/or using them. The disclosure does not imply any transfer of intellectual property rights on the document being disclosed.

To constitute an efficient “treatment”, this agreement should first of all define the meaning of the key terms:” confidential information” and “disclosure”. In case of a medium/long term partnership it might be difficult to assess “ex-ante” what are the documents or the information that need to be revealed throughout the project; it is therefore advisable to set up also a system to classify as confidential information that will be disclosed later and at various intervals over a period of time . Various degrees of confidentiality might also be agreed upon, depending on the sensibility of the document in question. Secondly, it is important to determine the operating conditions, that is the use that can be made of the revealed information, the time interval for which the agreement applies and the sanctions in case of breach of obligations.

The confidentiality agreement should mainly be seen as a tool for the parties to use and adapt according to the needs of the project.. The aim of the confidentiality agreement is to state explicitly the conditions and the circumstances in which one party(*the discloser*) agrees to disclose information that he regards as *CONFIDENTIAL* to its business partner(*the recipient*), so as to prevent others from

accessing and/or using them. The disclosure does not imply any transfer of intellectual property rights on the document being disclosed.

To constitute an efficient "treatment", this agreement should first of all define the meaning of the key terms:" confidential information" and "disclosure". In case of a medium/long term partnership it might be difficult to assess "ex-ante" what are the documents or the information that need to be revealed throughout the project; it is therefore advisable to set up also a system to classify as confidential information that will be disclosed later and at various intervals over a period of time . Various degrees of confidentiality might also be agreed upon, depending on the sensibility of the document in question. Secondly, it is important to determine the operating conditions, that is the use that can be made of the revealed information, the time interval for which the agreement applies and the sanctions in case of breach of obligations.

The confidentiality agreement should mainly be seen as a tool for the parties to use and adapt according to the needs of the project..

One of the major advantages of TrustCoM is the possibility to relate the contractual level closely to the security level. In particular, the general VO agreement or a lower level VO contract can include rules about how VO partners should treat and protect confidential information that belongs to other VO partners individually or collectively.

2.7 Policies and Risk Evaluation Criteria

The following table defines the risk evaluation criteria used in the analysis, based on the risk values defined in the risk matrix in Table 4:

Criteria ID	Stakeholder ID	Asset IDs	Description
C1	SI	All	If "Risk Value" is equal to "Low" then "Accept the risk"
C2	SI	All	If "Risk Value" is equal to "Moderate" then "Monitor the risk"
C3	SI	All	If "Risk Value" is greater than or equal to "Major" then "Treat the risk"

Table 11 Risk evaluation criteria

2.8 Approval

During the meeting with BAE Systems and IBM in London on January 27th the background documentation in this chapter was presented. Remarks and change requests were recorded in the approval registration form in Table 12. Due to time constraints during the meeting, the approval of each change was performed by the risk assessment team itself.

Change Description	Agreement (Owner decision)
Stakeholder changed to Airframe Ltd.	Yes
Product configuration database refers to aircraft configuration	Yes
Must distinguish between different kinds of 3D models	Remove 3D models as asset, because included in subsystem design
Analysis data should be asset (?)	Yes, value = “medium”
Business processes changed to engineering processes AND production processes	No
Asset “Requirements” should have higher value (?) -> new value “high”	Yes
Hierarchy of 3D models, e.g. asset wing model	No
Analysis report -> asset value “Medium”	Yes
New asset: subsystem design -> asset value “High”	Yes
Several analysis reports reflecting the subsystems(?)	No
New asset: “Availability of PDD”	No, not relevant to IPR
New asset: “Know-how on system integration”	Yes, replaces “business processes”; keep value
Differentiation between “market share” and “revenue” should give “market share” the higher value	Yes
”Client trust” higher value than “revenue”	Yes
Revenue -> asset value “high”	Yes
Partner trust -> asset value “high”	Yes (no change)
Client trust -> asset value “very high”	Yes

Table 12 Approval registration form

3 Risk Identification

This section presents the results of the risk identification sessions in Oslo (November 18th and 29th, January 11th) and London (January 28th). The risks have been categorised into risks related to trade secrets and other IPR related risks.

Figure 12 shows the risk categories we have identified. These risks will be described in more detail in the following sections.

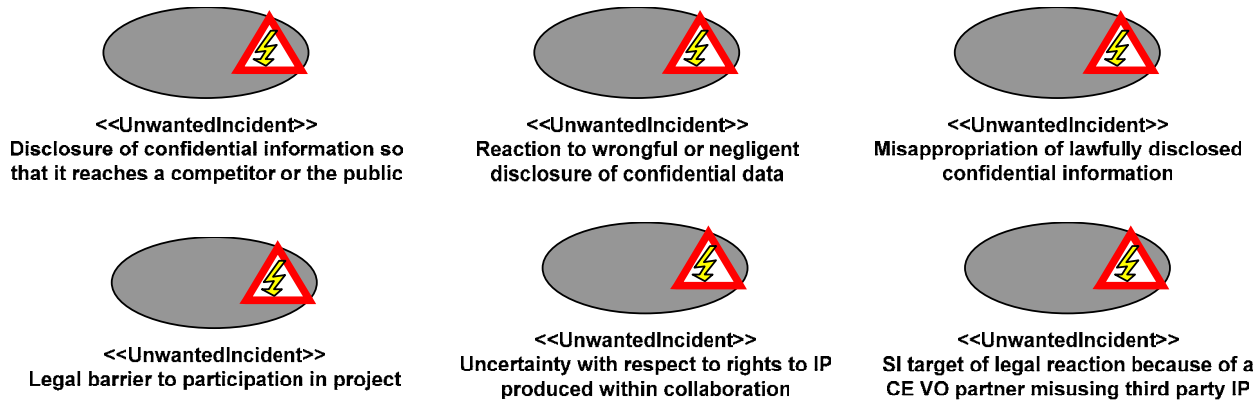

Figure 12 Risk categories

The risks mainly relate to two areas, namely confidential information and other IPR. These areas are detailed in the sections below.

3.1 Legal Risks Related to Confidential Information

3.1.1 Disclosure of Confidential Information so that it Reaches a Competitor or the Public

There is a risk that confidential information is disclosed to a third party and either reaches the public domain or the sphere of a competitor or another third party who could misuse the information. As mentioned above in section 2.6.1.6, the protection of trade secrets is closely related to the information being kept secret (Figure 13). Secrecy may be the only way to protect many of the CE's assets, including the customer requirements, information relating to different design stages (starting with the concept design, which over time will evolve into the integrated design, comprising several sub-system designs), and analysis data produced by the AVO.

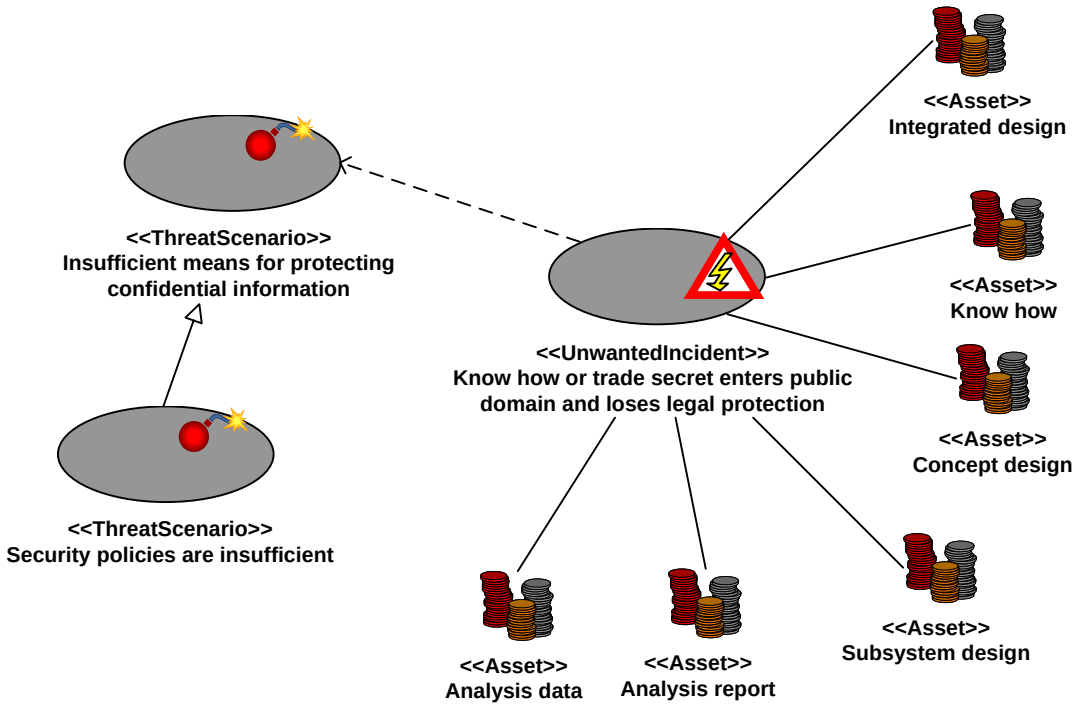

Figure 13 Confidential information loses legal protection

The ownership of this information will vary, some information (e.g. a subsystem design developed by one VO partner) will be owned by a single partner, possibly the SI itself. Other information, e.g. the integrated design, may have been developed by all partners together and may be owned by all partners collectively.

The following risks involve (1) different recipients of the confidential information and (2) the different possibilities for how the confidential information is disclosed.

3.1.1.1 Disclosure to a competitor

The risk depends on the recipient of the confidential information and what this person or entity may do with the information. A competitor may use the information in its own business, e.g. to compete for a similar project. The disclosure to a competitor could be caused e.g. by a client (a member of the AirVO), a CE VO partner or one of its employees or even one of the SI's employees (Figure 14).

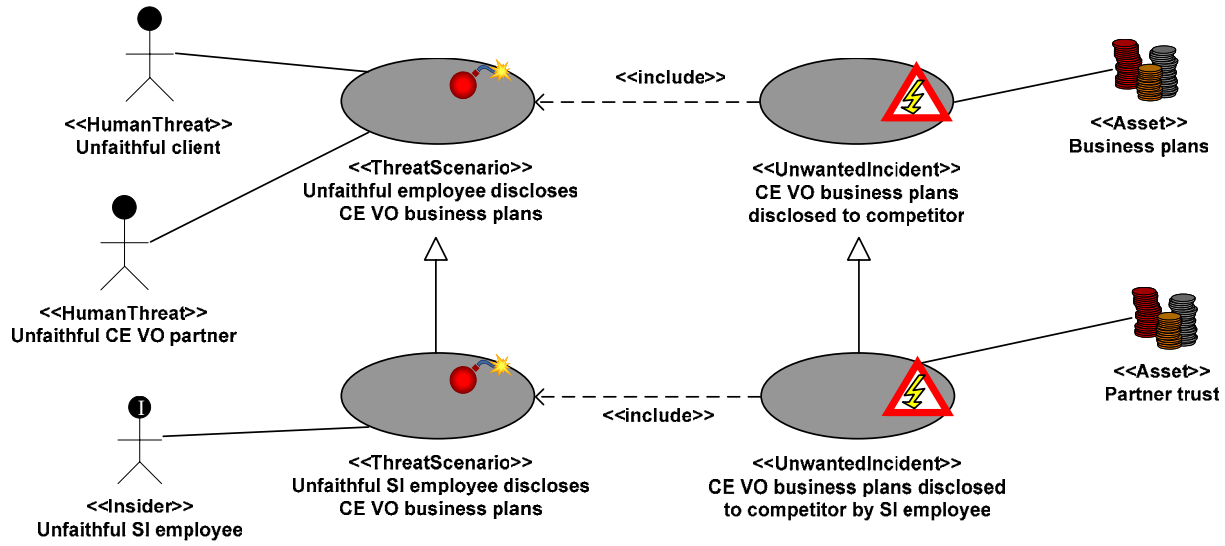

Figure 14 Disclosure of confidential information by unfaithful employee or partner

The value of the customer requirements for SI depends on their exclusivity. Hence, their disclosure would affect both the value of the requirements and the clients' trust in the CEVO and its members (Figure 15).

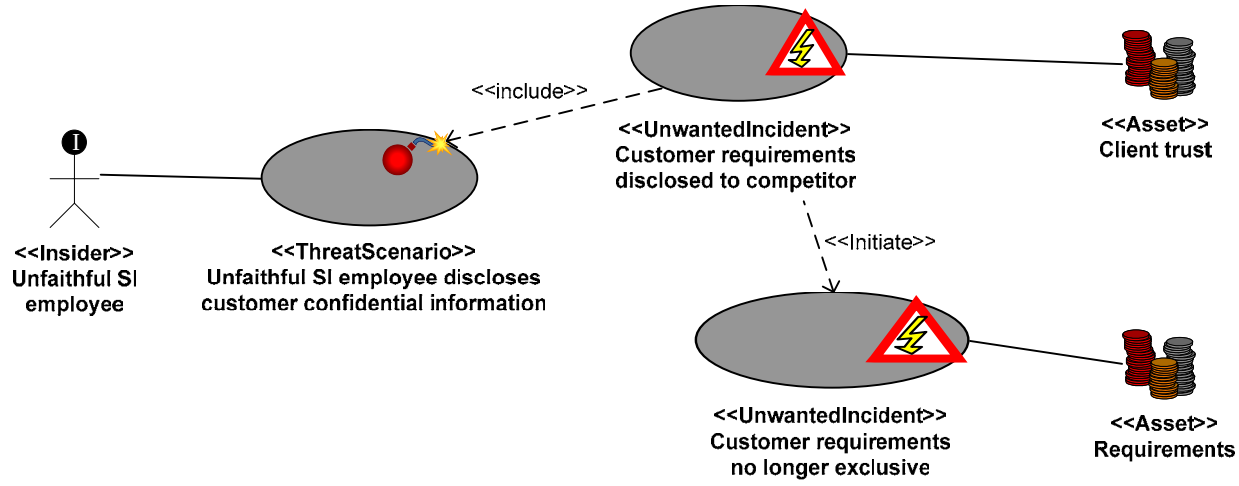

Figure 15 Disclosure of customer requirements

Confidential information can also be disclosed through industrial espionage, e.g. a hacker breaking into the system to steal the concept design (Figure 16).

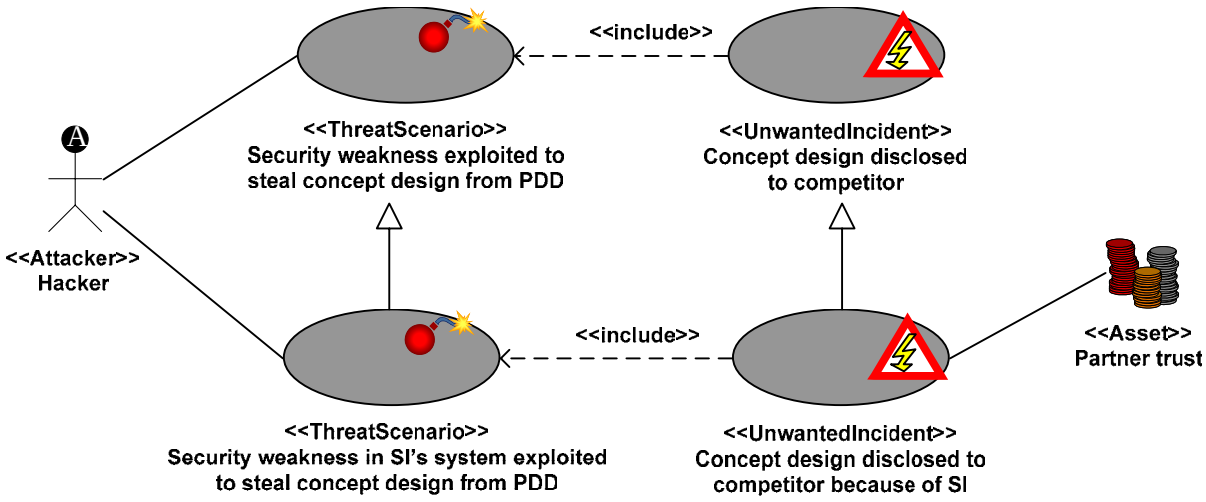

Figure 16 Security weakness exploited to steal confidential information

A competitor may use the information in its own business. In particular, a competitor of the CE VO could use confidential information to compete for the same project. An unwanted incident could be the CE VO losing this project (upgrade of the aircraft with in-flight entertainment system) to a competitor (Figure 17). In some situations this could even lead to the dissolution of the CE VO (Figure 18).

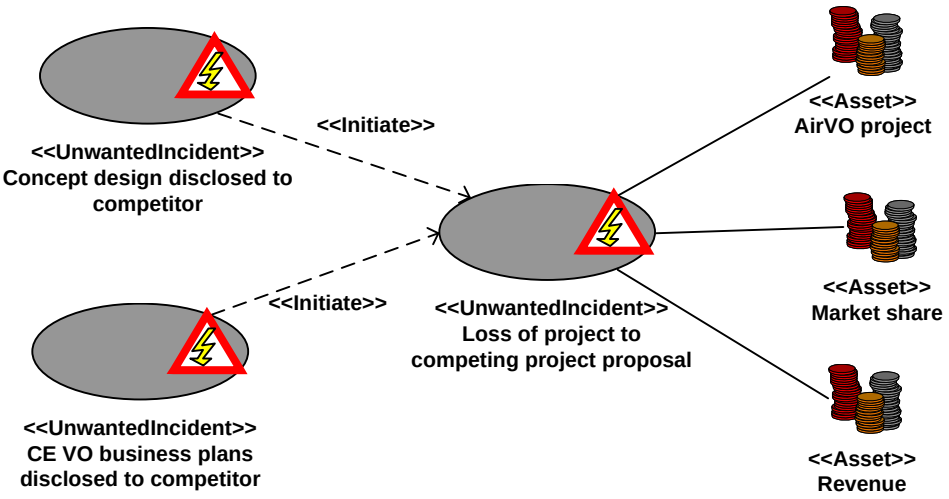

Figure 17 Loss of project to other proposal

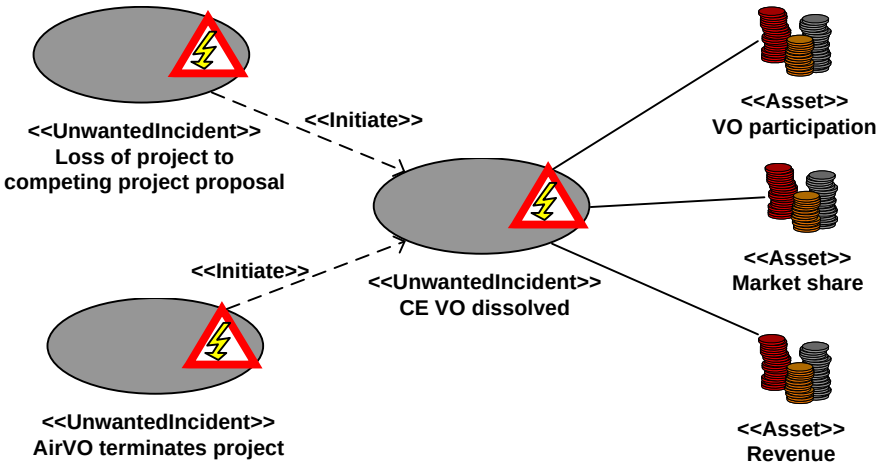

Figure 18 VO dissolved

3.1.1.2 Disclosure to Other Third Parties

But also a non-competitor could do a considerable harm, e.g. by publishing the information so that it reaches the public domain. The latter would lead to the loss of protection for this information (even though it may be possible to claim damages for this loss from the responsible actor). Even if the information is not published in the first place, it could be used to blackmail the affected parties.

3.1.1.3 Possibilities of Disclosure

There are numerous possibilities of how the confidential data could be disclosed. These include the following:

- Human insider: It is possible to think of an unfaithful employee who gets access to the information and discloses it for his own benefit (Figure 19).

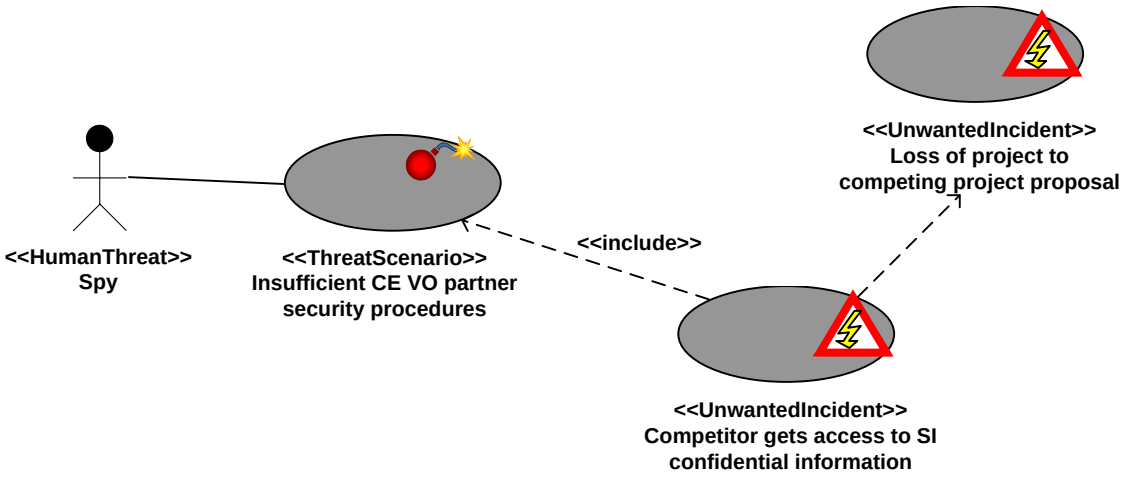

Figure 19 Industrial espionage leads to disclosure of confidential information

- Employee leaves: There is a risk that an employee of any of the involved partners joins a competing company and uses acquired know-how or confidential data with his new employer (Figure 20).

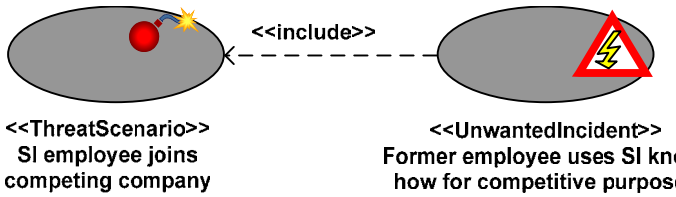

Figure 20 Former employee uses SI know how for competitive purposes

- Human Negligence: Confidential data may be disclosed due the insufficient awareness of confidentiality issues (Figure 21 and Figure 22).

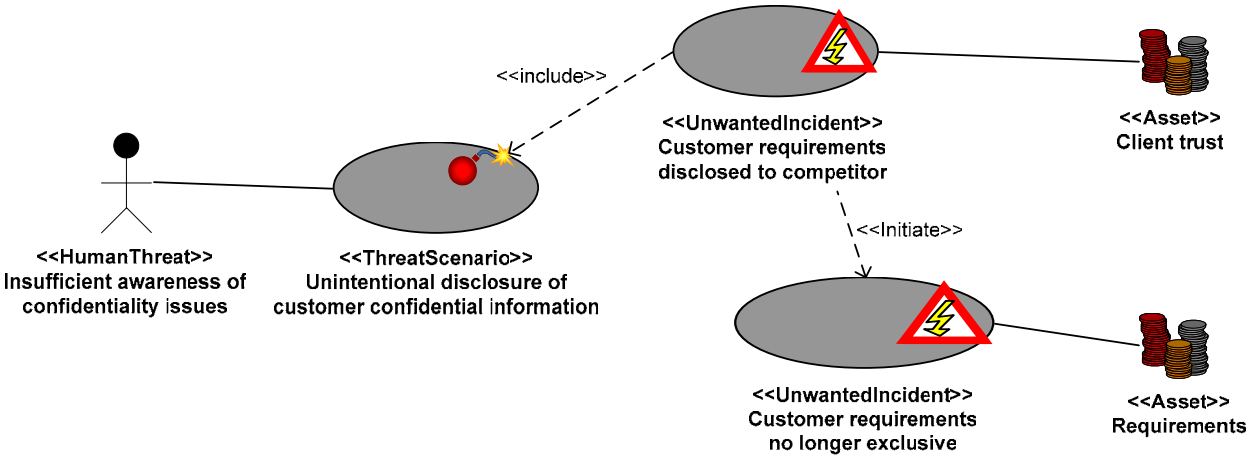

Figure 21 Confidential information disclosed because of insufficient awareness of confidentiality

- Human Error: Mistakes in handling confidential information can lead to disclosure, even if the employee is aware of the sensitivity of the information.

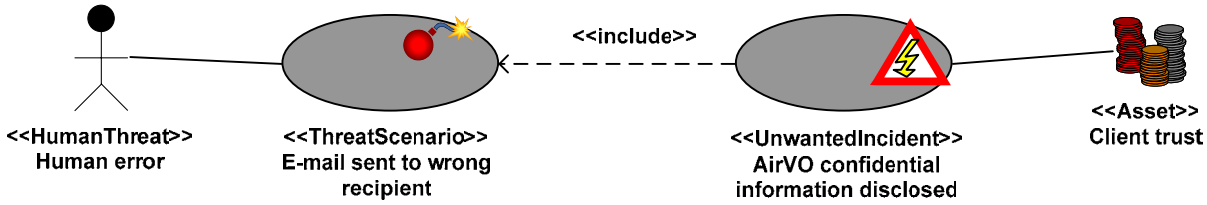

Figure 22 Confidential information disclosed through human error

- Conflicting business interests: Theoretically it could also be in the business interests of any of the involved parties (within or outside the CE VO) to

disclose the information, e.g. if this business entity has a close relationship with any of the competitors. The relationship with a competitor could also evolve over time or it could be established through a merger or an acquisition by a competitor, as illustrated in Figure 23.

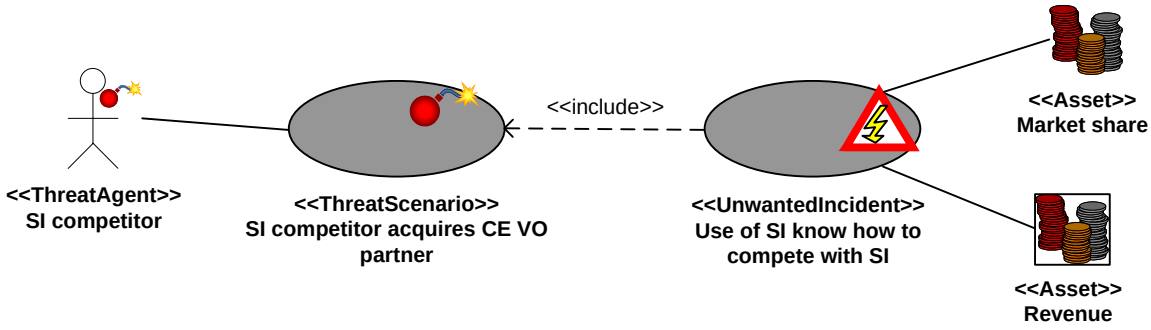

Figure 23 Acquisition of VO partner by SI competitor

- Third party: A third party could act as a hacker and/or use e.g. malicious software to get hold of confidential information. This party could take advantage of security weaknesses anywhere in the information system that is set up between the partners of the CE VO and the AVO (Figure 16 and Figure 24).

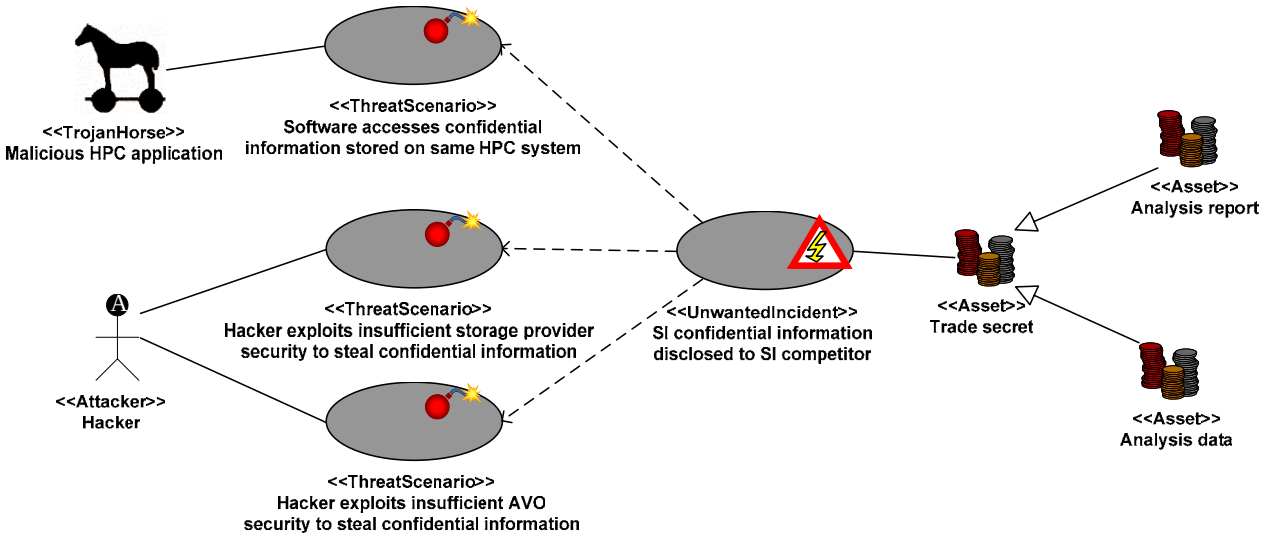

Figure 24 Insufficient AVO security leads to disclosure of confidential information

3.1.2 Reaction to Wrongful or Negligent Disclosure of Confidential Data

A number of risks relate to the SI being responsible for the wrongful or negligent disclosure of confidential information (partly) belonging to other VO members or third parties. For example, a wrongful disclosure could be caused by a spy among

the employees of the SI. A negligent disclosure could relate to insufficient security mechanisms for which SI is responsible.

If the SI is responsible for a wrongful or negligent disclosure, SI may risk reactions by other VO members. These reactions may come in addition to the possible loss caused by the leakage itself. The reactions to a wrongful or negligent disclosure could be everything from a lower trust level to being expelled from the VO (Figure 25), following a procedure according to the GVOA.

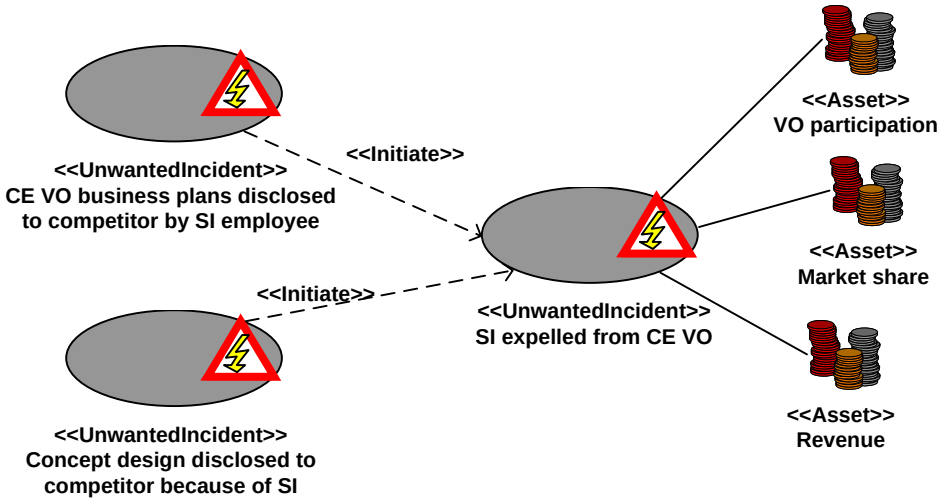

Figure 25 SI expelled from VO

The SI could also be the target of a lawsuit by the affected party, be it a member of the CE VO (Figure 26) or be it a customer, e.g. a member of the AirVO (Figure 27).

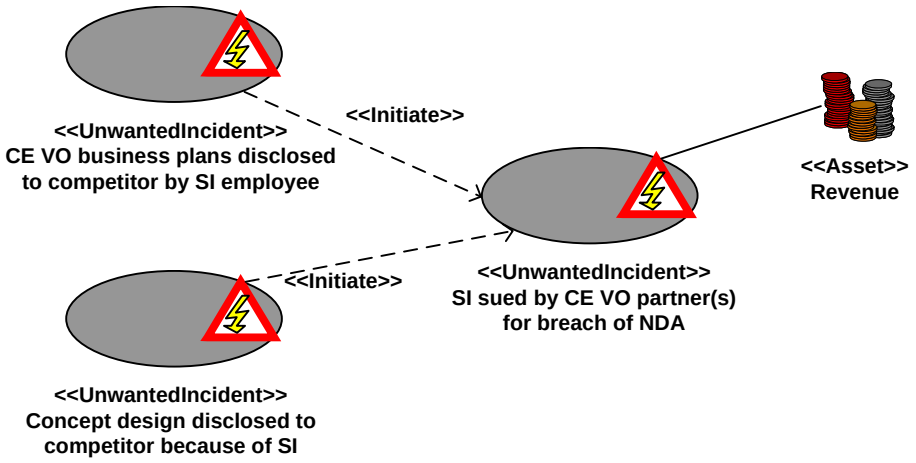

Figure 26 SI sued by VO for breach of NDA

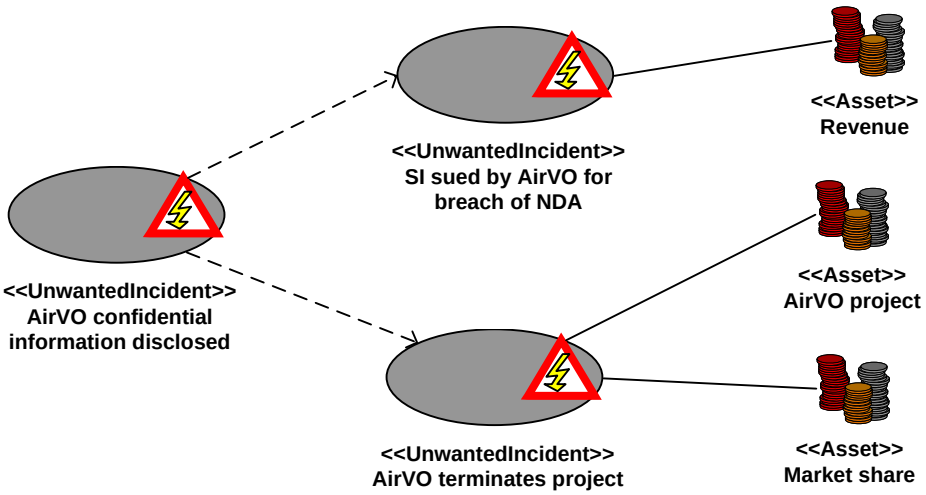

Figure 27 Disclosure of client's confidential information

Another similar risk relates to a situation where the disclosure of confidential information is neither wrongful nor negligent but where the disclosing partner (SI) would be forced to disclose confidential information due to a binding decision by a public authority (Figure 28). If this case is not included as a special case in the respective contracts, SI could find itself in a situation of conflicting obligations, being forced to breach the non-disclosure agreement.

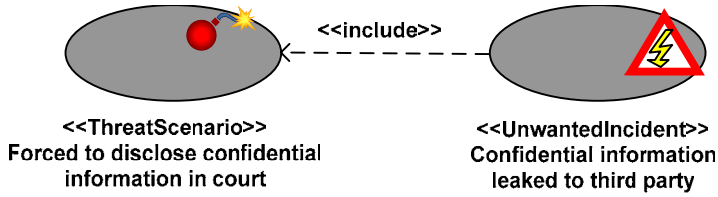

Figure 28 Forced to disclose confidential information in court

3.1.3 Misappropriation of Lawfully Disclosed Confidential Information

There is also a risk that confidential business information which is lawfully disclosed in the context of the collaboration is then used inappropriately by the recipient. The use of SI's confidential information for competitive purposes may enable one of the VO partners to compete with SI (Figure 29).

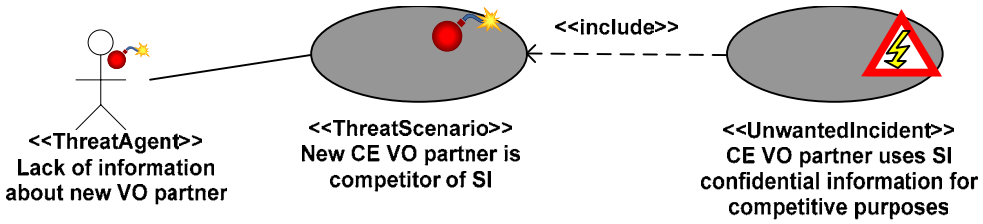

Figure 29 Competitor gains access to SI confidential information by joining VO

The relevance of this risk depends on whether or not SI will disclose any confidential information to any of the involved partners and whether this information could be used by the partner for competitive purposes. It is difficult to decide if any of the partners are in a position to directly compete with SI. SI seems to have a rather broad field of competencies related to the design and manufacturing of aircrafts, and the other involved partners seem to work in a more limited sector. However, it is possible to think of a situation where one of the CE VO partners is already part of a larger company or is acquired by or merges with a business that has business interests that are competing with SI (Figure 30).

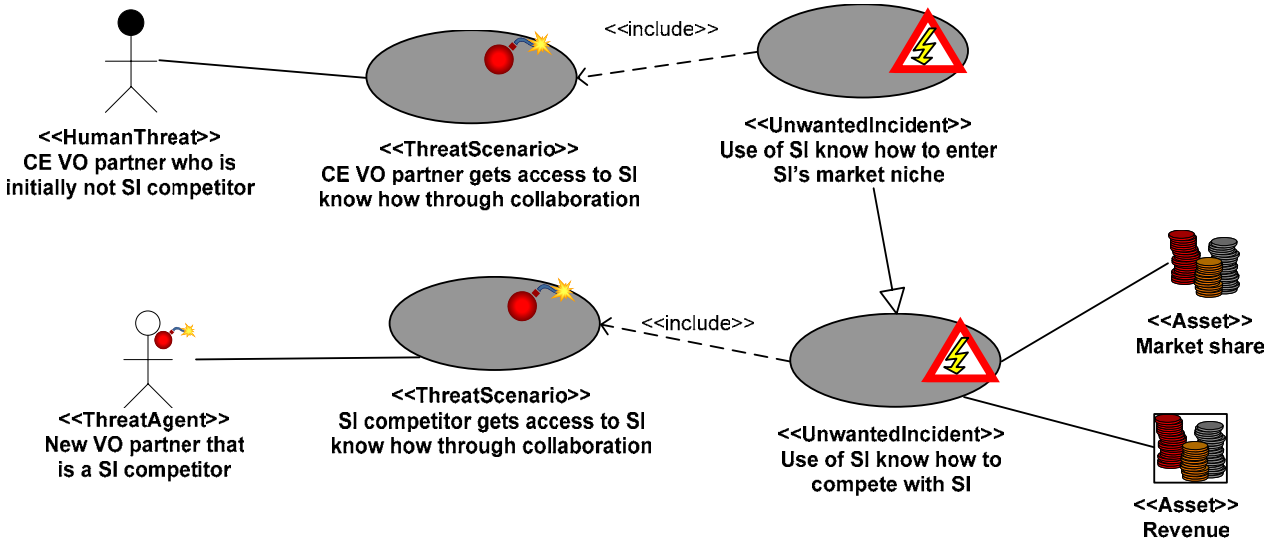

Figure 30 Competitor gains access to SI know how and uses it for competitive purposes

Similarly, one of the AVO members or other cooperating third parties could also be acquired or could merge with a business that has business interests that are competing with SI (Figure 31).

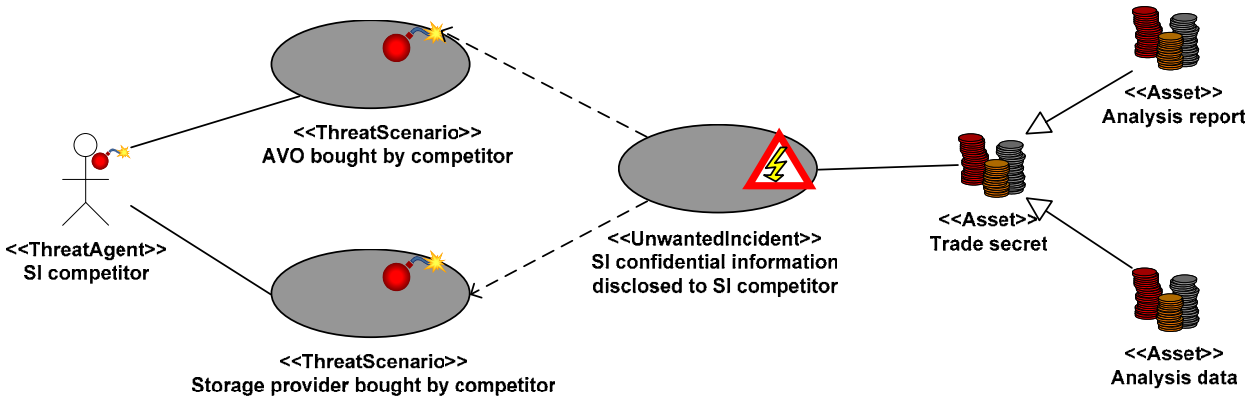

Figure 31 Competitor gets access to SI confidential information by acquiring AVO or third party

3.1.4 Severe confidentiality rules restrict participation in other projects

As mentioned in section 2.5.1.1, the GVOA will include rules about non-disclosure and possibly non-use of confidential information. A similar rule will be included in the contract between the CE VO and the AVO. From the point of some partners, there is a risk that such contract may present a barrier to participation in other projects. For example, the contract may prohibit the VO partner from joining a similar project or from assigning specific employees to similar projects, thereby inhibiting the use of confidential information outside the first VO collaboration. Such a contract rule would itself present a risk to the stakeholder (Figure 32).

Figure 32 NDA barrier to participation in project

3.1.5 Lack of Access to a Partner's Confidential Information

There is a risk that SI may fail to get access to a partner's confidential information, know-how or trade secrets or other information which is necessary in order to be able to carry out the project. A partner may not want to provide access to confidential information in order to protect his own assets. This lack of access could lead to a delay in the work or eventually to SI not being able to fulfil its contractual obligations towards the other parties (Figure 33).

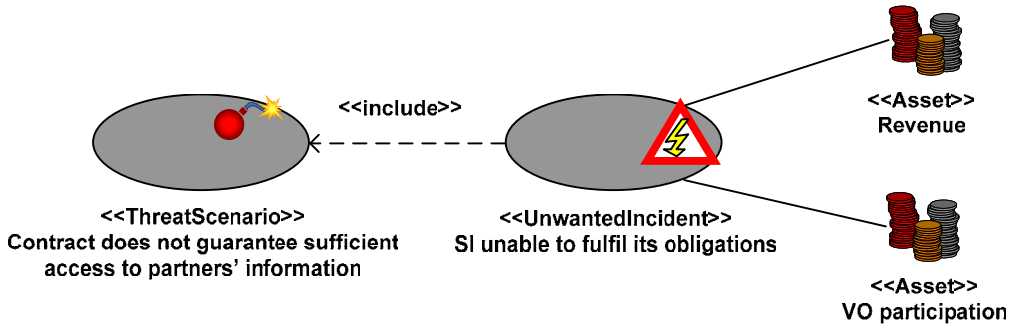

Figure 33 SI unable to fulfil obligations

3.2 Legal Risks Related to Other IPR

Some of the identified legal risks relate to other IPR.

3.2.1 Uncertainty with respect to rights to IP produced within collaboration

If the General VO Agreement for the CE VO does not contain rules about the ownership of IPR, then ownership will have to be determined by the applicable law. Alternatively, if the contract includes a provision on IPR, but this rule is unclear, this may lead to some uncertainties and possibly legal action with respect to the ownership of IPR developed in the collaboration and with respect to the use of this IPR in other projects (Figure 34).

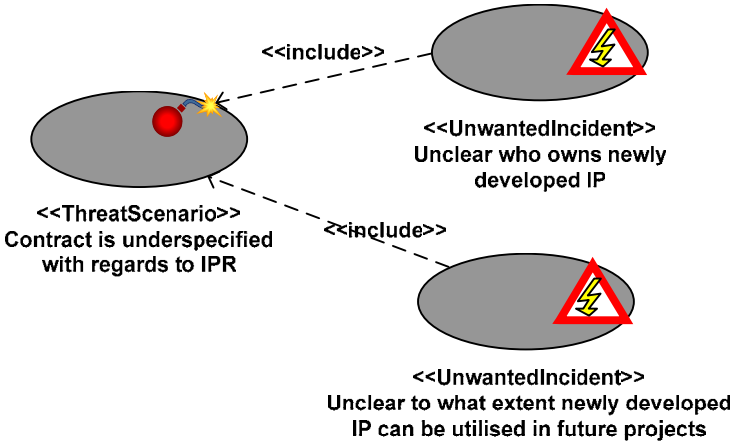

Figure 34 Uncertainty with respect to rights related to IP produced during collaboration

3.2.2 SI target of a legal reaction because of a CEVO partner misusing third party IP

If one of the CE VO members breaches third party IPR while carrying out work for the CE VO, this could lead to a legal reaction by the IPR owner. The risk for the system integrator would be that it could find itself as a target of a legal reaction for breach of IPR, even though another VO partner is responsible for the breach (Figure 35). This may occur due to the fact that third parties may consider the VO partners to be collectively responsible for infringements that occurred while carrying out the project. Particularly if SI is the CE VO partner with best liquidity, it would be the most attractive partner to claim damages from. This would leave it up to SI to claim their expenses from the VO partner who is actually responsible for the breach[22].

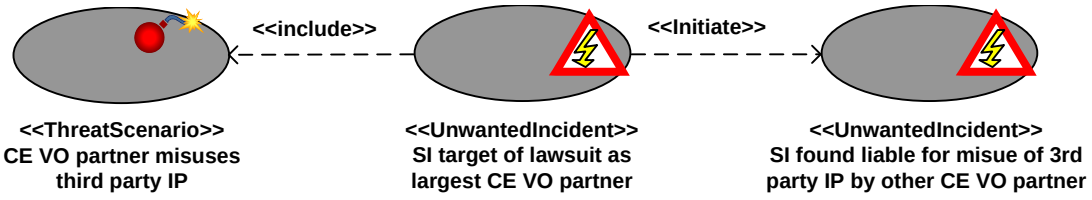

Figure 35 SI target of a lawsuit because of IP misuse by VO partner

[22] Though the partners do not form a new legal entity, some legal systems might consider them as collectively responsible in what concerns the relations to third parties. This will be addressed on our future studies.

4 Consequence and Frequency Analysis and Risk Evaluation

This section presents the results from the consequence and frequency analysis and risk evaluation sessions performed in London (January 28th). Not all the identified unwanted incidents have been assigned consequence and frequency values. This is due in part to the available time and information and in part to some of the unwanted incidents being "intermediary", i.e. they lead to other incidents which we have then assigned consequences and frequencies. The risk values were determined based on the risk matrix presented in Table 4.

Asset ID	Unwanted Incident	Diagram reference	Cons. Value	Freq. Value	Risk Value
Concept design	Concept design disclosed to competitor	Figure 16, Figure 17	Moderate	Unlikely	Moderate
Analysis data, Analysis report, Subsystem design, Concept design, Know how, Integrated design	Know how/trade secret enters public domain and loses legal protection	Figure 13			
Partner trust	Concept design disclosed to competitor because of SI	Figure 16, Figure 25, Figure 26	Moderate	Rare	Low
Client trust	AirVO confidential information disclosed to competitor	Figure 22	Moderate	Rare	Low
AirVO project	Loss of project caused by disclosure of confidential information		Moderate	Unlikely	Moderate
Market share	Loss of project caused by disclosure of confidential information		Moderate	Unlikely	Moderate
Revenue	Loss of project caused by disclosure of confidential information	Figure 14	Moderate	Unlikely	Moderate
Revenue	SI sued by CE VO partner(s) for breach of NDA	Figure 26	Major	Rare	Moderate

Asset ID	Unwanted Incident	Diagram reference	Cons. Value	Freq. Value	Risk Value
VO participation Market share Revenue	SI expelled from CE VO	Figure 25	Major	Rare	Moderate
Revenue	SI sued by AirVO for breach of NDA	Figure 27		Unlikely	
AirVO project, Market share	AirVO terminates project	Figure 18, Figure 27			
Business plans	CE VO business plans disclosed to competitor	Figure 14, Figure 17			
Partner trust	CE VO business plans disclosed to competitor by SI employee	Figure 14, Figure 25, Figure 26			
AirVO project, Market share, Revenue	Loss of project to competing project proposal	Figure 17, Figure 18, Figure 19, Figure 32			
VO participation, Market share, Revenue	CE VO dissolved	Figure 18			
	Key SI employee not allowed to work on project	Figure 32			
	Confidential information leaked to third party	Figure 28			
	Unclear who owns newly developed IP	Figure 34			
	Unclear to what extent newly developed IP can be utilised in future projects	Figure 34			
	Former employee uses SI know-how for competitive purposes	Figure 20			
	SI target of lawsuit as largest CE VO partner	Figure 35			
	SI found liable for misuse of 3rd party IP by other CE VO partner	Figure 35			

Asset ID	Unwanted Incident	Diagram reference	Cons. Value	Freq. Value	Risk Value
	CE VO partner uses SI confidential information for competitive purposes	Figure 29			
	Competitor gets access to SI confidential information	Figure 19			
Client trust	Customer requirements disclosed to competitor	Figure 15, Figure 21			
	Air VO confidential information disclosed	Figure 27			
Requirements	Customer requirements no longer exclusive	Figure 15, Figure 21			
Market share	Use of SI know how to compete with SI	Figure 23, Figure 30	Moderate	Possible	Major
Revenue	Use of SI know how to compete with SI	Figure 23, Figure 30	Moderate	Possible	Major
Market share	Use of SI know how to enter SI's market niche	Figure 30	Major	Unlikely	Major
Revenue	Use of SI know how to enter SI's market niche	Figure 30	Major	Unlikely	Major
Market share	SI competitor acquires MyInterLink		Moderate	Unlikely	Moderate
Market share	SI competitor acquires MyAvio		Major	Unlikely	Major
Integrated design	AVO partner acquired by or merges with competitor	Figure 31	Minor	Unlikely	Low
Trade secret (e.g., analysis report, analysis data)	SI confidential information disclosed to SI competitor	Figure 24, Figure 31			
Revenue, VO participation	SI unable to fulfil its obligations	Figure 33			

5 Risk Treatment

This section presents the results of the treatment identification session performed in London (January 28th).

In principle, the legal risks identified in section 3 above can be treated either proactively (prior to the occurrence of the unwanted incident) or reactively as a reaction to the incident. Laws provide a number of reactive treatments and legal action. However, most reactive treatments are in practice often rather inefficient, since they often involve a legal dispute that takes time, costs considerable amounts of money and is uncertain with respect to both its outcome and the degree to which a loss is really compensated. Hence, we have focused on proactive treatments that seek to avoid reduce the likelihood of the incident.

In the following section the treatments are categorised according to the three main areas addressed by TrustCoM, i.e. trust management, security management and contract management. This was done in order to facilitate the implementation of some of the results in other parts of the project.

An alternative approach would have been to group treatments that relate to a specific risk or risk category. However, one risk or risk category may require a variety of treatments and one treatment may reduce the likelihood of more than one of the identified risks. Another alternative would be to categorise the treatments into treatments that clearly fall into the legal domain (e.g. a specific contract clause) and treatments that relate to other (non-legal) domains. However, the stakeholder will be more interested in an integrated but effective treatment than in a treatment strategy where each sector is treated separately.

Consequently, the treatments reviewed in the following subsections should be understood as integrated in several ways: First, some trust management issues and some security issues may have to be included in the VO contract in order to be effective. Second, trust in the VO contract partners may play a role with respect to contractual provisions and with respect to special security measures that could be required. Third, security measures may depend on the degree to which the VO partner is trusted and some particular security measures may be implemented because they are contractually required.

5.1 Trust Management Treatments

Methods from trust management may be applied in order to reduce the likelihood of some of the legal risks outlined above. Note however that there is, from a legal perspective, a major difference between trust management prior to entering into a contract, and trust management once a general VO agreement is established. Once the contract is a fact, any type of trust management (e.g. reducing access rights of a VO partner who is no longer considered as completely trustworthy) has to be backed up by the GVOA or applicable law. This is contrary to the pre-

contractual phase, where the parties in principle[23] are free to decide if they want to enter into a contract, who should be the contractor and what should be the content of the contract. Consequently, there is a much greater freedom to apply trust management measures during the pre-contractual phase (VO identification formation), compared to the contractual phase (VO operation and dissolution).

5.1.1 VO identification and formation phases

With respect to the legal risks related to trade secrets, trust in the VO partners is a crucial issue.

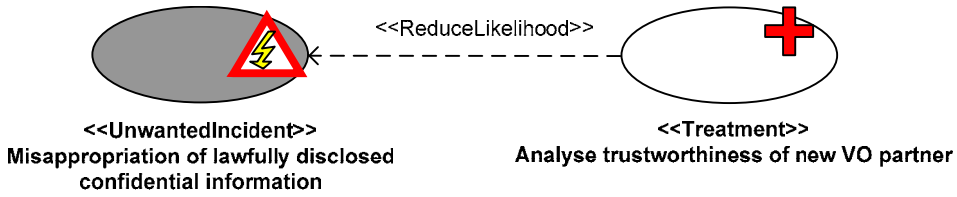

Figure 36 Analyse trustworthiness of new VO partner

The most general treatment would be not to collaborate with a potential VO partner who is not trustworthy with respect to the confidential information that will be shared. This is a direct consequence of the rather limited legal protection of confidential information and trade secrets. Once confidential information is leaked to the public, to a competitor or to a malicious third party, there are few effective legal remedies. In many cases it may not be feasible to prove who has disseminated the information, which would be necessary for any claims for damages. Furthermore, it is difficult to assess ex ante if the amount to be recuperated through reactive legal measures will be equivalent to the economic loss. This will particularly be the case if the person or organization responsible for the leakage does not have the economic means to compensate for the loss.

Assessing the trustworthiness of a potential VO business partner will therefore involve a number of different issues. In particular, a potential VO partner may not be regarded as trustworthy, if its previous conduct shows that this partner has e.g. leaked or misappropriated confidential information. Presumably, the availability of this type of specialized information is probably rather low. One may therefore take recourse to other kind of more general information about the trustworthiness of a party. However, it is questionable whether a very general statement (e.g. like the ones used in eBay) is sufficiently specific to be used for assessing the trustworthiness in this type of collaborations. For some commercial actors (take Coca-Cola and their recipe as an example) their confidential information is their most valuable asset, which will not be entrusted to any business partner without closer checks. In this context, financial information based on the creditworthiness of the potential VO partner may be of some relevance, since it can provide an

[23] Note however that many laws foresee pre-contractual duties, based on good faith and fair dealing. Moreover, a number of pre-contractual notes and preliminary contracts may be in place to rule this phase. For a more detailed description of this phase see ALIVE IST Project *VE Model Contracts, Deliverable D 17a* (2002).

indication for possible financial difficulties, which may motivate an unwanted behaviour. Credit information may also be relevant to assess whether the partner may be able to provide compensation in case it causes significant losses.

If we assume that the assessment of the collaboration partner's trustworthiness is positive, the next issue to assess would be if the prospective VO partner is a competitor or if it has close relations with a competitor. This has to be assessed with a view to the particular set of confidential information which will be communicated or shared during the VO lifecycle. If the confidential information is of any direct value to the prospective VO partner for other commercial activities outside the VO, then one should consider to either refrain from the collaboration with this entity or to include rules in the contract on the lawful use of this information (e.g. based on a license fee or based on the mutual exchange of confidential information of equal value).

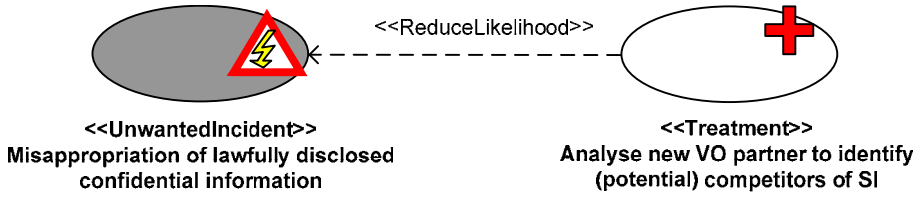

Figure 37 Identify (potential) competitors

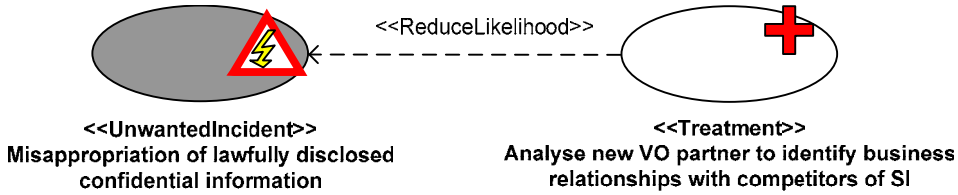

Figure 38 Identify business relationships with competitors

5.1.2 VO operation and dissolution phases

During the VO operation and dissolution phases, the possibilities for trust management are limited by the binding contract that obliges the VO partners to co-operate. Hence, if the VO partners want to use trust management measures during the operation phase, it is advisable to specify these in the contract (see further below in section 5.3.3).

Even though the VO partner itself is not a competitor, it may have close relations with competitors, e.g. in other similar projects or VOs, which may require more specific precautions. We should also note that such relations may evolve over time. For example, a VO partner could be acquired by a competitor or it could be in the process of merger with a competitor (see also operations phase below).

A certain monitoring of the VO partners' trustworthiness may thus contribute to reducing the risk of SI's confidential information being disclosed to a third party or being misappropriated. In principle, both the conduct of the VO partner organizations and the behaviour of individual employees working with a VO partner could be monitored.

However, it is challenging to identify those aspects that may effectively indicate changes in the trustworthiness. A number of factors, e.g. timeliness of payments to VO partners, may be relevant for the general trust level, while they say little about the trustworthiness with respect to entrusted confidential information. Thus, there should be a reasonable relation between the factors that indicate the trust level and the consequences or sanctions that are related to a lower trust level. In the context of protecting confidential information, the monitoring should therefore concentrate on those relevant factors. These include on the one hand factors that directly affect the cooperation between the VO partners, like the breach of security obligations and SLAs, and on the other hand changes in a VO partner's relation to third parties, e.g. corporate changes that involve a competitor.

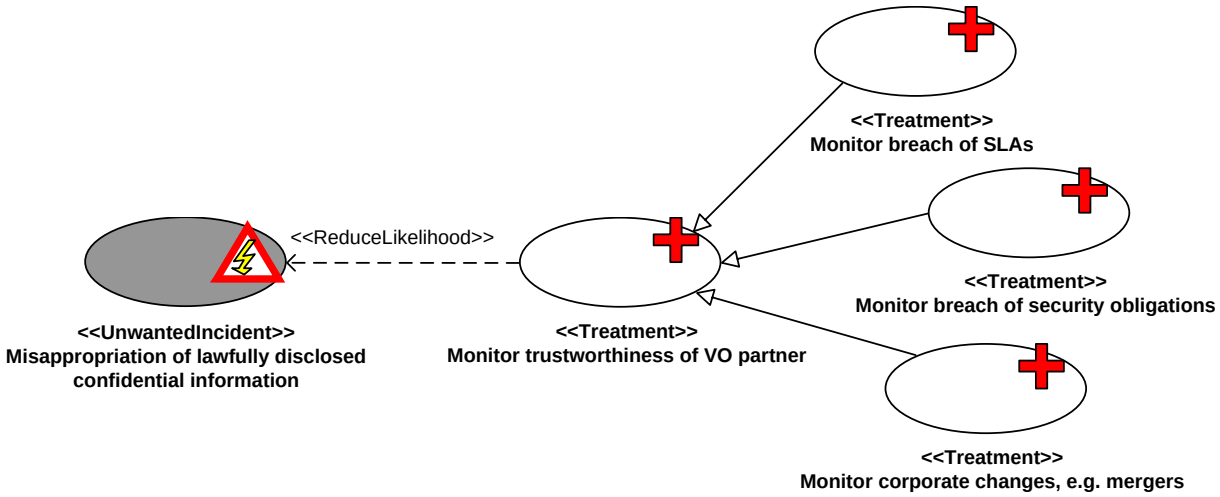

Figure 39 Monitor trustworthiness of VO partner

If certain corporate changes (like merger with or acquisition by a competitor of a VO partner) should have consequences for a partner's access to confidential information, this could be included in the contract.

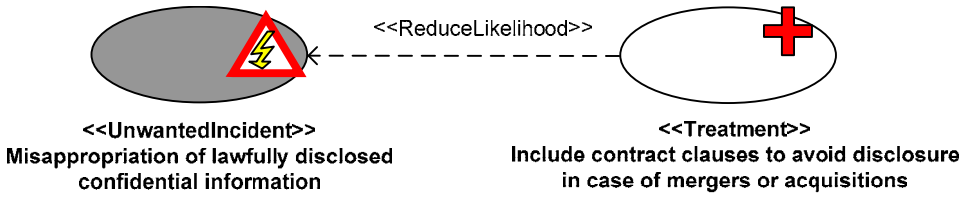

Figure 40 Include contract clauses regarding mergers and acquisitions

Monitoring employees is directly related to a contractual obligation of all VO partner organisations to impose confidentiality obligations on their employees. Monitoring the VO partners' employees could thus contribute to an enhanced protection of confidential information and trade secrets. In particular, user accounts could be monitored in order to detect behaviour that is not related to carrying out work for the VO. However, there are certain privacy and data protection limits to such monitoring, which could involve the processing of personal data. From the privacy and data protection perspective it may be advantageous to be open about the fact that some activity is being monitored.

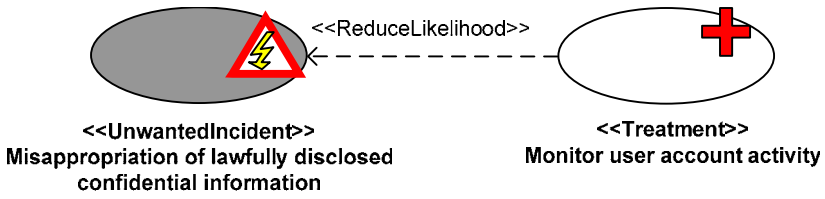

Figure 41 Monitor employee trustworthiness

5.2 Security management treatments

Security management plays an important role with respect to the protection of confidential information and trade secrets from misappropriation and disclosure. The objective of the following section is not to point out the specific security measures to be applied in this scenario or to be implemented by TrustCoM. Instead, we aim to review some security measures in order to highlight their role in solving some of the identified legal issues. If these measures are available and effective, their implementation in the TrustCoM framework could solve some of the legal risks identified in the analysis of the CE scenario. It is of course up to other TrustCoM WPs to decide whether or not these measures are available and effective.

From a legal point of view, the TrustCoM framework should ensure that adequate security measures are in place, that effectively reduce the likelihood of confidential information or trade secrets either being disclosed to third parties (including competitors and the public) or being misappropriated in the sense that the information is used by a VO partner in a way incompatible with the VO contract.

Possible measures include:

- Role-based access control: Access to particularly sensitive shared resources should be granted on a need-to-know basis, in terms of relevant information that must be accessible in order to carry out work for the VO.

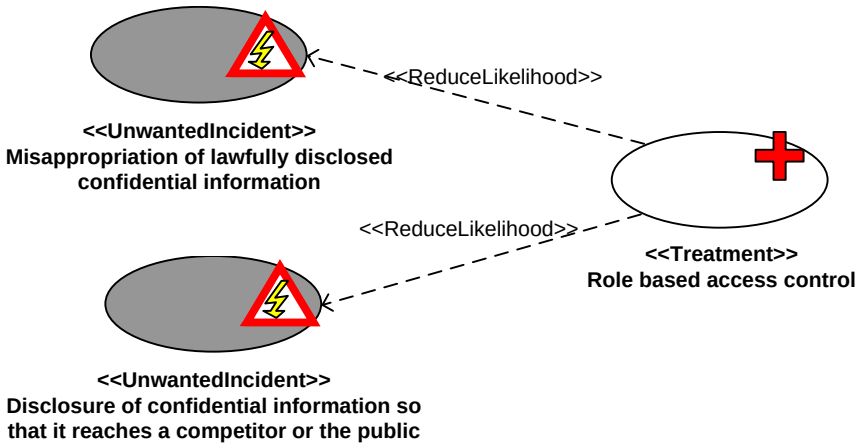

Figure 42 Implement access control

- Different security levels: Different sets of information may require different security levels, in order to ensure the effective protection of particularly sensitive information and to make sure that the handling of less sensitive information is not hampered by unnecessary security procedures.

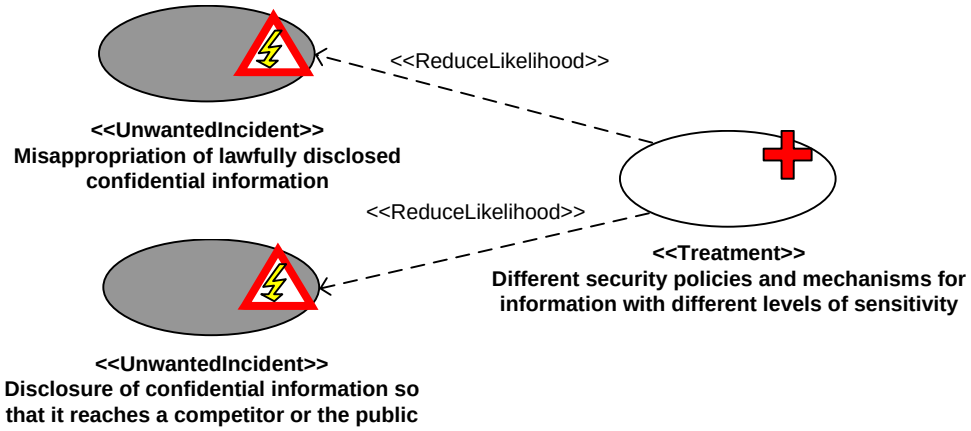

Figure 43 Different security levels

- More advanced access control, e.g. Multi-Level Security: The objective of a Multi-Level Security (MLS) system is to handle information at a variety of sensitivity levels without disclosing information to an unauthorized person. In theory, a "MLS device" will automatically enforce those restrictions. A device achieves its MLS objective if it can't be induced (accidentally or intentionally) to release information to the wrong person. This is meant to solve problems such as malicious (authorized) users being able to leak classified information or an innocent user being tricked into releasing classified information if subjected to a virus or other malicious software. MLS

is also referred to as *mandatory access control* because it is always enforced and users can not disable or bypass it. [24]

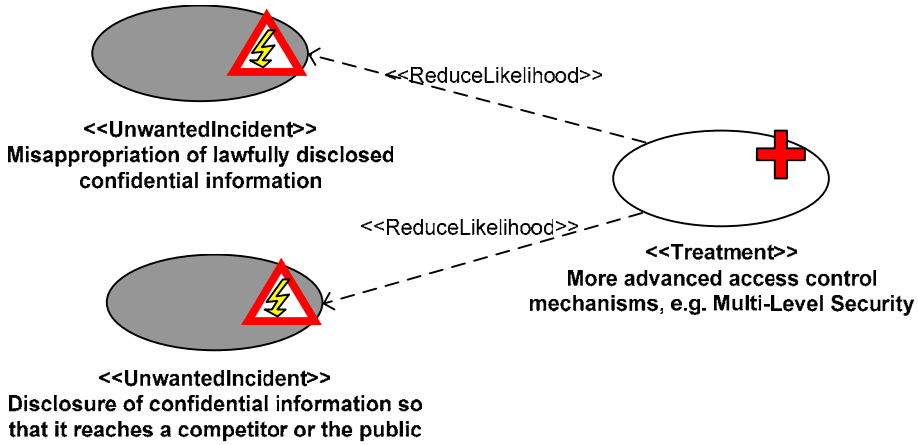

Figure 44 Use more advanced access control, e.g. MLS

- Certification of security level: A security certificate issued by an independent third party may be an important indication of the ability to fulfil security requirements.

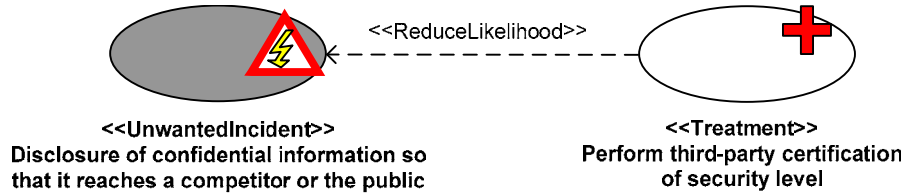

Figure 45 Certification of security level

- Monitoring user account activity and breach of security obligations. As mentioned before, the breach of security obligations may have consequences for trust level and lead to contractually prescribed consequences and sanctions.

[24] Multi-Level Security: http://www.smat.us/crypto/mls/

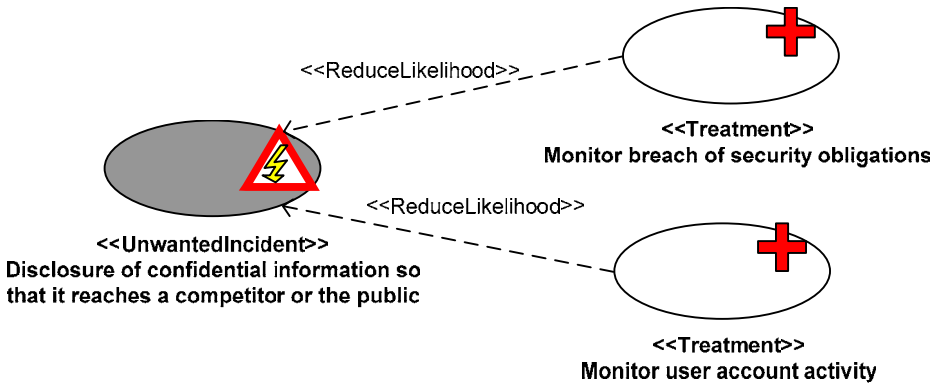

Figure 46 Monitor security

- More specific security measures may also be put in place with respect to members of the Analysis VO. For example, in relation to the HPC provider one could require that no other applications are allowed to run on the same system during computation to reduce the likelihood of malicious software running on the same system acquiring confidential information.

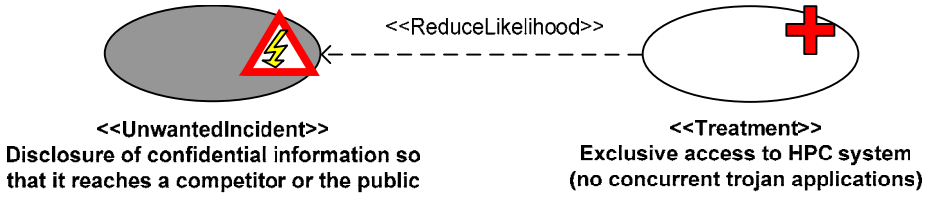

Figure 47 No other applications allowed to run on the same HPC system during computation

- DRM technologies: From a legal point of view, it would be useful if some elements of enterprise DRM technologies could be utilized. This could be done at two different levels: First, metadata could be used to indicate who owns a particular set of information, what level of confidentiality is foreseen for this information, what are the conditions of accessing and using this information, etc. The second level would be to not only to provide information about such limitations, but also to enforce them by inhibiting use of this information in a way that conflicts with the GVOA or other VO agreements. Whether or not such technologies are efficient and/or available is up to other TrustCoM WPs to determine.

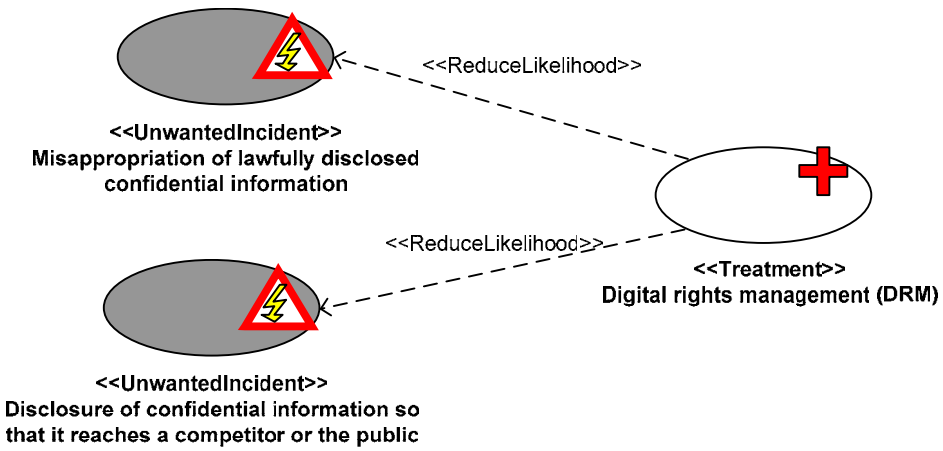

Figure 48 Use DRM technologies

5.3 Contract management treatments

The contract management issues discussed below relate to the content of the contract, not the way the contract is established or monitored. The above mentioned legal risks can be treated by including or further specifying a number of contractual rules.

5.3.1 Contract Rules Related to IPR

5.3.1.1 Who holds project IPR?

The ownership of newly created IPR may be an issue both for the internal relations within the core CE VO and for the relations to the Analysis VO and its integrants.

First, since the collaborative work in the CE VO may generate results which can be protected by IPR, it is advisable that the parties clarify who will own these rights. This general issue was already addressed in ID 6.2.2, section 3. The ALIVE template includes a clause according to which the parties have to discuss the protection for project technology during the operation of the VO. Since it may be

difficult if not impossible to identify more specifically what kinds of project IPR will be produced, this approach seems reasonable for the CE VO.

Second, since the work of the AVO may have results that can be protected by IPR (e.g. possibly the analysis report), the contract between the members of the CE VO and the members of the A VO should prescribe that all IPR generated during this work is assigned to/transferred to the members of the CE VO.

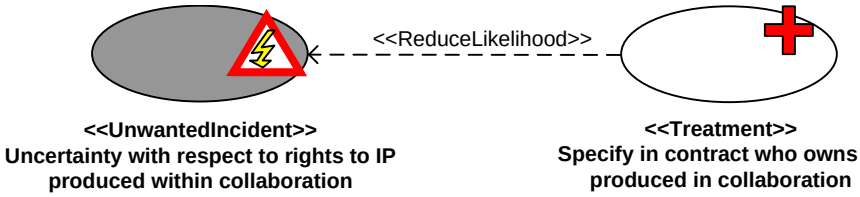

Figure 49 Specify ownership of produced IP

5.3.1.2 Access Rights

The above analysis revealed a risk that SI will not be able to fulfil its obligations due to its lacking access to a partner's confidential information which is necessary to carry out the project efficiently. This risk can be reduced by including a contract provision that allows VO partners to access such information which is necessary to enable the VO to carry out the project.[25]

5.3.1.3 Disclosure and Use of Confidential Information

As mentioned above in section 2.5.1.1, the GVOA will include a confidentiality clause. Such clauses regulate the disclosure and possibly the use of confidential information disclosed in the VO context.

- Disclosure prohibition: This prohibition may relate to any information disclosed in the context of the collaboration or it can refer to a specific set of information that is described more precisely. In particular, the prohibition can be limited to information that is disclosed as confidential. In a digitalized context this would refer to information that is marked in a particular way as confidential, e.g. by including the information in a certain file or by adding meta-information stating the confidentiality status.

[25] See Alive VE agreement template, section 8, ALIVE IST Project *VE Model Contracts, Deliverable D 17a* (2002).

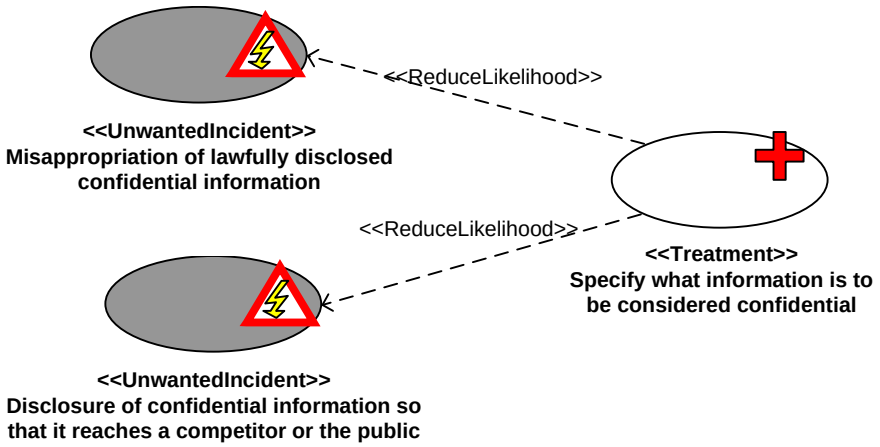

Figure 50 Specify which information is to be considered confidential

- Permission to disclose: On the other hand, partners must be permitted to disclose confidential information internally when carrying out work for the VO. Furthermore, the disclosure to a third party should be expressly permitted in case of a binding decision by a public authority (e.g. a court decision), if the owner of the confidential information has been given notice and a possibility to stop the disclosure by legal means.
- Non-use: The GVOA should also contain rules about the use of confidential information that is disclosed to VO partners during the operational phase. It is clear that the use of confidential information for project purposes should be allowed. However, the parties should also determine whether or not confidential information belonging to a partner can be used for other purposes outside the project. This refers both to pre-existing know-how, know-how created separately by a VO partner and to know-how created by one or more VO partners in relation to carrying out work for the VO. One option is to rule that confidential information (including know-how and trade secrets) disclosed in the VO context may not be used in other contexts by the VO partners. From the point of view of the SI, there are few if any reasons why it should allow the other VO partners to use disclosed information for other purposes. Hence, the CE GVOA should prohibit the use of disclosed confidential information for purposes outside the VO collaboration.

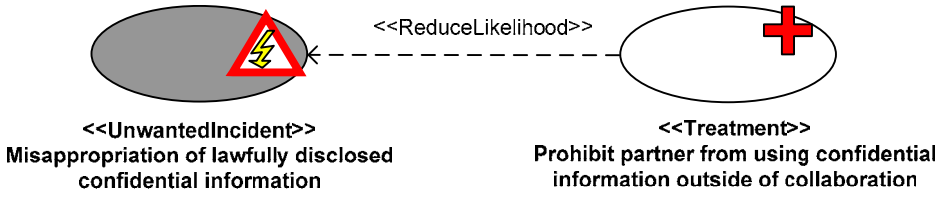

Figure 51 Limit use of confidential information

- The above mentioned restriction with respect to the use of confidential information may be difficult to police in some cases. Then, the parties may wish to allow the use of (all or a defined set of) disclosed confidential information, for which a license fee is paid.

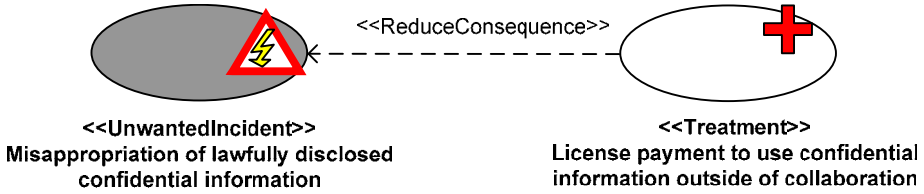

Figure 52 License payment for use of confidential information

- If the parties know that the information that will be disclosed during the collaboration is of equal value, they may consider mutually allowing the use of this information, which will however still have to be kept confidential.
- If the confidential information to be disclosed in relation to the VO is particularly sensitive, a party may even limit the possibility of a VO partner to engage in a similar project, where the same confidential information could be used by a competitor. This prohibition could also include employees, prescribing that those employees who participate in the VO are not allowed to participate in other similar projects (Figure 53). From the perspective of the SI, this could be an effective measure to prevent confidential information from being misappropriated.

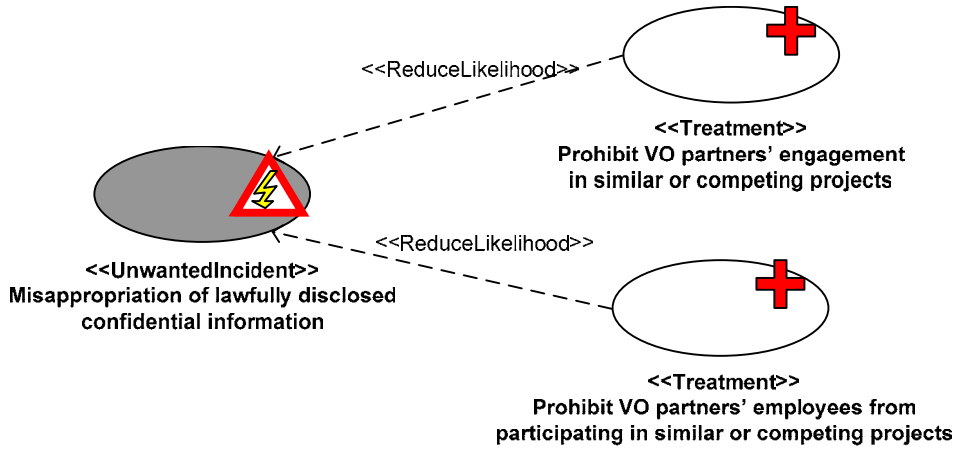

Figure 53 Prohibit engagement of VO partners or specific employees in competing projects

- As indicated above in section 3.1.4, there is a risk that a too restrictive confidentiality clause may limit SI's possibilities to engage in future similar projects or to assign specific employees to such projects. However, it is more likely that such a restriction would affect the smaller partners involved

in the CEVO. Nevertheless, if such a rule was considered a significant limitation for future other engagements, it should not be adopted.

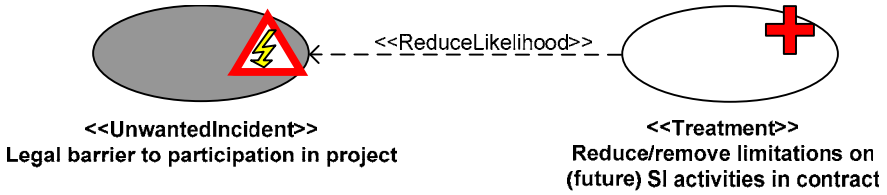

Figure 54 Remove limitations on (future) endeavours

5.3.1.4 VO Liability for IPR Breaches Caused by VO Partner

As mentioned above in section 3.2.2, there is a certain risk that SI may be the target of a legal reaction to an IPR breach caused by another CE VO member. This is in fact a general liability issue, which however is relevant also for IPR breaches. The consequence of this risk could be reduced by two contractual provisions which both are included in the ALIVE template[26]. First, the GVOA should provide that each partner is liable for obligations towards other parties in accordance with this partner's fault. Second, if one partner has compensated a third party for the VO's breach of third party rights, this partner may exercise a right of recourse against the liable party or parties.

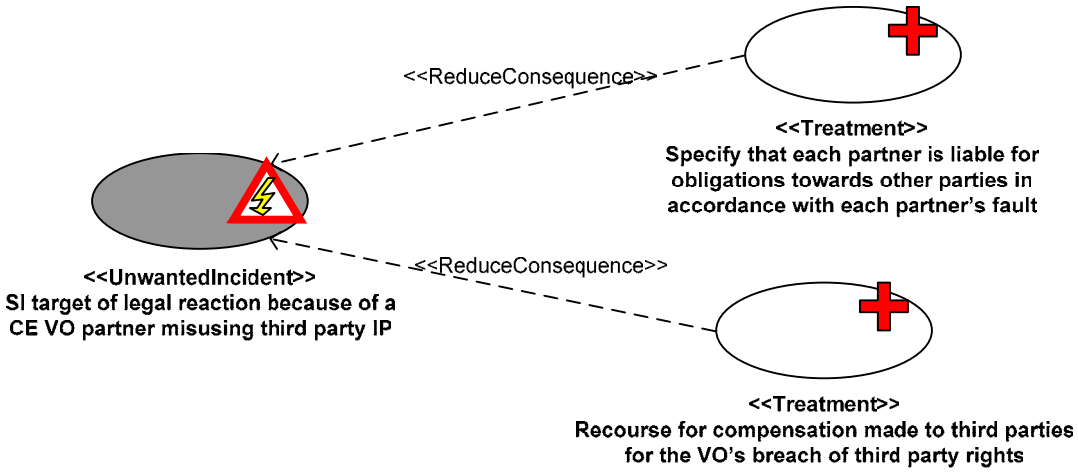

Figure 55 Specify liability obligations and recourse

5.3.2 Rules on Security Requirements

Both the CE VO internal general VO agreement and the agreement between the CEVO and the AVO should include specific rules about information security. The

[26] Both provisions are included in the VE Agreement template, Section 11, ALIVE IST Project *VE Model Contracts, Deliverable D 17a* (2002).

following section outlines some security measures that may contribute to limiting the risk of confidential information being disclosed or misappropriated.

- Particularly the agreement between the CE VO and the AVO should include provisions limiting the storage time for certain information (e.g. analysis data), and a duty to delete data when the analysis is completed.

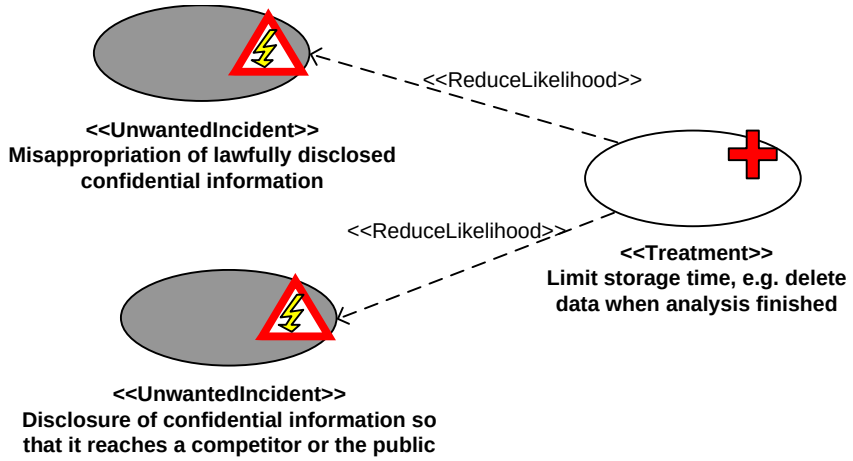

Figure 56 Limitations on storage time

- Certification of security level: A security certificate issued by an independent third party may be an important indication of the VO partner's ability to fulfil security requirements. The contract may require that partners provide such certificates prior to getting access right to shared confidential information.

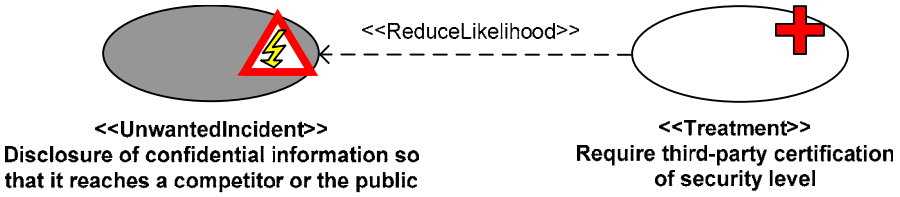

Figure 57 Require certification of security level

- The contracts may include restrictions on which personnel are allowed to access and process (confidential) VO related information. If the confidential information is particularly sensitive, one may even want to specifically list the persons who will have access to certain information.

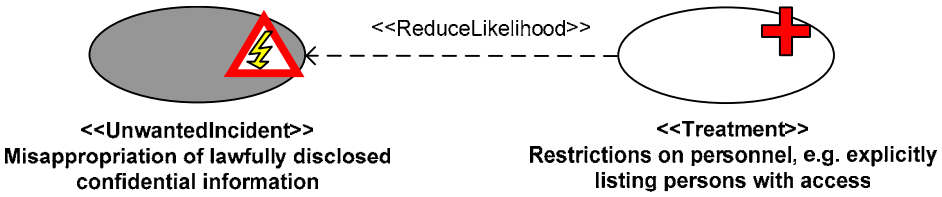

Figure 58 Restrictions on personnel

- The contract may also include restrictions on the computer system used to access and work with the information, e.g. which operating system to use, which software is allowed on the system or requirements for anti-virus and firewall software.

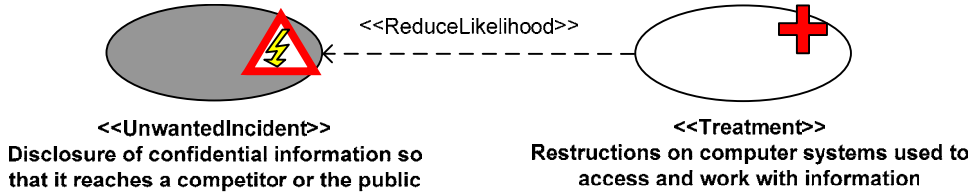

Figure 59 Restrictions on systems used to access information

- The contract could also provide rules about the physical security level required from a VO partner.

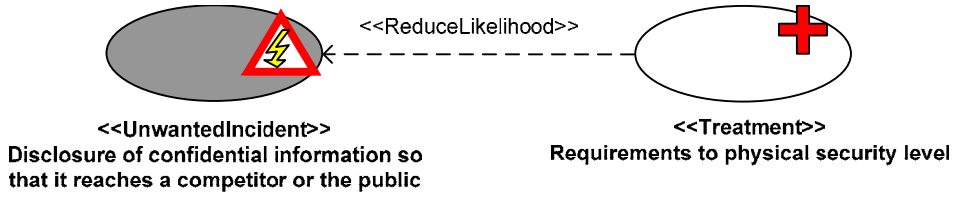

Figure 60 Physical security requirements

5.3.3 Rules on Trust Management

During the VO operation and dissolution phases, the possibilities for trust management are limited by the binding contract that obliges the VO partners to co-operate. Hence, if the VO partners want to use trust management measures during the operation phase, it is advisable to specify these in the contract. In particular, the contract could include a number of conditions that will be considered as an indication of a partner's lacking trustworthiness (e.g. breach of security obligation x) and the consequences or sanctions that can be adopted in these cases (e.g. the suspension of the VO partner's access to certain resources). It is particularly important that there is a reasonable relation between the incident that indicates the lower trust level and the consequence or sanction this may have. For example, an unjustified delay in effectuating a payment to VO partners may generally indicate that the partner is less trustworthy. However, this fact provides no indication of the partner's trustworthiness with respect to confidential information, and it should not be used to justify the suspension of access to shared information resources.

This contractual rule should be included in order to avoid claims by a VO partner affected by such sanctions, alleging that its performance in the VO was being jeopardized by the other parties unlawfully applying sanctions.

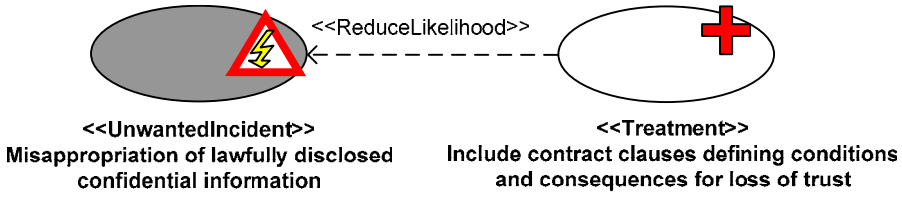

Figure 61 Include contract clauses dealing with loss of trust

Moreover, the contract should include some procedural rules both for the adoption of such measures (by humans, e.g. by the executive committee) and for the resolution of related disputes. In particular, the partner affected by such a sanction should be able to take appropriate measures to have an unjustified sanction removed. If sanctions are effectuated in an automated way, there should be a process in place to review and amend automated decisions, if solicited by one VO partner.

Some of the trust-relevant factors may be so important that the VO partners may not be willing to continue the cooperation. If possible, such factors should also be included in the GVOA. One factor that was identified above is the relation of a VO partner to a competitor; in particular the possibility of corporate changes that involve a close cooperation of one VO partner with a competitor of another VO partner or a competitor of the VO itself. The GVOA could foresee that the agreement may be renegotiated in such cases and that the partner involved in the corporate change may be replaced.

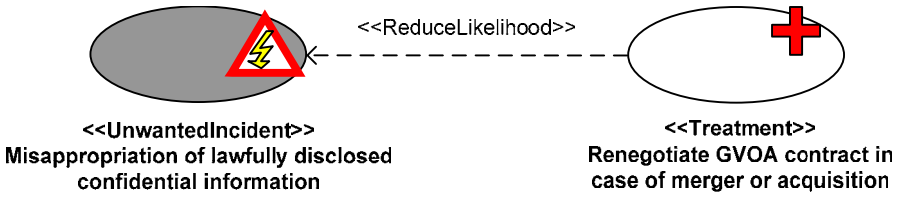

Figure 62 Renegotiate contract on merger or acquisition

5.4 Treatment Evaluation

Once treatment options have been identified, the treatments are evaluated with respect to their usefulness. The degree to which the treatment reduces the level of risk is determined, and a cost/benefit analysis is performed. Due to the limited time available during the workshop, we did not perform a treatment evaluation for this analysis. However, Table 13 shows an example of the kind of result one would get from this activity. Based on these results, the treatments can then be prioritized and implemented based on the available resources.

Unwanted incident	Asset	Treatment	Risk reduction	Cost/Benefit
Customer requirements disclosed to competitor	Client trust	Monitor user account activity	Major -> Moderate	Low
Customer requirements disclosed to competitor	Client trust	Restrictions on personnel	Major -> Moderate	High
Know how or trade secret enters public domain	Partner trust	Monitor user account activity	No	N/A
Know how or trade secret enters public domain	Partner trust	Role based access control	Major -> Moderate	Medium
Know how or trade secret loses legal protection	Partner trust	Monitor user account activity	Major -> Moderate	Low
Know how or trade secret loses legal protection	Partner trust	Role based access control	No	Medium

Table 13: Treatment evaluation

6 Concluding Remarks

We have presented results from the analysis of a collaborative engineering VO scenario, where a number of legal risks and treatments were identified. Our risk analysis results indicate how legal risks, such as the loss of protection of confidential information, can be treated by an integrated solution, including contractual elements, trust management and security management. Interestingly, many of the relevant contractual treatments were also included in a general manner in the ALIVE contract template for VOs (ALIVE 2002a). The performed legal risk analysis provided indications about how these rules can be adapted to the specific scenario. Since the graphical representation implies a simplification, a lawyer would have to integrate analysis results into the contractual document in an appropriate way, taking into account the terminology and the system of the contractual template.

The analysis results were generated during a number of brainstorming sessions involving participants with varied backgrounds, including law, informatics, economics and philosophy. Based on our experiences, the graphical models can indeed facilitate the communication and understanding with respect to legal issues in a multidisciplinary context.