Agreement title	**KIS4SAT: European Innovation Platform for Knowledge Intensive Services in the Satellite downstream Application Sector**
Project acronym	**KIS4SAT**
Agreement ref. No	**ENTR/CIP/07/C/N04S00-4**

D14: IPR Manual for SAT KIS Ventures

Due date of deliverable: 31st January 2010

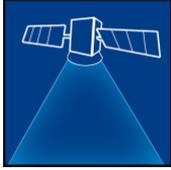Actual submission date for internal review: October 17-th 2008

Start date of project: 01st February 2008   Duration: 36 months

Authors: Vincent Morfouace, Tiziana Pagano (TECHNOFI)

Revision [V6]

Nature:		
R	Report	X
O	Other	
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

ACKNOWLEDGEMENTS

---

[1] GJU stands for Galileo Joint Undertaking

GLOSSARY

"ESA" is the European Space Agency

"IP" stands for Intellectual Property in the broad meaning. It includes any kind of protection measure, either formal or informal, that helps securing human intellectual creation.

"IPR" stands for Intellectual Property Rights. It is meant any kind of formal protection of human intellectual creation.

"KIS" stands for Knowledge Intensive Services. It is meant services involving science-based and technology-based innovations, commercial and business model innovations.

"RTD" stands for Research and Technical Development and designate the related activities.

"SIS ICD" stands for Signal In Space Interface Control Document

"SME" stands for Small and Medium size Enterprise, as defined by the European Commission (see http://ec.europa.eu/research/sme-techweb/pdf/sme-definition_en.pdf).

Value-Adding SMEs are SMEs that work with raw or semi-processed data from remote sensing instruments, and convert the data into information that brings value to end-users

Value-Adding Services (VAS) are defined as any business process meeting any of the following criteria:
- enhancing or upgrading the space signal;
- targeting specific end-users with dedicated applications;
- combining several applications at once.

TABLE OF CONTENT

1 INTRODUCTION

This Manual is a tool to be used by innovation experts willing to support SMEs offering services using satellite data, but also by these very same SMEs.

The targeted service SMEs are the ones operating in the Downstream Value-Adding sectors of space–based applications, as shown in the exhibit below.
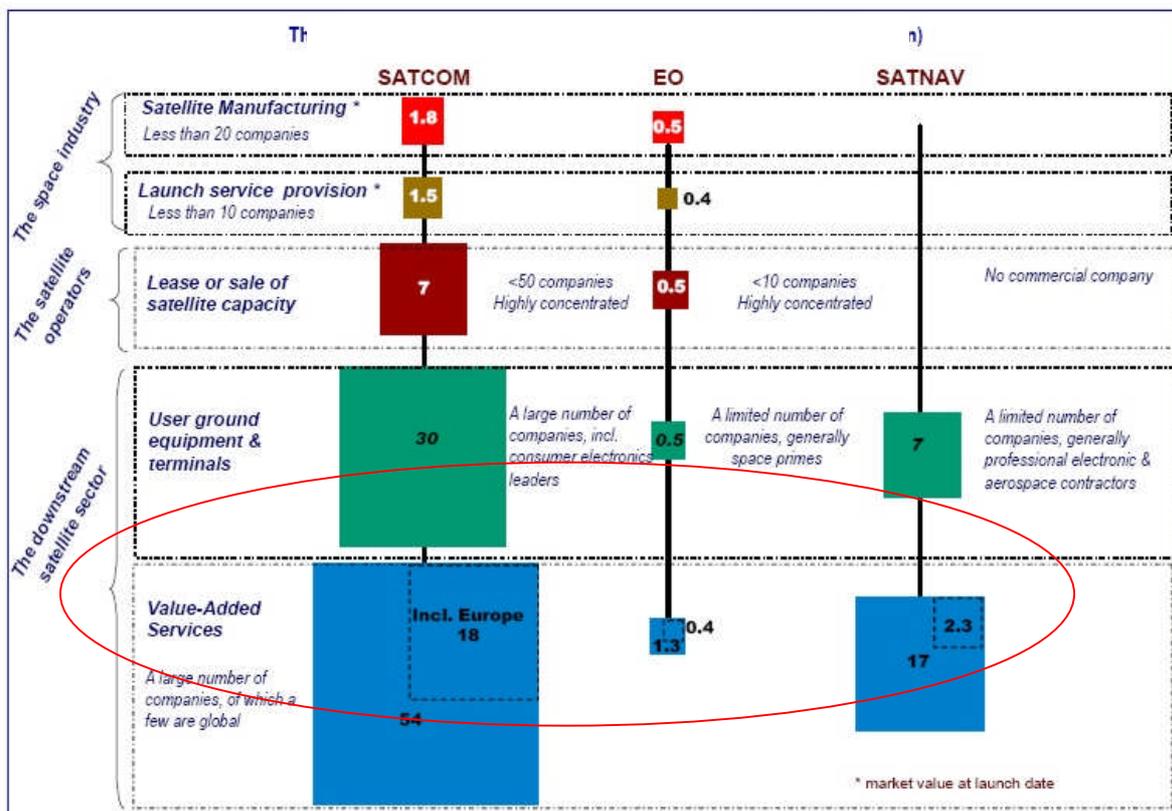
Source: Role & Impact of Dual Use Technologies, Symposium on Aerospace Technologies and Applications for Dual Use, Rome, 14 September 2007

Exhibit 1**: The three value-chains in commercial satellite applications in 2005 (EUR billion)**

The targeted innovation experts are:

- public bodies, such as Innovation Agencies, Space Agencies, Incubators, Chambers of Commerce, etc…

- private bodies, such as Space focused Clusters, Professional Associations, Innovation management Consultants, etc…
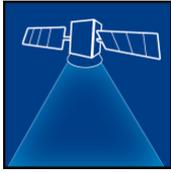
The Manual is organized in three sections:

1. The uses of IP management in SMEs providing value-adding services;

2. A review of the existing formal and informal intellectual property protections of relevance for these SMEs;

3. A set of recipes that can help company managers and/or innovation experts in providing their clients with appropriate options to implement coherent IPR policy.

The main sources used to produce this manual are listed in the "References" section at the end of the document. A key reference is reference [1] describing interviews performed amongst 300 SMEs in Finland and the UK in the framework of the ProACT project, which are the background of a report published by Pro-INNO[2]. A second important source was a report from the Galileo Joint Undertaking task force on IPR [5].

---

[2] Pro INNO is a European project co-funded by the European Commission, DG Enterprise & Industry, in the framework of the Europe INNOVA programme.

2 IPR MANAGEMENT IN SERVICE SMEs

2.1 IP protection in the SME population

The SME ecosystem is made of very heterogeneous groups of businesses that cover different sectors, growth strategies, degrees of innovativeness and a broad variety of IP strategies. Generally speaking, it is acknowledged[2] that the use of IPRs by SMEs is rather low. However, empirical research demonstrates that many SMEs have realised the value of their IP: they know how to manage such intangible assets. They use a wide range of informal as well as formal methods which aim at protecting their creativity and know-how. As a matter of fact, Intellectual Property Rights (IPRs), such as patents, trademarks and copyrights, represent only part of the IP management and protection practices used by SMEs.

Very often, SMEs are in a weak position to make use of IP rights, as the following business cases illustrate. Hence, SMEs are usually less likely to capture returns from their innovative efforts than large firms. Moreover, there is some evidence that the present segmented patent system neither fosters innovation, nor effectively protects the results of SMEs' innovation activities [7].

Business case 1	Business case 2
An SME files a patent about an innovative car suspension system based on composite materials.	An SME develops a sensor dedicated to medical applications in the heart surgery.
The industrial development requires cooperation with at least one car manufacturer. The SME signs a Non-Disclosure Agreement (NDA) with such a large company and presents the background gained by internal research and development.	It is patented and then manufactured by the company at small volume.
	A large world-based manufacturer copies the design and starts selling it worldwide.
The day after, the large company files a patent application on the very same idea. Patent reviewers refuse to accept the claims, because of the prior patent (whose application was not disclosed to the large car manufacturer). The SME is, therefore, protected against the infringing use of its creative knowledge. A license was granted by the SME exclusively to a foreign car part manufacturer (first tier contractor), who did not succeed in selling the technology to the car manufacturers.	The SME files a patent suit against the large company and starts bearing huge court expenses to fight against the infringer. At the same time, the company's sales slow-down. After 18 months of court battle, the SME wins, but the royalties paid by the big group do not cover the losses due to falling sales. The SME goes bankrupt.

Furthermore, approaches towards IPR management vary from sector to sector: this is shown by the different types of intellectual property practices and strategies. R&D-intensive manufacturing businesses appear to be the most active in using IPRs (especially patents).
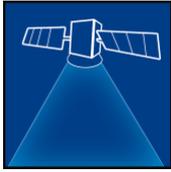
On the contrary, the awareness about different property rights protection methods and, hence, their utilisation in the service sector is relatively low compared to the manufacturing and software product sectors. Arguably, the low level of IPR utilisation in services reflects problems related to protection of intangible knowledge and to the novel business concepts developed by service companies. In addition, the multidimensional and often incremental nature of service innovation can lead to situations where formal IPR is of no use.

IPRs are therefore seen as irrelevant by many SMEs, which typically rely more on informal practices [6]. These protection practices are often simple, easy to control and affordable: to some extent, they are very often embedded in normal business working practices.

Metal and electronics industry

-Patents are commonly used

-Fairly good knowledge on IP-related issues

Software industry

-Rather negative attitudes towards patenting

-Speed of development and commercialisation is crucial

Knowledge intensive services

-Problems with IP-protection are recognised

-Use of copyrights and trade marks varies between firms

Formal protection

Informal protection

Exhibit 2**: A gross picture of IP protection practices by SMEs according to their core activity** (source [1])

Exhibit 2 shows that the IPR system (formal protection) is more important for SMEs operating in the metal or electronics industry. This is due to the strong industry tradition in using patenting. As a matter of fact, the IPR system itself has been originally developed to serve the product manufacturing industry.

Return on investment

| Patents Copyrights | Secret know-how | Trademarks Designs | IP |

| R&D | Manu-facturing | Marketing & Sales | Products |

Return on investment
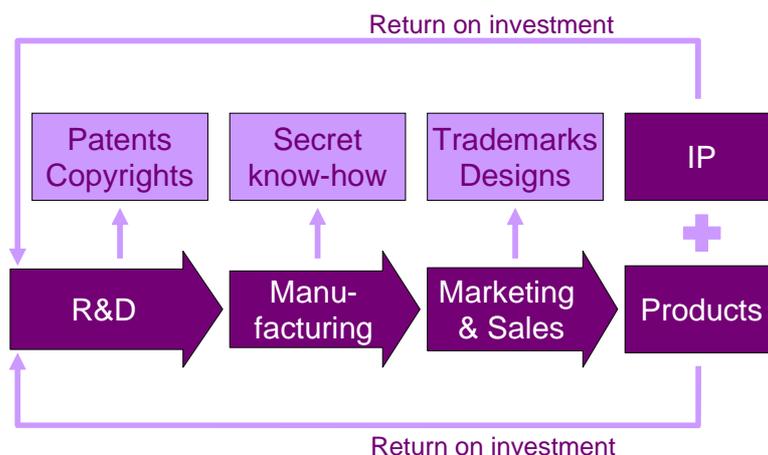
Exhibit 3**: Uses of IP protection in industry** (source [12])

In the software sector, patenting by SMEs is an issue: it is often used for marketing reasons and as a way to make sure that the firm's products are protected by its own patent(s),

thereby limiting the risk of violating other firms' protective rights. Things are moving at a European level to define patentable software. In terms of IP protection, the patenting process sometimes tends to be too slow to benefit businesses that are operating in a highly dynamic and rapidly developing business environment.

In knowledge intensive services, informal IP management and protection dominate. Although the importance of IP issues is well recognised, the nature of the intangible knowledge and innovations does not favour the use of a structured IPR system. However, the use of informal methods often leads to sophisticated practices.

The following section provides more insights into the informal IP management and protection practices of knowledge intensive service companies.

2.2 IP protection practices in Knowledge Intensive Service Companies

In Service Companies, and especially in Knowledge Intensive Service (KIS) Companies, knowledge and innovations are mainly intangible and typically co-produced by the supplier and the client within their contracting relationship.

IP management and protection are highly relevant for KIS companies since their core activity is knowledge co-production and innovative solutions development for their clients: KIS companies are known as carriers, sources and facilitators of innovation. Most service innovations are not patentable because of their intangible or, respectively, non-technical nature: existing formal methods of IP protection are then considered as irrelevant by service innovators. But still, effective IP protection is a significant motivation for innovation, and increasing service R&D highlights the need to protect on ever evolving IP. Moreover, is well-known that investors of all types prefer to invest in companies with strong IPR since, IPR are considered assets, representing a barrier to entry.

Besides formal protection methods (IPR), informal practices can also be an effective way of protecting and managing IP. Emerging informal protection practices are extremely heterogeneous in nature and they reflect a variety of needs among service businesses. The protection methods are either targeted to protect the business against internal threats, such as departure of the key personnel (methods like personnel committing, documentation and task swapping), or against external threats, such as competitors (methods like technical protection, fast innovation cycle and secrecy). Furthermore, some methods cover the risks related to co-operative relationships with external partners.
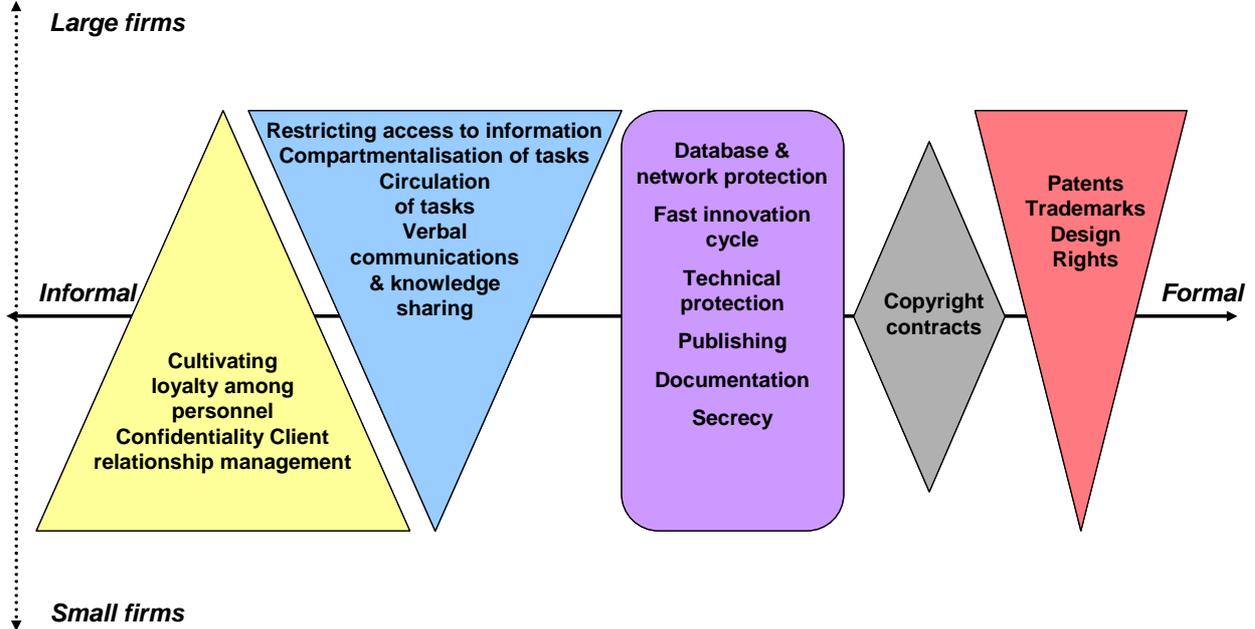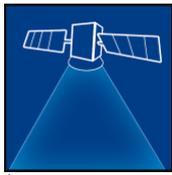
Exhibit 4**: Relative positioning of current IP protection practices on formal and informal aspects** (source [1])

It can be argued that the systematic use of both formal and informal methods may provide the optimum level of protection for the firm, using the positive aspects of both informal and formal protection practices.

The primary asset of KIS companies is mainly knowledge and intellectual[3] capital. Hence, service firms' production processes are often wholly dependent on the employees' knowledge and skills, the physical capital and tangible assets having a less significant role. In particular, when IP depends on tacit knowledge, formal protection methods cannot be used efficiently. Generally speaking, informal and formal protection methods of IP are not mutually exclusive or even competing with each other; rather, they are supporting each other in many different ways.

---

[3] Intellectual capital combines expertise and motivation
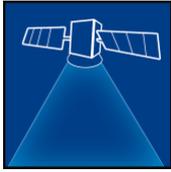
3 FORMAL, SEMI-FORMAL AND INFORMAL INTELLECTUAL PROPERTY PROTECTIONS

Exhibit 5 depicts the different types of IP protection that have been identified as used in KIS enterprises.
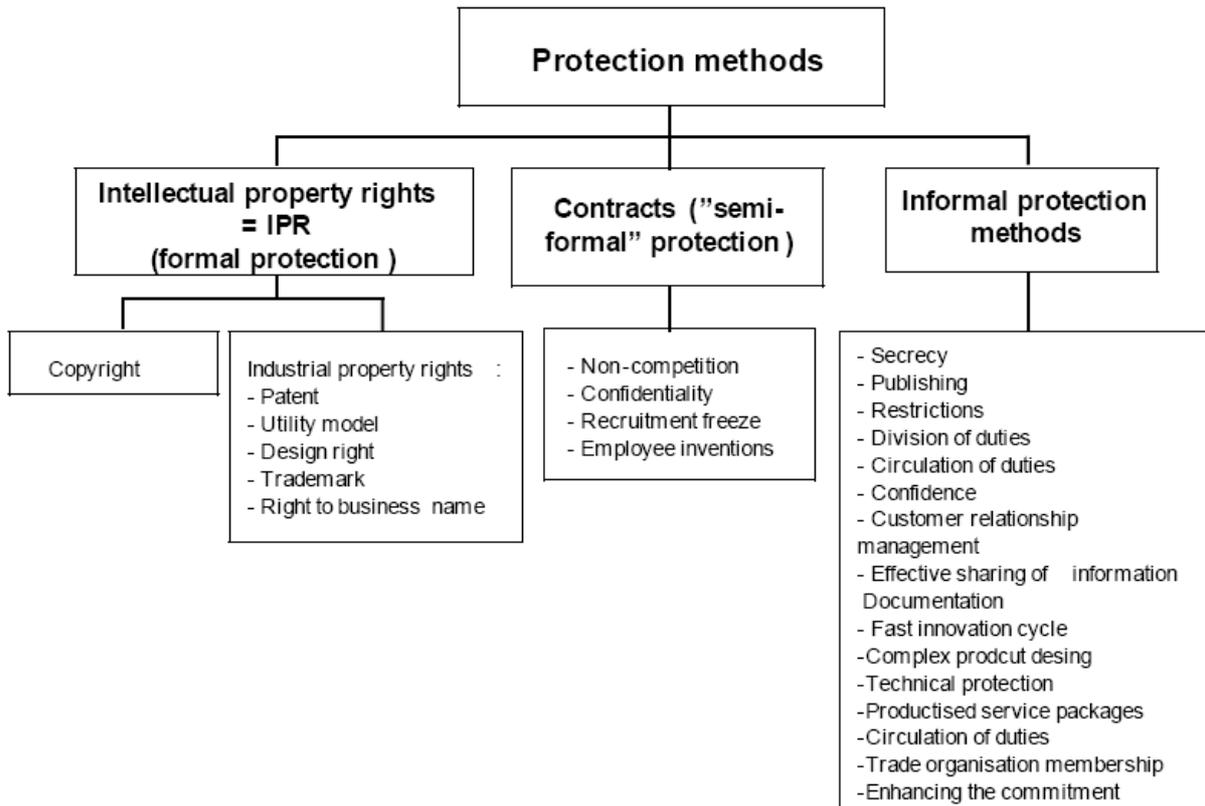
Exhibit 5**: Use of different IP protection types among KIS enterprises** (source [1])

3.1 Formal IP protection

Formal IP protection deals with legally recognised ways of obtaining a proprietary advantage (Rights) on the market, which leads to a time-limited monopoly for idea and innovation exploitations granted by a public authority, and a systematic publication. Formal IP includes the following protection tools.
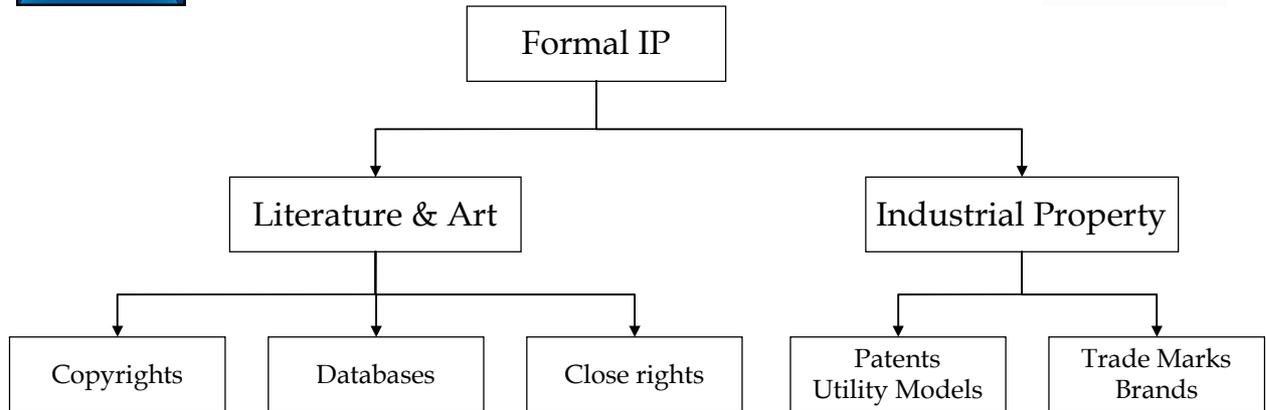
Exhibit 6: **Formal IP protection tools**

As previously underlined, IPR is poorly addressed by SMEs, and even less by KIS enterprises, as shown by a study based on a telephone survey of 300 Finnish and UK knowledge intensive service (KIS) businesses in three dynamic industries (software consultancy and supply, business and management consultancy activities and advertising agencies).
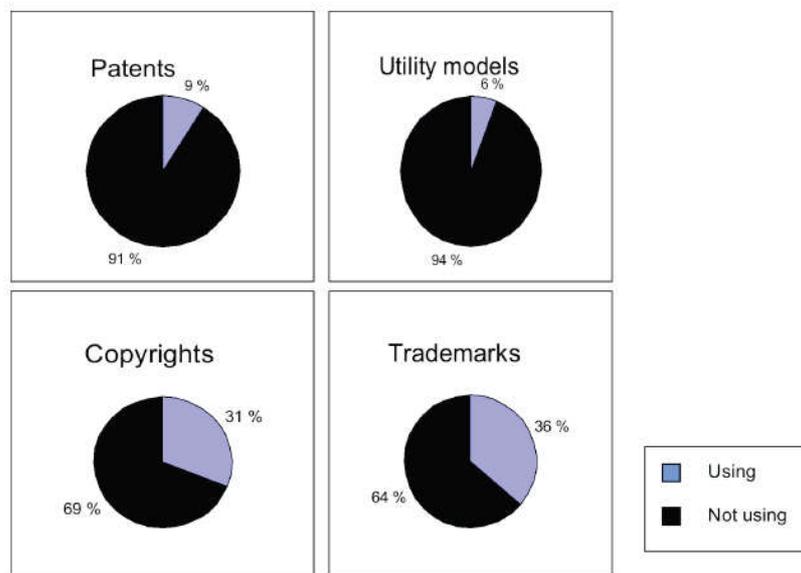
Exhibit 7: **Use of formal IPR among KIS enterprises in Finland and UK (source [1])**
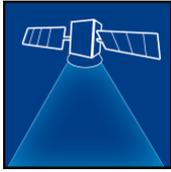
Today, the main formal IP protection used by KIS enterprises in the downstream satellite service sector are:

Databases	Databases are big amounts of numerical information stored for multi-purpose and multi-users utilizations.
	Satellite downstream services rely on space-based observation and in- situ data. Access contracts or licenses to data of guaranteed validity and continuity over time are therefore the basis for making business in downstream applications
Copyrights	They are used to protect intellectual creations (art, literature, fragrances, software encoding, etc…), which can be linked to their author by a self standing "signature"
Trade Marks	They are used to protect commercial names and logos, including their design
Secrecy	Secrecy, which prevents confidential information from being distributed to outsiders, is a widely used strategy in the EO sector value adding SMEs

However, service enterprises need more and more technological tools to deliver their services at the right performance and quality levels. For instance, final satellite applications always rely on the arrangement of a specific system architecture which might comprise innovative technological blocks to ensure the final service performance and differentiation: ranging from specific receivers to transmitters or local elements, they usually require hardware production with highly specific developments and frequent updates in regards with related technologies' evolutions. Specific R&D and engineering companies do operate to support sometimes the final service providers in building adequate system architecture and in selecting the best for value hardware components. Moreover, Service enterprises increasingly face a global economy, in a way similar to what the manufacturing industry does. Hence, they might be obliged in the next decades to think about IPR protection of their internal tools, software and/or brands.

IPR regarding access to space-based data and satellite infrastructures are carefully managed by the European competent institutions (ESA, EU Member States, etc…) together with the key industrial companies of the sectors and the related consortia developing the so-called KOPERNIKUS (ex-GMES) Core Services. Consequently, enterprises willing to commercialise satellite downstream services will have to conclude license contracts with providers of satellite data and products, which is semi-formal IP protection actually (see section 3.5 for the special case on access to data and products needed for KOPERNIKUS downstream services development).

A survey performed by the INVESAT project (2006-2008) over a pool of 20 European SMEs offering SATCOM, SATNAV and EO based services showed that there is a growing awareness of the importance of patents as a formal IP protection: the majority of the sampled SMEs had a patent driven strategy, with a preference for European patents (see exhibit below).

TECHNOFI

However, within the EO services industry represented in the study sample, the majority of SMEs had a secrecy-based strategy despite devoting between 10% and 20% of their revenues to R&D. From the IPR perspective, it is interesting to note that there are two extreme categories of SMEs operating in the EO sector:

- SMEs with low R&D activities: these are consulting firms relying on the expertise of their staff and selling on a skills basis. These kind of firms retain little IPR of their customised offer.
- SMEs selling research-oriented services as projects: their service is the research activity itself. The resulting IPR belong to their customers and, as a result, they do not develop a marketable service for their own use.

Between these two extremes, there are also SMEs engaging in research to develop services for sale to their customers. As most of these R&D activities are funded through public funds (ESA, EC or government contracts), the IPR of the related funding agency apply (see section 3.4 for a special case on the ESA's IPR rules).

What is your protection strategy?

48%   52%

☐ Patent driven
■ Secrecy based

In case of a patent, what kind of patents have been applied for?

24%   24%

52%

☐ National

■ European

☐ Other countries (please specify)
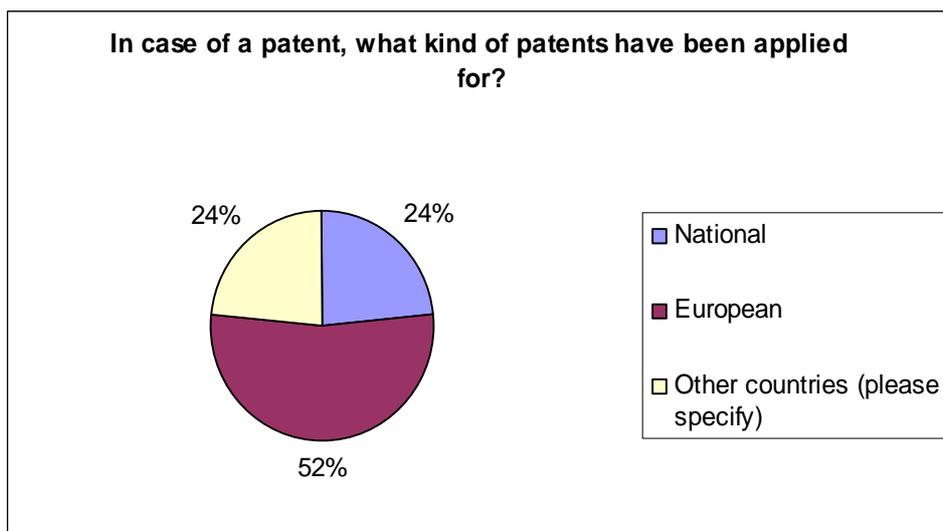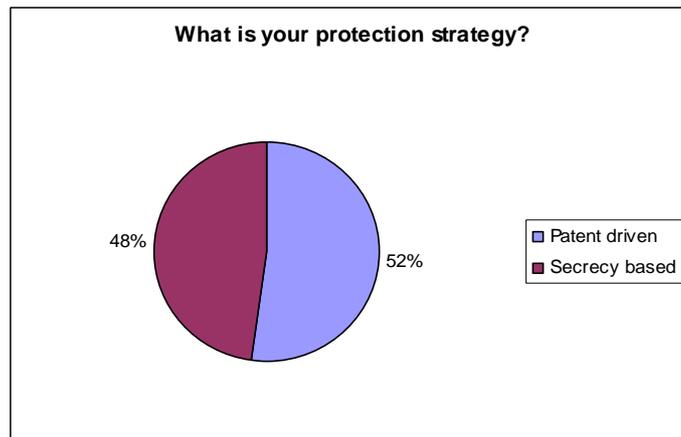
Exhibit 8**: Use of IPR among SATCOM, SATNAV and EO SMEs in Europe** (source [14])
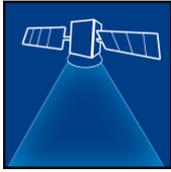
3.1.1 Patents

Patents belong to the <u>industrial</u> part of intellectual property protection, also called "Industrial Property".

A patent is an **exclusive right** granted for an **invention (**which is a **product** or a **process)** that provides, in general, a new way of doing something, or offers a new technical solution to a problem. A patent provides **protection** for the invention to the **owner** of the patent. A patent protection means that the invention cannot be commercially **made, used, distributed or sold** without the patent owner's **consent**[4]**.**

Obtaining a patent is acquiring the right to exclude others from using the protected invention in products, processes etc. without the inventors' consent. Getting a patent in Europe means also obtaining a legal industrial exploitation monopoly for a limited duration of generally 20 years from filing, provided that the annual fees to keep the patent alive are paid in due time. The protection is awarded in exchange for the publication of the invention.

To be patentable, an invention must fulfil three criteria:

- Being new: it offers functionalities which do not exist on the market, and it has not been published, whatever the medium.

- Being innovative: the invention does not come from an obvious deduction of several existing techniques being combined to accomplish a new task.

- Being useful, thus bringing more economic value: the invention must be industrially exploitable for an economical benefit. It must solve a technical problem.

Basic rules about timing and geographical coverage of a patent are recalled hereafter:

Timing (average)

To	Filing of the patent application.
To+9 months	Preliminary patentability advice (containing priority search results)
To+12 months	Deadline for requesting a geographical extension of the patent without losing the priority date, when filed nationally first.
To+18 months	Publication of the patent <u>application</u>. The final version of the patent can be different, especially when priorities are opposed during the examination process by the patent office concerned[5]. Then, claims are modified so that no more priorities can be opposed (restriction of the patent coverage)
To+21 months	Potential Observations
To+27 months	Delivery of the final patent.

---

[4] WIPO definition

[5] The final patent can also differ from the original application on minor adjustments that do not impact the content of the claims, nor their coverage, but clarify and meet the standards of claims writing.

To+30 months   Decision deadline for confirming geographical extensions

Geographical coverage

Most often a patent is filed first nationally. Then, extensions in other countries where the enterprise has strategic market interests are decided. International agreements have been settled to simplify the procedures and limit the costs when a significant number of countries are targeted:

- The European pathway through the European Patent Office (EPO)

- The PCT pathway through the World Intellectual Property Organization (WIPO), which addresses many more signatory countries.

However, some countries allow applicants to apply directly an international patent at EPO or WIPO (depending on national laws).

The particular case of software patenting

First of all, no precise definition of *software* exists in the Code of IP. According to a project of European Directive (COD/2002/0047), it would be an invention materialized by use of a computer.

A source code, or software *per se*, cannot be patented. However, relying on the principle of solving a technical problem, there are exceptional cases for which software can be considered as a product and a patent can then be delivered.

To be patentable, software must [10]:

- Be used in a technical field

- Solve a technical problem

- Process technical data thanks to technical functionalities

- Have claims qualified by technical characteristics

For example, software which allows for synthesising the voice in view of its transmission via numerical radio communication is eligible. The problem solved is the voice transmission over long distance through a numerical process. The same applies to software that builds a 3D image from radiographic imagery, etc…

On the other hand, accounting software, financial transaction software, semantic sorting programmes, etc. cannot be patented, because the functions they provide can be done easily by persons (even if it takes much more time than the software does).

It is underlined that the law is more flexible in the US, since the concept of code or software "per se" does not exist, nor the idea of a "technical solution to solve a technical problem". Only the result is analyzed: it must be new, useful and tangible.

For example, Hitachi patented a web-based tool such as "*e-Bay"* in the US:

- it offered something new (enabling multi-actors auction sales remotely),

- it was useful since avoiding people to move from their home to participate,

- it was tangible since visible on an internet-connected computer screen.
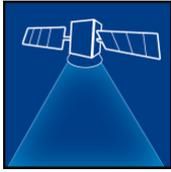
Their European extension was rejected for lack of innovativeness by the European Patent Office[6], arguing that "the claims are about steps of a method consisting in modifying an economic activity model and aiming at circumventing a technical problem rather than solving it by technical means, thus not relevant to the technical character of the claimed object".[10]

To conclude, if the targeted IP protection of software aims to protect a code, an algorithm or not patentable software, copyrights and open source may be the most appropriate scheme (see Exhibit 9 hereafter).
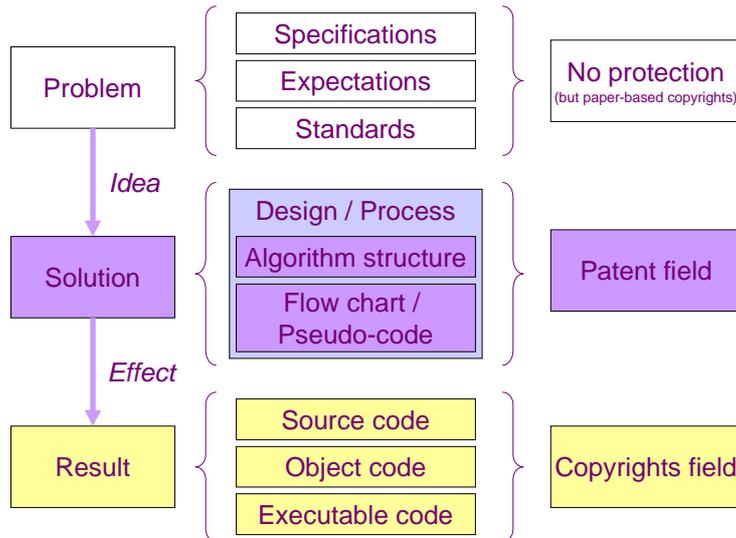
Exhibit 9: **Software IP protection** (source INPI [10])

3.1.2 Design patents

A design patent is the type of protection devoted to the intellectual creation used by designers. It is not meant drawings of a technical product, but designs having an aesthetic goal.

Some examples are:

- Aesthetic shape of a wind turbine
  (ENERCON egg-shaped drive system cover)

- The famous Philippe Starck tabouret

---

[6] EP97306722 (EPO Chamber of Technical Remedy 351, Hitachi 21/04/2004, T0258/03)

3.1.3 Copyrights

Copyrights aim at protecting non-technical intellectual creations, which can be linked to their authors by self standing "signatures". Among the most common creations registered under copyright, are found:

- Literature

- Music compositions

- Fragrances[7]

- Recipes

- Etc…

Software and programming codes can also be protected under copyright, provided that the way they are encoded is unique and specific to their authors (the idea of "signature" or idea-expression dichotomy). It means that copyright protects the shape of the code, but not its function.

It must be underlined that copyrights basically belong to the author, who keep the moral property rights whatever his/her situation. In most of the European countries, an employer can only claim use of such copyrights. The particular case of Germany gives more rights to the employer; most often, the employment contract will confer full copyrights property to this moral person.

Copyright advantages are kept by the author, then his/her heirs until 70 years after the Author's death.

The particular case of Open Source software

Open source software means that the source code is publicly accessible[8]. It lies on the principle of contagion: any new software developed using an open source code becomes automatically open source software, whatever the size of the first open source technological brick. Successively, software can therefore be improved, functionally augmented and shared again with the others. It works thanks to communities of contributors having shared interest in developing a software product.

Open source software does not mean that software can be obtained for free. This will depend on the strategic choices of the developer. Sometimes the developer will choose to make money by direct sales of a new product using open source bricks. In other cases, he/she will make business on the commercialisation of the services associated to the product. Generally, the market drives the choice. When there is purchase potential from the customers for the software product, the licensing is often retained. When there is more need for customization of the software parameters, then sales of services are preferred.

---

[7] No other case confirming the copyright protection of fragrances than the favourable decision for L'Oreal in France

[8] For more information, visit the Free Software Foundation http://www.fsf.org/ and the Open Source Initiative http://www.opensource.org/.

But open source software offers much more flexibility than the above mentioned ones. Some developers use the "versions system" to commercialise the latest available version as a software product, whereas the previous ones become downloadable for free, playing the role of teasers [13]. Some duration can be decided for a paying product (e.g. 1 year) before it becomes free of charge.

"Communities"[9] is the key word in the open source world. To access the community, one has to sign a licence contract, which gives rights (free access…) and binds to obligations (contagion…). The use of open source code is never constrained, but distribution freedom of derivate products can be limited. Among others, an open source license calls rules and regulations related to:

- Intellectual property

- Contracts

- Consumers

Two types of communities are distinguished:

- Academic licenses

    o Total distribution freedom of knowledge

    o No obligation of improvements feedback to the community

    o Examples : BSD – MIT/W3C – Apache, CeCILL-B

- Counterpart licenses

    o Counterpart: upgrades feedback to the community

    o Contamination of the derived productions

    o Total and dogmatic:

        ▪ Protection against any appropriation as ultimate freedom

        ▪ Examples: GNU GPL, CeCILL, EUPL..

    o Partial and pragmatic licenses:

        ▪ Adapted to the particular case of library components

        ▪ Eased interest of- and adoption by- industrials

        ▪ Examples: LGPL, CeCILL-C, MPL...

3.1.4 Trademarks

TradeMark (TM) protection targets commercial names and logos. It may include non-exclusively the name itself, its typology, and its graphical representation.

For example, in the case of Technofi, the name and the graphical representation are protected, but not the typology of the name.

---

[9] Today, about 60 open source licenses are recognised by the Open Source Initiative

Trademarks protection covers only the classes chosen by the owner, which are defined in line with the activity types of the trade mark owner. The more classes one wants to cover, the higher the trademark filing costs.

In view of avoiding unused TradeMarks bookings, some countries (US, Mexico, etc…) ask for regular proof of use of the TM (every year to every 3 years depending on the country). Regarding community trademarks, they can be cancelled after 5 years of consecutive non-use, subject to a respect action, e.g., by an accused infringer.

3.1.5 Utility models

A utility model is an exclusive right granted for an invention, which allows the right holder to prevent others from commercially using the protected invention, without his authorization, for a limited period of time. In its basic definition, which may vary from one country (where such protection is available) to another, a utility model is similar to a patent. In fact, utility models are sometimes referred to as "petty patents" or "innovation patents."

The main differences between utility models and patents are the following:

- The requirements for acquiring a utility model are less stringent than for patents. While the requirement of "novelty" is always to be met, that of "inventive step" or "non-obviousness" may be much lower or absent altogether. In practice, protection for utility models is often sought for innovations of a rather incremental character which may not meet the patentability criteria.
- The term of protection for utility models is shorter than for patents and varies from country to country (usually between 7 and 10 years without the possibility of extension or renewal).
- In most countries where utility model protection is available, patent offices do not examine applications as to substance prior to registration. This means that the registration process is often significantly simpler and faster, taking, on average, six months.
- Utility models are much cheaper to obtain and to maintain.
- In some countries, utility model protection can only be obtained for certain fields of technology and only for products but not for processes.

Utility models are considered particularly suited for SMEs that make "minor" improvements to, and adaptations of, existing products. Utility models are primarily used for mechanical innovations.

3.2 Semi-formal IP protection: contracts

Some methods are closely linked to formal methods, such as contracts, which have a legal basis, even though not being included in "IPR".

A great variety of contracts provides a flexible and legally binding way to protect IP within the firm and in view of future external relations. Typically businesses make contracts with their employees, customers, suppliers and various types of financing partners. The purpose of the contracts is not only to protect IP, but also to organise the daily working routines of the business in a more systematic manner. As such, contracts provide a flexible tool for IP protection and management because parties are free to agree about almost anything on a

contractual basis, naturally following the limitations of the relevant legislation. Contracts can include different types of sanctions that can be implemented through legal actions. In case parties end up in disputes, arbitration and civil court procedures can be used to enforce the agreed cooperation rules or the sanctions, as stipulated in the contract. But it is recognized that many contracts, such as subcontracting, are weakly anticipating potential IP ownership conflicts due to excess of confidence. The most typical types of contracts, which are used in intellectual property protection include:

- non-disclosure agreements
- non-competition clauses
- agreements about the ownership of IPRs
- recruitment freeze (e.g. limiting staff from working for a given set of competitors)
- agreements that forbid reverse engineering and product modifications
- agreements on the compensation for employee inventions

The particular case of satellite downstream services, license contracts will have to be concluded with the data providers to get access to the databases (SATNAV, EO) or to the telecommunication network (SATCOM). Basically, these contracts will include royalties to remunerate the IPR granted by the satellite infrastructure players, and an access fee to the database or the network. This access fee will pay the operation and maintenance of the infrastructure. The license contracts will also include clauses of NDA type to protect licensors from undesired copies of transferred data and clauses regarding privacy protection of persons.
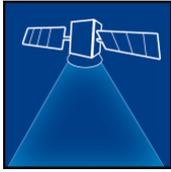
3.3 Informal IP protection

The primary goals of informal IP protection techniques are:

- to decrease the risk of losing the core knowledge
- to prevent the leaking of confidential knowledge to outsiders
- to reduce the risk of incidences, which could cause knowledge leaks
- to reduce the risk of being copied or imitated by competitors
- to prevent from the risk of losing key employees or to minimize the impacts of employees' mobility
- to create a 'lead-time' advantage over competitors
- to assist the patenting process
- to increase business efficiency and innovativeness

The various informal protection methods are not entirely independent from each other: they partially seem to overlap. Motivations for the use of each method vary as well: sometimes the main objective of the method is merely to protect IP. Sometimes it may simply be used to support the business activity.

Exhibit 10 gives the overview of the various types of informal protection practices and the related rational for IP protection[10] that will be discussed in more details later on.

Informal protection practice	Rationale for IP protection
• Secrecy	• Prevents confidential information from being distributed to outsiders
• Restricted access to information	• Decreases the risk of knowledge leaks through employees
• Database and network protection	• Prevents the risk of information diffusion to outsiders • Prevents from attacks, viruses and other abuses
• Confidentiality	• Prevents the risk of being copied

• Technical protection:
  Complex product design
  Software code protection
	• Makes copying and imitation difficult and time-consuming

• Documentation	• Increases efficiency • Decreases the risk of losing knowledge • Assists in patenting process
• Compartmentalising of tasks	• Decreases the risk of losing knowledge through the departure of an employee
• Circulation of staff between tasks	• Decreases the dependency on individual employees
• Loyalty building among personnel	• Decreases the risk of losing knowledge bound to employees • Increases motivation and efficiency
• Client relationship management	• Prevents knowledge leaks
• Membership in professional organisation	• Seeks to supervise IPRs among the members.
• Information sharing and exchange of knowledge	• Decreases the risk of losing knowledge bound to employees • Increases efficiency and innovativeness
• Fast innovation cycle	• Creates 'lead-time' edge over the competitors • Makes copying and imitation less harmful
• Publishing	• Prevents the risk of being copied or imitated and builds credibility of the inventor / originator of knowledge. Prevents other parties patenting of the published idea.

Exhibit 10: **Rationale of informal IP protections among KIS enterprises** (source [1])

---

[10] Results of the interview study performed in Finland and UK regarding informal IP protection by KIS SMEs
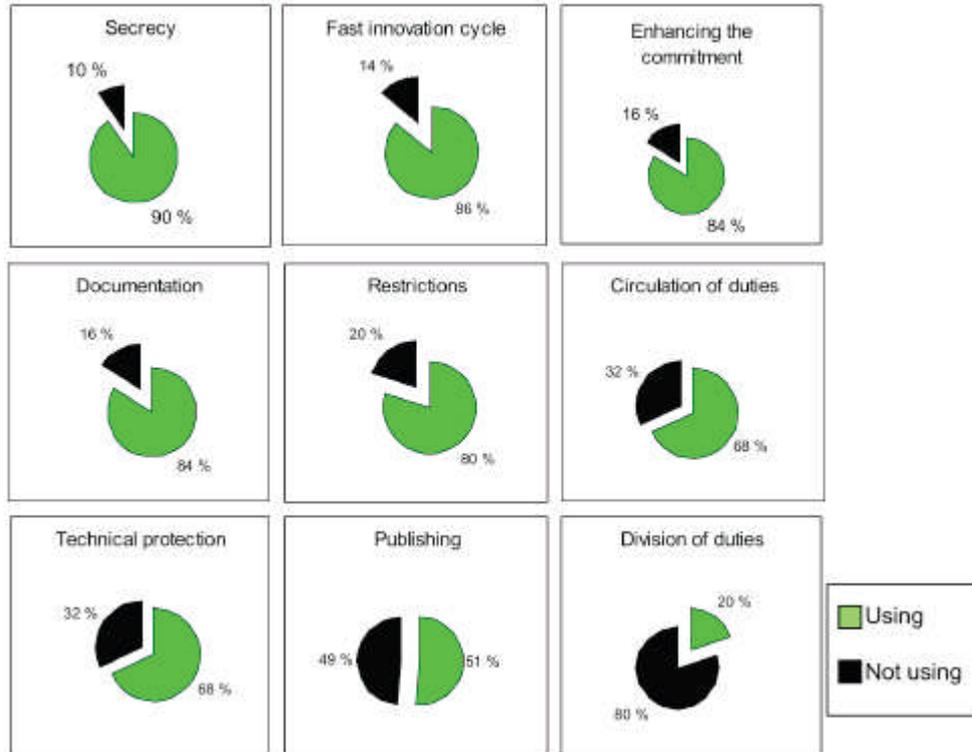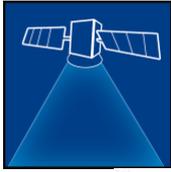
Exhibit 11: **Use of informal IP protection methods in KIS Finnish and UK firms**
(source [1])

3.3.1 Non Disclosure

Key knowledge can be kept secret either for some of the employees inside the firm and/or from external collaborators, such as business partners or customers. Many companies are defining carefully what type of information is classified and which parties should be kept away from such information. Secrecy may have a negative impact on innovativeness and the quality of the collaboration since it prevents from open attitudes, thus narrowing information flows between parties. A way to manage this issue is to use semi-formal protection methods through contracts (e.g. NDA or confidentiality agreements). Furthermore, in some companies, secrecy aims to maintain a lead-time advantage over competitors.

3.3.2 Publishing

In contrast to secrecy, the new idea or working practice can be published as widely as possible and the initial developer of the idea will become well-known as the innovator. That might lead to prevention of copying the new idea because imitation is seen unethical by society. Reputational sanctions can then be effective barriers to imitation, in particular when firms consider reputation for innovation to be a factor of differentiation [11]. This protection method is critical particularly in the service sector, for instance in advertising, where copying and imitation of ideas are easy and quite the common rule.

Publishing is also legally valid in the sense that publishing in any way is an obstacle to novelty patenting. Hence, publishing can be used to prevent other businesses from claiming patents in the same area. For instance, the key information can be published in small local newspapers. In such case patenting will be prevented and there is very limited chance that

any competitor would pick up the key information from a local paper with a limited number of readers.

3.3.3 Restrictions about using knowledge

IP related risks can be limited by restricting the number of people who have access to sensitive data. Such limitations may concern people inside and outside the business, hence the limitations encompass internal as well as external relationships. In principle this method is similar to secrecy. For instance, a company database may include documents and files accessible for viewing and editing only by those employees who are working on a certain project. Company premises may house facilities with limited access, for instance using access control. However, extensive use of restrictions within the business may lead to insufficient knowledge sharing which then becomes a barrier to innovativeness and productivity. In addition, restricted knowledge sharing poses a threat of a sudden loss of IP in the form of the departure of a key employee.

3.3.4 Enhancing the commitment of personnel

Effective building strategies of staff loyalty are seen powerful tools to protect intellectual property, since much of the knowledge lies with the brain of key employees. Different loyalty building methods can be used, regardless of the sector and the size of the company. In the service sector, employees are considered the most valuable asset of the company, and the departure of a key person may cause a sudden loss of IP. Effective strategies to maintain staff loyalty encompass financial incentives, training opportunities or other occupational development related incentives. Moreover, one successful way to enhance employees' motivation is to place company ownership arrangements with the key-employees. However, significant incentives to recognize individual employees' effort may also harm the atmosphere inside the company. They become counter-productive when competition among employees discourages cooperation.

3.3.5 Task allocation

Fragmentation of labour means that work tasks within the business are divided between employees, so that each employee controls only a fraction of the knowledge to be produced: no single person knows the overall concept underlying a new product or service. This method is also tightly linked to secrecy inside the business: the objective is again to minimise employee-related risks, e.g. to avoid the loss of valuable knowledge in case an employee chooses to leave the firm. However, in small firms, human resources are often limited and tasks cannot be fragmented. Such fragmentation of work tasks may also yield problems in firms where free flow of information is important. In practice, this method is typically more suited for very large organisations.

3.3.6 Suited swapping of tasks

Rotating staff from one task to another (together with naming deputies for employees) can be used to decrease the dependence on key personnel. The advantages of this protection practice are acknowledged especially in the marketing and advertising sectors, where employee mobility is high and long-term commitments of personnel are rare. Effective task rotation is, however, difficult in small businesses where the key employee is often the sole expert in his/her own narrow field of work. This issue can be managed with systematic and comprehensive documentation. Yet, this method naturally fits better to larger organisations where the knowledge structure overlaps substantially.

3.3.7 Documentation

Documentation of ideas, resources and thoughts can reduce the risk of losing key knowledge. Businesses can transfer tacit knowledge into more explicit forms, e.g. into written documents, CD Roms or databases. To be effective, documentation should be simple to implement; the process should be carried automatically in parallel of the innovation process or the idea development. Documentation has two different dimensions. First, it enables the effective gathering and sharing of knowledge inside the company. Secondly, documentation allows firms reducing the risk of a sudden loss of IP through the departure of a key person.

3.3.8 Fast innovation cycles

By maintaining a fast innovation cycle and bringing new products and services to market quickly, businesses can create a lead time advantage over their competitors. Introducing new products fast enough helps companies reducing the risk of being copied or imitated by competitors. As a result, by the time any product or service is copied, the business has already moved on to the next generation of products. Fast innovation cycle may have a significant role especially in fast developing businesses such as software and mobile phone technology. This method may suit smaller firms due to their ability to respond quickly to changing market demands. In this kind of business, patenting has clearly low value, but the branding strategy can take the front scene.

3.3.9 Technical protection

Technical protection provides a number of instruments to protect the intellectual assets. Some common methods in software protection are e.g. (1) coding or scrambling the information so that it can only be decoded and read by someone who owns the appropriate key (encryption), (2) using security keys (dongles) or (3) converting a program into an equivalent one that is more difficult to reverse engineer (obfuscation). Also firewalls and passwords are widely used. Technical protection can also mean incorporation of specific identification codes into software programs or e.g. in photographs or other documents. Such codes can later be used to prove the copyright. In addition, software products can be sold as a black box (object code), which means selling the product without releasing the source code.

On the opposite, open source software goes against this protection strategy. It must be known that any new algorithm using an open source module becomes automatically an open source algorithm. Thus, the increasing use of open source codes will lead to an action against IPR, which is actually a trend in the whole software industry. Start-up entrepreneurs, looking carefully after all their expenses, may widely use open source software while purchasing installation, customization and maintenance services.

3.4 Special Case: ESA's IPR rules[15]

Clause 37.1 of the General Clauses and Conditions of the European Space Agency (and other similar clauses for different forms of intellectual property right protection) indicates that the contractor is the sole proprietor of all intellectual property rights on results achieved under ESA funded projects.

However, the Agency and the Member States (or Participating States) are entitled to a free of charge, non exclusive, irrevocable license to use these results. The Agency is moreover

entitled to grant sub-licenses to third parties, including companies. No limitation on the use that can be made of the (sub-) licensed results is included in the General Clauses and Conditions and based on these clauses any third party could be granted the same commercialisation rights as the spin-off company (Clause 37.2 and other similar clauses). These rights granted to the Agency are of course a logical consequence of the funding by the Agency of the research and development work performed under the projects.

Under Clause 40, the Agency is entitled to receive, under the form of royalties, a compensation based on the commercial results achieved (this obligation is not applicable to cases where the exploitation takes place within the framework of space research and technology and space applications, Clause 40.2)

3.5 Special Case: Galileo IPR

Information on GALILEO IPR can be found on the following web-sites:

- the European GNSS Supervisory authority: http://www.gsa.europa.eu/. Legal questions including IPR issues can be asked to : legal@gsa.europe.eu

- The Galileo Joint Undertaking: http://www.galileoju.com/

3.6 Special Case: Access to Core Service data and products for the development of KOPERNIKUS (ex-GMES) downstream services[15]

The development of Kopernikus Downstream Services often requires access to data and products resulting from the Kopernikus Core Services[11].

The EC has defined geo-data access conditions for certain types of downstream services: "Geo-data and information resulting from the *core services* projects *should be made accessible, without charges, and on a non-discriminatory basis to downstream service providers* when such activities involve **developing, implementing and monitoring community policies related to the environment and security through research activities**" (EC, 2008 FP7 Space Call, page 9)

Geo-data access conditions for any other type of activities (e.g. involving the sale of downstream services to private customers) are to be negotiated with the Core Service providers.

For instance, for the land Monitoring Core Service (developed by the FP7 GEOLAND2 project), as of today, access conditions to its products and services involve the following[16]:

- The downstream service provider signs GEOLAND2 data user license

- GEOLAND2 will grant licenses for FP7 R&D in framework of FP7 Space GMES downstream services call

---

[11] These comprise 3 FAST TRACK services (Emergency Response, Land Monitoring and Marine) and 2 Pilot Services (Atmosphere and Security)
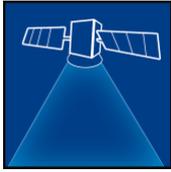
- • The license will oblige the receiving parties to provide user requirements, validation / utility assessment results.

Moreover, future Kopernikus services, both during their pilot phase and when fully operational, will require an appropriate supply of input data from both space and in-situ observation systems[12]. Until now, most R&D actions aimed at developing Kopernikus services have typically obtained their required input data by directly accessing them from the relevant operators (data providers), with ad-hoc negotiations of data access conditions. This approach, while linking directly data operators with their direct customers, i.e. the services operators, lacks a coherent European and inter-service coordination and inter-operability, and often leads to duplications.

One of the key areas to be funded under the ongoing 2008 FP7 Space call is "the coordinated provision of observation data (both from space-based infrastructure and in-situ observing systems". The advantages of a coordinated access to data would include:

- - *to the service providers* (and ultimately to the *end users*): a coherent market of data and lower costs, already pre-processed data (e.g. ortho-rectification, digital elevation models) in a coherent way across all other services, and a guarantee of long-term availability of data.

- - *to the data providers*: a **bulk agreement** (rather than separate small agreements), leading to a more stable industrial investment strategy, with better complementarity among different operators. This would entail general data access conditions for all service providers.

As far as the provision of *space-based* data is concerned, including from non-dedicated missions (e.g. national or commercial missions), ESA is seen as by the EC the appropriate coordinator of the supply side during the development phase covered by the EC Space Call Work Programme, in full cooperation with the relevant national and European mission operators. The European Space Agency is managing the GMES Space Component Data Access (GSC-DA) project in the frame of the FP7 space programme as part of the European Space Policy focusing on coordinating the access to space-based observation data to support Kopernikus services. The GSC-DA should supply the FP7 projects implementing Kopernikus Services with all the required space data in a seamlessly integrated, timely, secure and coordinated fashion. The FP7 funded three fast track services and the two pilot service projects should be served as a first priority, and other FP7 actions, in particular those implementing downstream services as a second priority**.** The GSC-DA aims at providing a comprehensive and coordinated access to such data allowing the capacity to link directly the different Earth Observation (EO) Data Providers and the different Service Providers using coordinating functions. The GSC-DA projects' driver is the EO-Data Access Portfolio (EO-DAP), its maintenance and evolution. The EO-DAP is the portfolio of available EO data products from existing space based sensors that will be provided from the Kopernikus Space Component to the operators of the Kopernikus Services during the Kopernikus pre-operation period 2008-2010, and beyond within an evolution cycle of both Service requirements and EO-DAP data provision.

Since satellites dedicated primarily to Kopernikus services (ESA-Sentinels) will be available only from 2011, the portfolio starts using currently available data from various EO data sources defined as Contributing Missions.

---

[12] FP7 Cooperation Work Programme : Space

Responding to the requirements of the Kopernikus Services, the EO Data Access Portfolio (EO-DAP) document describes the Earth Observation (EO) data being made available by the Kopernikus Space Component (GSC) to the operators of Kopernikus Services during the Kopernikus pre-operations period, i.e. from 2008 to end 2010. The document identifies the space-based observation needs and describes the Kopernikus EO data package from all the contributing missions, including:

- the conditions (e.g. ordering mechanisms, processing level, delivery timeliness)
- the constraints (e.g. data quantities, satellite tasking, data licensing**)** and the interfaces between the GCS and Kopernikus Services, and indirectly to the Kopernikus users.

A copy of this document will be available from the European Commission on request.

For more information, see:

- http://ec.europa.eu/enterprise/space_research/proposals.htm
- http://www.esa.int/esaLP/SEMYU10DU8E_LPgmes_0.html

4 BUSINESS CASES DESCRIBING IP PROTECTION STRATEGIES AND EXPLOITATION BY SERVICE SMEs IN THE SATELLITE DOWNSTREAM SERVICES SECTOR

Nine typical Service company profiles of the satellite downstream applications sector have been put under scrutiny regarding their potential concerns about Intellectual Property protection. In each situation, recommendations are presented, without taking into account the financial aspects, which remain the choice of each entrepreneur.

For each of them, a mapping of the IP types is graduated according to the frequency of use as follows:

■ To be used often   ▣ To be used sometimes   ☐ Rarely of use

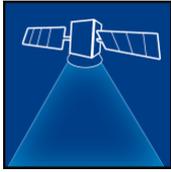| **Formal IP**	**Semi-Formal IP**	**Informal IP**
☐ Patents	☐ License contracts	☐ Secrecy
☐ Design patents	☐ Client subcontracts	☐ Publication
☐ Copyrights	☐ Confidentiality agreements	☐ Restriction on knowledge access
☐ Trade Marks	☐ Employee contract policy	☐ Enhanced commitments of personnel
☐ Utility Models		☐ Division of duties
☐ Databases		☐ Circulation of duties
		☐ Documentation
		☐ Fast innovation cycles
		☐ Technical protection

4.1 Business case 1: R&D Outsourcing SME

Formal IP

☐ Patents

☐ Design patents

☐ Copyrights

☐ Trade Marks

☐ Utility Models

☐ Databases

Semi-Formal IP

☐ License contracts

■ Client Contracts/Subcontracts

▨ Confidentiality agreements

■ Employee contract policy

Informal IP

■ Secrecy

☐ Publication

☐ Restriction on knowledge access

▨ Enhanced commitments of personnel

▨ Division of duties

☐ Circulation of duties

■ Documentation

☐ Fast innovation cycles

☐ Technical protection

An R&D outsourcing SME provides its clients with research based services as projects. Its service is the research itself, which can involve the use of signal processing techniques, algorithms, instruments. The IPR resulting from this R&D activity belong to its customers and, as a result, this company does not develop a marketable service for its own use. This kind of company can also act as subcontractor of a bigger player in a large contract.

Its main assets are know-how and creativity. Its employees rely on tools such as signal processing techniques, algorithms and instruments. These tools can be proprietary if built from past public–funded contracts.

According to this SME profile, the following IP management approaches should be considered:

Contracts/Subcontracts: referring to the "Semi formal IP protection" section above, this kind of SMEs are strongly advised to care about the "ownership" section of their contract with their clients, at least when there is potential innovation or future business potential. The outsourcing contract should clearly mention what is considered as background, i.e. existing knowledge that is claimed as proprietary and will be used in the framework of the contract. It should specify who will be the owners of the foreground (new knowledge created in the frame of the contract) and the exploitation rules of that foreground beyond the end of the contract. The usual rule is that the one who pays has the rights to exploit in the business area of interest. Yet, exploitation outside that area can be granted to the contractors/subcontractors with fees back to the one who paid (the client). The same principle applies in the frame of multi-contractor projects.

Confidentiality: Confidentiality rules can be inserted in the contracts/subcontracts when particular knowledge and/or know-how are intended to be used, and for which the SME requires protection with regards to divulgation to outsiders. They can be either covered in a separate Non-Disclosure Agreement (NDA), or inserted directly as dedicated Articles of the contract/subcontract. They will always have a limited duration depending on the standard innovation cycle time of the product (say 2 to 5 years after the contract termination).
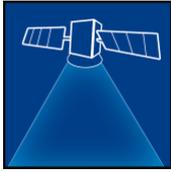
Secrecy: it aims at preventing confidential information from being distributed to outsiders

Employee's contract: Closer to the informal IP protection but still having a legal basis, the job contract is often used as a protection against the release of knowledge and know-how outside the company. Several clauses can be used, such as:

- No competition rule: an employee can be forbidden to be hired to a direct competitor for a couple of years to avoid immediate operational loss of the competitive advantage. Such a clause is usually subject to a financial compensation (from 2 to 24 monthly salaries depending on the financial challenge). It must be underlined that this clause is not valid when the sector of activity is highly specialised with a very limited number of players, because, in that case, the employee would have too much difficulty to find another job if fired by the company.

- Non disclosure commitment

- Ownership of the generated knowledge: most often, the IPR generated in the frame of a working contract belongs to the employer. However, this must be written in the job contract. Otherwise the inventor can get the rights with priority. In practice, courts consider that when the occupied position is naturally aiming at producing new knowledge (typically R&D activities) and the invention comes from this activity, the property is transferred to the company. Anyhow, an inventor must always be remunerated for the IPR that has been generated, unless otherwise agreed.

Enhanced commitment of personnel: In R&D outsourcing SMEs, the employee's loyalty towards the enterprise is based on a set of incentives like:

- financial incentives as a recognition of expertise;

- ownership sharing with the enterprise;

- trainings to acquire new competences;

- job evolution in the company.

Division of duty: In such SMEs, task split among the employees is driven by the individual skills rather than by a strategic IP protection decision.

Documentation: To avoid release of knowledge and know-how out of the company, many SME put knowledge management as a key priority. It is often advised for such companies to invest in knowledge management tools, since knowledge is part of the company assets.

4.2 Business case 2: Consulting/Engineering SMEs

Formal IP	Semi-Formal IP	Informal IP
☐ Patents	☐ License contracts	■ Secrecy
▣ Design patents	☐ Client subcontracts	☐ Publication
☐ Copyrights	☐ Confidentiality agreements	☐ Restriction on knowledge access
▣ Trade Marks	■ Employee contract policy	■ Enhanced commitments of personnel
☐ Databases		■ Division of duties
☐ Utility Models		☐ Circulation of duties
		☐ Documentation
		☐ Fast innovation cycles
		☐ Technical protection

This type of SME relies on the sole expertise of its staff and sells on a skills basis. Hence, it retains little IPR from its customised offer. The only assets are knowledge and know-how. Its employees rely on tools like methodologies and experience in previous contracts. These tools are mostly not proprietary.

According to this profile, the following approaches should be considered:

Branding (Trade Marks): Sometimes, the SME can be filed as a TM for marketing purpose.

Design Patents: In addition to trade mark protection, if designs are used in the business (e.g. logo), design patent protection is also an option.

Secrecy: it aims at preventing confidential information from being distributed to outsiders

Employee's contract: Close to the informal IP protection but still having a legal basis, the job contract is often used as a protection against the release of know-how outside the SMEs. Several clauses can be used, such as:

– No competition rule: an employee can be forbidden to be hired to a direct competitor for a couple of years to avoid immediate operational loss of the competitive advantage. Such a clause is usually subject to a financial compensation (from 2 to 24 monthly salaries depending on the financial challenge). It must be underlined that this clause is not valid when the sector of activity is highly specialised with a very limited number of players, because, in that case, the employee would have too much difficulty to find another job if fired by the company.

– Non disclosure commitment

Enhanced commitment of personnel: The employee's loyalty towards the enterprise is based on a set of incentives:

- financial incentive , as a recognition of a training expertise;

- ownership sharing of the enterprise;

- trainings to acquire new competences, within the company;

- increased responsibility in the company.

Division of duty: In such SMEs, task split among the employees is driven by the individual skills rather than by a strategic IP protection decision.

4.3 Business case 3: SME offering geo-information services based on software

Formal IP	Semi-Formal IP	Informal IP
☐ Patents	■ License contracts	■ Secrecy
☐ Design patents	☐ Client subcontracts	☐ Publication
☐ Copyrights	☐ Confidentiality agreements	■ Restriction on knowledge access
☐ Trade Marks	■ Employee contract policy	■ Enhanced commitments of personnel
■ Databases		■ Division of duties
☐ Utility Models		☐ Circulation of duties
		■ Documentation
		■ Fast innovation cycles
		■ Technical protection

This type of SMEs sells standardised off-the-shelf geo-information services and/or customised geo-information solutions based on EO data interpretation and processing. These SMEs engage in research to develop their services. Hence, they retain the IPR of their offer. Most often these research activities are funded by public agencies, in which case the agency's specific IPR apply. The assets are <u>knowledge</u> and <u>know-how, data processing techniques, and software products (most often proprietary)</u>. Its employees rely on tools like numerical models, EO data, in situ observations, high resolution remote sensing, and software.

According to this profile, the following approaches should be considered:

Software patenting:

A patent application can be an opportunity when the enterprise develops its own software for data processing to deliver the geo-information services. When software is proprietary, its patenting in view of its licensing can be envisaged if the software can:

- Be used in a technical field
- Solve a technical problem
- Process technical data thanks to technical functionalities
- Have claims qualified by technical characteristics

Copyright: These SMEs handle large amounts of data which have commercial value. Provided that they constitute a self standing piece of knowledge as a whole, they can be registered as a proprietary creation.

Branding (Trade Marks): Sometimes, the SME can be filed as a TM for marketing purpose.

Design Patents: In addition to trade mark protection, if designs are used in the business (e.g. logo), design patent protection is also an option.

Databases: These SMEs usually purchase access to raw EO data, which they process in their software to deliver customer-oriented services. The databases they create subsequently can also be seen as protectable databases.

License contracts: In relation to the above mentioned needs for raw data from satellites, their access will be systematically framed by a license contract with the satellite operator or the data access provider.

Employee's contract: Close to the informal IP protection but still having a legal basis, the job contract is often used as a protection against the release of knowledge and know-how outside the SMEs. Several clauses can be used, such as:
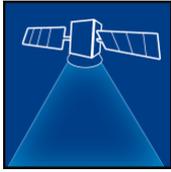
- No competition rule: an employee can be forbidden to be hired to a direct competitor for a couple of years to avoid immediate operational loss of the competitive advantage. Such a clause is usually subject to a financial compensation (from 2 to 24 monthly salaries depending on the financial challenge). It must be underlined that this clause is not validated when the sector of activity is highly specialised with a very limited number of players, because, in that case, the employee would have too much difficulty to find another job if fired by the company.

- Non disclosure commitment

- Ownership of the generated knowledge: most often the IPR generated in the frame of a working contract belongs to the employer. This must be written down in the job contract. Otherwise, the inventor can get the rights with priority. In practice, courts consider that when the occupied position is naturally aiming at producing new knowledge (typically R&D activities) and the invention comes from this activity, the property is transferred to the company. An inventor must always be remunerated for the IPR that he has been generated, unless otherwise agreed.

Secrecy is a wide spread practice in this type of SME. It deals with the commercial value of processed satellite data and their storage in databases. This knowledge (processed data) and know-how (e.g. numerical models) are usually protected by non disclosure rules (due to the high cost of data acquisition and processing).

Access restriction to knowledge: Complementarily to the above non disclosure practice, access to the databases can be put under control by the management to avoid someone going to the competition with a whole self-standing data set.

Enhanced commitment of personnel: The employee's loyalty towards the enterprise is based on a set of incentives:
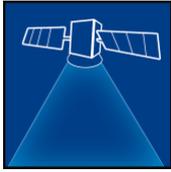
- financial incentive , as a recognition of a training expertise;

- ownership sharing of the enterprise;

- trainings to acquire new competences, within the company;

- increased responsibility in the company.

Documentation: the main goal of the documentation will be to capitalise and train employees on the techniques used for EO data processing.

Fast innovation cycles: accuracy and reliability of the satellite data processing is a key asset and there is continuous improvement on the existing techniques, and speed up of the innovation cycle can be expected.

Technical protection: With regards to access to the databases, some technical protections can be used, such as encryption of data or firewalls.

4.4 Business case 4: SMEs offering integrated solutions for Earth Observation

Formal IP	Semi-Formal IP	Informal IP
■ Patents	☐ License contracts	■ Secrecy
☐ Design patents	☐ Client subcontracts	☐ Publication
☐ Copyrights	☐ Confidentiality agreements	■ Restriction on knowledge access
☐ Trade Marks	■ Employee contract policy	■ Enhanced commitments of personnel
☐ Databases		■ Division of duties
☐ Utility Models		☐ Circulation of duties
		■ Documentation
		■ Fast innovation cycles
		■ Technical protection

These are SMEs whose offer combines EO services with other elements, such as hardware, software and system maintenance. These SMEs engage in research both to develop their services and the hardware components. Hence, they retain the IPR of their offer. Most often these research activities are funded by public agencies, in which case the agency's specific IPR apply. The assets are <u>knowledge</u> and <u>know-how, data processing techniques, software products (proprietary or not), hardware components</u>. Its employees rely on tools like numerical models, EO data, in situ observations, high resolution remote sensing, software and hardware components.

According to this profile, the following approaches should be considered:

Patents: Patenting will be highly relevant for SMEs which develop their own hardware and other specific technical components. A patent application can be an opportunity when the enterprise develops its own software for data processing

Copyright: These SMEs handle large amounts of data which have commercial value. Provided that they constitute a self standing piece of knowledge as a whole, they can be registered as a proprietary creation.

Branding (Trade Marks): Sometimes, the SME can be filed as a TM for marketing purpose.

Design Patents: In addition to trade mark protection, if designs are used in the business (e.g. logo), design patent protection is also an option.

Databases: When offering software based on satellite data processing, these SMEs might purchase access to raw EO data. The databases they create subsequently can also be seen as protectable databases.

License contracts: In relation to the above mentioned needs for raw data from satellites, their access will be systematically framed by a license contract with the satellite operator or the data access provider.

Employee's contract: Close to the informal IP protection but still having a legal basis, the job contract is often used as a protection against the release of knowledge and know-how outside the SMEs. Several clauses can be used, such as:

- No competition rule: an employee can be forbidden to be hired to a direct competitor for a couple of years to avoid immediate operational loss of the competitive advantage. Such a clause is usually subject to a financial compensation (from 2 to 24 monthly salaries depending on the financial challenge). It must be underlined that this clause is not validated when the sector of activity is highly specialised with a very limited number of players, because, in that case, the employee would have too much difficulty to find another job if fired by the company.

- Non disclosure commitment

- Ownership of the generated knowledge: most often the IPR generated in the frame of a working contract belongs to the employer. This must be written down in the job contract. Otherwise, the inventor can get the rights with priority. In practice, courts consider that when the occupied position is naturally aiming at producing new knowledge (typically R&D activities) and the invention comes from this activity, the property is transferred to the company. An inventor must always be remunerated for the IPR that he has been generated, unless otherwise agreed.

Secrecy: is a wide spread practice in this type of SME. It deals with the commercial value of processed satellite data and their storage in databases. This knowledge (processed data) and know-how (e.g. numerical models) are usually protected by non disclosure rules (due to the high cost of data acquisition and processing).

Access restriction to knowledge: Complementarily to the above non disclosure practice, access to the databases can be put under control by the management to avoid someone going to the competition with a whole self-standing data set.

Enhanced commitment of personnel: The employee's loyalty towards the enterprise is based on a set of incentives:

- financial incentive , as a recognition of a training expertise;

- ownership sharing of the enterprise;

- trainings to acquire new competences, within the company;

- increased responsibility in the company.

Documentation: the main goal of the documentation will be to capitalise and train employees on the techniques used for EO data processing.

Fast innovation cycles: accuracy and reliability of the satellite data processing is a key asset and there is continuous improvement on the existing techniques, and speed up of the innovation cycle can be expected.

Technical protection: With regards to access to the databases, some technical protections can be used, such as encryption of data or firewalls.

4.5 Business case 5: EO Data resellers

Formal IP	Semi-Formal IP	Informal IP
☐ Patents	■ License contracts	■ Secrecy
☐ Design patents	☐ Client subcontracts	☐ Publication
☐ Copyrights	☐ Confidentiality agreements	■ Restriction on knowledge access
☐ Trade Marks	☐ Employee contract policy	■ Enhanced commitments of personnel
◼ Databases		☐ Division of duties
☐ Utility Models		☐ Circulation of duties
		☐ Documentation
		☐ Fast innovation cycles
		☐ Technical protection

These SMEs resell EO images data (with little added-value) based on partnership (often long-term) with satellite data providers. Sometimes, they offer consultancy and advisory services related to the choice of proper data, recommended processing and integration with existing tools and databases. The key assets are the data, long-term partnerships with data providers.

According to this profile, the following approaches should be considered:

Databases: These SMEs need access to the raw data of satellites from the satellite operators, but do not claim any property rights unless they convert them into more directly exploitable new databases.

License contracts: Data resellers compulsorily sign license agreements with the satellite operators to guarantee a long term access to their customers.

Secrecy It deals with the commercial value of satellite data and their storage in databases. This knowledge (data) can be protected by non disclosure rules (due to the high cost of data acquisition).

Access restriction to knowledge: Complementarily to the above non disclosure practice, access to the databases can be put under control by the management to avoid someone going to the competition with a whole self-standing data set.

Enhanced commitment of personnel: The employee's loyalty towards the enterprise is based on a set of incentives:

- financial incentive , as a recognition of a training expertise;
- ownership sharing of the enterprise;
- trainings to acquire new competences, within the company;
- increased responsibility in the company.
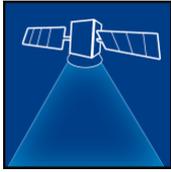
4.6 Business case 6: SMEs specialised in data processing software development

Formal IP	Semi-Formal IP	Informal IP
◩ Patents	☐ License contracts	■ Secrecy
■ Design patents	■ Client subcontracts	◩ Publication
◩ Copyrights	◩ Confidentiality agreements	☐ Restriction on knowledge access
■ Trade Marks	◩ Employee contract policy	◩ Enhanced commitments of personnel
☐ Databases		■ Division of duties
☐ Utility Models		☐ Circulation of duties
		■ Documentation
		■ Fast innovation cycles
		■ Technical protection

These SMEs sell software packages under license to support the use of EO data or images, including maintenance. Their main assets are software products (proprietary or not), know-how and creativity. Their employees rely on tools like prior software building blocks and mathematical models to achieve their tasks.

According to this profile, the following approaches should be considered:

Patenting: Referring to section 3.1.1 about patenting software, a patent application can be an opportunity in some cases. The best example is, about 25 years ago, a software application which simulates dynamically a fluid flow in a complex geometry (plasma motors for position control of satellites). Clearly in the past, such software solved a technical problem which could not be handled easily. Nowadays, opportunities for patentable innovations in that field should be limited. Moreover, software life cycle is so short that patenting becomes a worthless investment.

Copyright: Referring to section 3.1.3 about software copyright, there might be opportunities of IP protection via copyrights in this business, if the enterprise develops its own software products and employs programmers. This is of limited scope and impact.

Branding (Trade Marks): Simulation software SMEs made use of Trade Marks for the commercialisation of the software products. Even if the software application is bought to/licensed from a supplier for simulation tasks only, the name of the used tools can be exploited for external communication. Besides, the company name is often filed as a TM too.

Design Patents: In addition to trade mark protection, if designs are used in the business (e.g. logo), design patent protection is also an option.
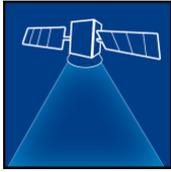
Subcontracting: referring to the "Patenting" section above, simulation software SMEs are strongly advised to take a specific care of the ownership section of their contract with their clients, at least when it may lead to innovations with business potential. The subcontract (or outsourcing contract) should clearly mention what is considered as background (existing knowledge that is claimed as proprietary and will be used in the frame of the contract), specify who will be the owners of the foreground (new knowledge created in the frame of the contract). The same principle applies in the frame of multi contractor projects.

Confidentiality: Confidentiality rules can be inserted in the subcontracts when particular knowledge and/or know-how are intended to be used, and for which the <u>client</u> requires protection with regards to divulgation to outsiders. The simulation subcontractor will rarely request for such a protection, since it has the ability to protect <u>technically</u> (see below) its knowledge and know-how. Confidentiality rules can be ruled either in a separate Non-Disclosure Agreement (NDA), or inserted directly as Articles of the subcontract. They will always have a limited validity duration, depending on the standard innovation cycle time of the product (say 2 to 5 years after the contract termination).

Employee's contract: Closer to the informal IP protection but still having a legal basis, the employer contract is often used as a protection against the release of knowledge and know-how outside the simulation software company. Several clauses can be used, such as:

- the competition rule: an employee can be forbidden to go to a direct competitor for a couple of years in order to avoid immediate operational loss of the competitive edge of its former company. Such a clause is usually subject to a financial compensation (from 2 to 24 monthly earnings depending on the financial challenge). It must be underlined that this clause is not valid when the sector of activity is highly specialised with a very limited number of business players. In that case, the employee would have too much difficulty to find another job when fired from the company.

- Non disclosure commitment

- Ownership of the generated knowledge: most often the IPR generated in the frame of a working contract belongs to the employer. This must be written down in the job contract. Otherwise, the inventor can get the rights with priority. In practice, courts consider that when the occupied position is naturally aiming at producing new knowledge (typically R&D activities) and the invention comes from this activity, the property is transferred to the company. An inventor must always be remunerated for the IPR that he has been generated, unless otherwise agreed.

Secrecy: Secrecy is a wide spread practice in the simulation software business. It deals with the combination of different mathematical models to simulate complex phenomena as closely as possible to reality. This knowledge (a compendium of mathematical models) and know-how (the way to combine and compile them) are usually protected by technical means (see below), so that non disclosure is reached naturally.

Publication: In this science-based business, scientific papers are published about new models developed to simulate more and more complex phenomena. Mathematical models cannot be patented, which explains the publication attitude. However, publication is not much used by private companies.
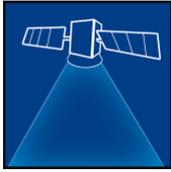
Enhanced commitment of personnel: In simulation software SMEs, the employee's loyalty towards the enterprise is based on a set of incentives:

- financial incentive, as recognition of expertise;

- ownership sharing of the enterprise;

- trainings to acquire new competences;

- job position upgrading in the company.

But this offer will depend strongly on the competition and the related financial capacities of the SME.

Division of duty: In simulation software SMEs, the split of the tasks among the employees is driven by the individual skills rather than by a strategic IP protection decision.

Documentation: For SMEs which only perform simulations using commercial software, knowledge management is a key priority. It is even advised to such companies to invest in knowledge management tools, since this knowledge is part of the company assets. For those SMEs which develop their own software, the documentation is often embedded in the software thanks to comments that are inserted to ease the navigation for the next colleague who will use it. The quality of the comments in the software will make the quality of the knowledge management.

Fast innovation cycles: the software world is known for its short innovation cycle. Two drivers pull the simulation performance:

- The accuracy of the simulation results, based on the models used

- The functionalities offered.

The lifetime of a software version extends from 12 to 24 months, which lowers the interest of potential IPR protection.

Technical protection: Referring to section 3.3.9, the software world is typically the one using technical protection of the source codes to lock access to the knowledge. Only the function remains available to the user.
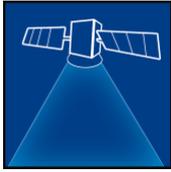
4.7 Business case 7: Training SMEs

Formal IP	Semi-Formal IP	Informal IP
☐ Patents	☐ License contracts	☐ Secrecy
◻ Design patents	☐ Client subcontracts	■ Publication
■ Copyrights	☐ Confidentiality agreements	☐ Restriction on knowledge access
◻ Trade Marks	◻ Employee contract policy	◻ Enhanced commitments of personnel
☐ Databases		■ Division of duties
☐ Utility Models		☐ Circulation of duties
		■ Documentation
		■ Fast innovation cycles
		☐ Technical protection

These are SMEs offering training courses on a commercial basis, including e-learning. A training organization is contracted by several clients at the same time (most often). Its main assets are <u>knowledge</u> and <u>know-how</u>. Its employees rely on tools like <u>software</u> and <u>equipments</u> to fulfil their tests. Tools are sometimes <u>proprietary</u>.

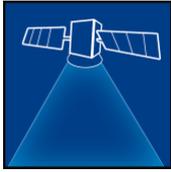According to this profile, the following approaches should be considered:

Copyright: A training organization will produce publicly accessible documentation with high knowledge content. It can be seen as non-technical intellectual creation. Therefore, it is strongly recommended to use Copyright protection to prevent from dealers use of this material by competing organizations. It may also apply to proprietary training software.

Branding (Trade Marks): Most of the time, the organization name is filed as a TM for marketing purpose.

Design Patents: In addition to trade mark protection, if designs are used in the business (e.g. logo), design patent protection is also an option.

Employee's contract: Close to the informal IP protection but still having a legal basis, the job contract is often used as a protection against the release of knowledge and know-how outside the training organization. Several clauses can be used, such as:

- No competition rule: an employee can be forbidden to be hired to a direct competitor for a couple of years to avoid immediate operational loss of the competitive advantage. Such a clause is usually subject to a financial compensation (from 2 to 24 monthly salaries depending on the financial challenge). It must be underlined that this clause is not valid when the sector of activity is highly specialised with a very limited

number of players, because, in that case, the employee would have too much difficulty to find another job if fired by the company.

- Non disclosure commitment
- Ownership of the generated knowledge: most often the IPR generated in the frame of a working contract belongs to the employer. This must be written down in the job contract. Otherwise, the inventor can get the rights with priority. In practice, courts consider that when the occupied position is naturally aiming at producing new knowledge (typically R&D activities) and the invention comes from this activity, the property is transferred to the company. An inventor must always be remunerated for the IPR that he has been generated, unless otherwise agreed.

Publication: A training organization is used to distribute a full documentation at the end of the training session. Copyright is a prerequisite.

Enhanced commitment of personnel: The employee's loyalty towards the enterprise is based on a set of incentives:

- financial incentive , as a recognition of a training expertise;
- ownership sharing of the enterprise;
- trainings to acquire new competences, within the company;
- increased responsibility in the company.

Task allocations: In training organizations, the split of tasks among the employees is driven by the individual skills rather than by a strategic IP protection decision.

Fast innovation cycles: As Knowledge is expanding continuously, a professional training must be "state of the art". Training approach is performed on at least a yearly basis, to be ahead of competitors.

Documentation: To avoid release of knowledge and know-how out of the company, many training organization put knowledge management as a key priority.

4.8 Business case 8: SMEs specialised in embarked satellite control software development

Formal IP	Semi-Formal IP	Informal IP
☐ Patents	■ License contracts	■ Secrecy
☐ Design patents	■ Client subcontracts	☐ Publication
■ Copyrights	☐ Confidentiality agreements	☐ Restriction on knowledge access
■ Trade Marks	☐ Employee contract policy	☐ Enhanced commitments of personnel
☐ Databases		☐ Division of duties
☐ Utility Models		■ Circulation of duties
		■ Documentation
		☐ Fast innovation cycles
		☐ Technical protection

This case is inspired by a real life legal case1.[18]. An SME selling control systems contracted with a major satellite manufacturer in order to provide control software embedded in a new satellite to orbit Earth. The major company signed a license agreement to exploit this software having specific features that ensure its reliability. The agreement stated that the major company would have a "worldwide" license to use the software for their intended purpose to convey that there are no geographic restrictions on the recipient's use of the licensed technology.

Yet, **does a worldwide license actually give sufficient rights to use software in a satellite that is arguably out of this world (i.e. orbiting Earth)?** What, exactly, is the geographic scope of a worldwide license? Could the licensor take advantage of this ambiguity to extract additional payments from an unsuspecting licensee? In the space industry, it is worth spending a few moments considering how a court might interpret this term in the outer space context.

In real life, more and more people are encountering such "everywhere" and "forever" language to avoid excluding possible future markets, even beyond our atmospheric layers.

According to this profile, the following approaches should be considered:

Copyright: Referring to section 3.1.3 about software copyright, it is strongly recommended to claim IP protection via copyrights in this business, if the enterprise develops its own software products and employs programmers.

Branding (Trade Marks): Simulation software SMEs make use of Trade Marks for the commercialisation of the software products. Even if the software application is bought to/licensed from a supplier for simulation tasks only, the name of the used tools can be exploited for external communication. Besides, the company name is often filed as a TM too.

Licensing: referring to the "Copyrights" section above, control software SMEs are strongly advised to take a specific care of the conditions for use of their control software by their clients. The License contract should clearly mention what is considered as proprietary knowledge and will be used in the framework of the contract. The same principle applies in the framework of multi contractor projects. Moreover, it should clearly stipulate that the rights are applicable in any geographical location, including beyond the Earth (see further details about the particular case of embarked software presented at the end of this case study).

Subcontracting: referring to the "Copyrights" section above, control software SMEs are strongly advised to take a specific care of the ownership section of their contract with their clients, at least when it may lead to innovations with business potential. The subcontract (or outsourcing contract) should clearly mention what is considered as background (existing knowledge that is claimed as proprietary and will be used in the framework of the contract), and specify who will be the owners of the foreground (new knowledge created in the frame of the contract). The same principle applies for multi-contractor projects. Moreover, it should clearly stipulate that the rights are applicable in any geographical location (see further details about the particular case of embarked software at the end of this case study).

Confidentiality: Confidentiality rules can be inserted in the license contracts and subcontracts when particular knowledge and/or know-how are intended to be used, and for which the client requires protection with regards to divulgation to outsiders. The simulation subcontractor will rarely request such a protection, since it has the ability to technically protect its knowledge and know-how (see below). Confidentiality rules can be defined either in a separate Non-Disclosure Agreement (NDA), or included directly as Articles of the contracts. They will always have a limited validity duration, depending on the standard innovation cycle of the product (say 2 to 5 years after the contract termination).

Employee's contract: Closer to the informal IP protection, but still having a legal basis, the employee's contract is often used as a protection against the release of knowledge and know-how outside the software company. Several clauses can be used, such as:

- the competition rule: an employee can be forbidden to go to a direct competitor for a couple of years in order to avoid immediate loss of the competitive edge of its former company. Such a clause is usually subject to a financial compensation (from 2 to 24 monthly earnings depending on the financial challenge). It must be underlined that this clause is not valid when the sector of activity is highly specialised with a very limited number of business players. In that case, the employee would have too much difficulty to find another job.

- Non disclosure commitment

- Ownership of the generated knowledge: most often the IPR generated in the frame of a working contract belong to the employer. This must be written down in the job contract. Otherwise, the inventor can get the rights with priority. In practice, courts consider that when the occupied position is naturally aiming at producing new knowledge (typically R&D activities) and the invention comes from this activity, the property is transferred to the company. An inventor must always be remunerated for the IPR that he has generated, unless otherwise agreed.

Secrecy: Secrecy is a wide spread practice in the control software business. It deals with clever combinations of parameters that will result in actuations. This knowledge and know-how are usually protected by technical means (see below), so that non disclosure is reached naturally.

Enhanced commitment of personnel: In control software SMEs, the employee's loyalty towards the enterprise is based on a set of incentives:

- financial incentive, as recognition of expertise;

- ownership sharing of the enterprise;

- trainings to acquire new competences;

- job position upgrading in the company.

But this offer will depend strongly on the competition and the related financial capacities of the SME.

Circulation of duty: In control software SMEs, the main asset is know-how. Hence, know-how preservation within the company is a key issue. Sharing this know-how for different applications is one of the possible keys to keep the IP in-house.

Documentation: For the same reason as above, knowledge management is a key priority. It is even advised to such companies to invest in knowledge management tools, since this knowledge is part of the company assets. For those SMEs developing their own software, the documentation is often embedded in the software thanks to comments that are included in order to ease the navigation by the next colleague who will use it. The quality of the comments in the software will impact the quality of the knowledge management.

Technical protection: Referring to section 3.3.9, the software world typically uses technical protection of the source codes to lock access to the knowledge. Only the function remains available to the user. However, in the control software business, it is often necessary to open access to some parameters to another company in order to allow this company controlling its own part of the satellite system. The language compatibility is a real issue then, which limits the potential for full technical protection.

Further details about outer space utilization of control software are presented below.

The liability of the satellite operator would depend on how the court interprets the scope of the "worldwide" software license. Without a legal precedent or a record of negotiations between the parties as a guide, the court would probably look at the common dictionary definition of the term "worldwide." *Dictionary.com* defines "worldwide" as "extending or spread throughout the world" Definitions in other dictionaries are mostly similar and include e.g., "spanning or extending through the entire world", "involving the entire Earth", "not limited or provincial in scope", "universal." *Black's Law Dictionary* defines "world" in the geographical sense as "the planet Earth", whereas Webster's online dictionary has 14 definitions for "world," with the relevant definitions for our purpose being: "the Earth with its inhabitants and all things upon it" and "a celestial body (as a planet)."

The less common definitions "not limited or provincial in scope" and "universal" conform to the common understanding of the term "worldwide" as used in license agreements. If the

court adopted one of these definitions, the satellite operator would be successful in defending its use of the software in Earth orbit. However, the software company would surely urge the court to adopt one of the most common and restrictive definitions.

Technically there is no clear boundary between the Earth's atmosphere and outer space. Nevertheless, the Kármán line, located at an altitude of about 100 kilometers, is a commonly used reference point. The Kármán line might therefore be a reasonable delineation for leaving the "world" for the purposes of interpreting intellectual property licenses. In fact, using the atmospheric boundary to differentiate legal rights has precedent in international law. Spacecraft in Earth orbit are generally permitted to overfly a country's airspace without permission, whereas an aircraft flying within the atmosphere may not do so. In addition, the 1972 U.N. Convention on International Liability for Damage Caused by Space Objects applies a fault-based standard for damage caused to objects in outer space and a strict liability standard for damage caused to objects on the Earth's surface or to aircraft in the atmosphere.

Of course, adopting an atmospheric standard, such as the Kármán line, would result in an unfavorable outcome for the satellite operator. To counter this, the satellite operator could argue that using an atmospheric standard is not the only option to determine when something has left the "world," even under a restrictive definition of "worldwide." A satellite in Earth orbit, even if above the atmosphere, still "involves" the entire world since it remains captured by Earth's gravity. Under this broad interpretation of Webster's definition of "worldwide" ("involving the entire world"), a spacecraft would travel beyond the scope of a worldwide license only once it has left the pull of Earth's gravity; thus, a satellite in Earth orbit would still be in compliance with a worldwide license agreement.

Therefore, it is strongly advised to use words that have clearer meaning than "world" to designate the whole space, like "universe" or "in the world and beyond" for instance, in licensing contracts in order to mitigate potential interpretation problems.
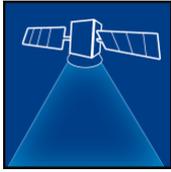
4.9   Business case 9: SME broadcasting contents via satellite

Formal IP	Semi-Formal IP	Informal IP
☐ Patents	■ License contracts	■ Secrecy
☐ Design patents	☐ Client subcontracts	☐ Publication
☐ Copyrights	▨ Confidentiality agreements	■ Restriction on knowledge access
☐ Trade Marks	☐ Employee contract policy	☐ Enhanced commitments of personnel
☐ Databases		☐ Division of duties
☐ Utility Models		☐ Circulation of duties
		☐ Documentation
		☐ Fast innovation cycles
		■ Technical protection

This case, inspired by a real life legal case1.[18], concerns a broadcasting SME which signed an exclusive license agreement with the Lambda Film Festival Organization, allowing the diffusion of the competing movies during the film festival all over the world. Since small sized, the SME contracts directly with French cinemas but cannot afford to outreach individual cinemas all over the world. Hence, it contracts sub-licenses with other broadcast agencies/companies abroad, which are in charge of delivering the program in their respective territories. For convenience reasons, these foreign partners receive the contents and broadcast them towards their subscribers via telecom satellites. Although the sub-licensees will be asked to deliver the paying service to their territorial cinemas and not to the wide public TV audiences, there is no other technical means than giving a dedicated frequency channel to this festival program and to communicate it to the subscribing cinemas. But, any client to the sub-licensee having a satellite program decoder may receive the Festival program if it scans again the available channels it can receive on TV. Thus, any subscriber of the satellite broadcast services has the appropriate decoder to watch the Lambda Festival program without extra cost. Moreover, even a cinema having such a satellite data decoder could publish the contents for a lower cost than by buying a dedicated license.

To get its return on investment, the SME intends to charge a fee amounting to € 10.000 each licensed cinema willing to broadcast the movie competition. But an unfair competition could arise from the above described situation, because of buying the decoding equipment for foreign satellite services costs around €1000 per year rather than the €10,000 that would have to be paid for the license.

The following issues have to be addressed:

– *Is our broadcasting SME infringing the license contract that it signed with the Lambda Film Festival Organization, when the dissemination escapes from its control through the use of satellite data decoding equipment?*

No. It is highly probable that the broadcasting SME has signed a contractual engagement with the Lambda Film Festival Organization with regards to the license fee amount to be paid, whatever happens in the dissemination of the contents and

provided that they are not transformed without the consent of the movie authors. The responsibility is on our SME to secure its return on investment.

- *Are the decoding equipment owners infringing any intellectual property of the Lambda Film Festival Organization or of the broadcasting SME?*

No, they have paid a subscription to get their decoding equipment and to benefit from the contents channeled through the satellite. By chance they detected this undisclosed program that they could technically receive and watch. It is the responsibility of the broadcast agencies/companies which signed sub-licensing contracts with our SME to ensure that they will get their return on investment, either from cinemas seat sales only or from an exceptional fee on their usual satellite TV subscription.

- *How can the licensing scheme be better secured with regards to the payment of royalty fees?*

The key is in the content of the sub-licensing contracts.

- *What should be the terms of the contract between our SME and its sub-licensees, who purchase the rights to broadcast the movies of the Lambda Festival?*

1. This sub-licensing contract may foresee either a commitment on the total royalty fee to be paid (like between the Festival Organization and the broadcasting SME) or a charge of € 10.000 applied to any cinema subscribing the service, from which a percentage is paid back to our SME. In the first case, our SME is on the safe side and the financial pressure is shifted to the sub-licensee. In the second case, some more contractual terms should secure a minimum amount of fees collected by the sub-licensees.

2. This sub-licensing contract may foresee a commitment on a minimum amount of royalty fee to be paid plus a commission on any subscription sale.

3. This sub-licensing contract must guaranty the respect of the intellectual property (copyrights) of the movie makers, thus forbidding any uncontrolled disclosure and transformation of the contents. This will result in an obligation for the sub-licensee to control the dissemination of the content. The disclosure may happen through the satellite TV subscription, or through the allocation of a private channel (e.g. with over encryption) to the cinema subscribers, but not to free-of-charge services for the end user.

4. An article on confidentiality is also advised to engage the sub-licensee's responsibility towards undesirable leakage about the existence of the Festival program in the bunch of satellite data flows.
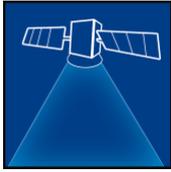
Beyond these recommendations about semi-formal protections, some informal means should be used as well:

- Secrecy
- Restriction on knowledge access
- Technical protection

REFERENCES

[1] "IP Protection and Management in KIBS and their Collaborative Networks", Päällysaho S. and Kuusisto J. (2006), Final report, ProACT project, pp. 73.

[2] "Informal ways to protect intellectual property in small and medium size businesses", Kuusisto J., Päällysaho S. and Kulmala R. (2005), Final report, ProACT project, pp. 50.

[3] "Intellectual Property (IP) protection as a key driver of service innovation: an analysis of innovative KIBS businesses in Finland and the UK", Päällysaho S. and Kuusisto J. (2008) Journal of Services Technology and Management 9: 268-284.

[4] "A memorandum on removing barriers for a better use of IPR by SMEs", PRO INNO EUROPE, June 2007

[5] Report from the IPR task force of the Galileo Joint Undertaking (GJU) Executive Committee.

[6] "Intellectual property and Innovation Management in Small Firms", Kitching and Blackburn, Routledge, London, UK. (2003)

[7] "Patents and Policy in the Innovation of Small and Medium Enterprises: Building on Rothwell". Macdonald, S. & Lefang, B., Routledge, London, UK (1998).

[8] "Commission recommendation on the management of intellectual property in knowledge transfer activities and Code of Practice for universities and other public research organisations", European Commission, Ref C(2008)1329, April 2008.

[9] "IPR in the frame of Subcontracting" seminar organized by CCI & INPI, held in Sophia-Antipolis – France – on the 25th of March 2008

[10] "Software protection" seminar organized by INPI & INRIA, held in Sophia-Antipolis – France – on the 15th of May 2008

[11] "Effects of reputational sanctions on the competitive imitation of design innovations", Gemser, G. and Wijnberg, N. (2001).

[12] "A memorandum on removing barriers for a better use of IPR by SMEs" by ProINNO, a European project co-funded by the European Commission, DG Enterprise & Industry, in the frame of the Europe INNOVA programme.

[13] "How to make value of a project thanks to the open source choice ?", seminar organized by INRIA, held in Sophia-Antipolis – France – on the 12th of June 2008

[14] INVESAT "Bridging the gap between INnovative enterprises and financial inVEstors in the emerging ICT markets of SaTellite applications", EC-funded FP6 project

[15] FINANCESPACE" Guide to Space Financing" EC-funded FP6 project

[16] GMES core-services under the Seventh Framework Programme: Geoland2 – Implementation of the Land Core Service Summary description of products and services, EC ,DG ENTR, Aerospace, GMES, security and defence Space Research and Development

[17] European Commission, FP7 Cooperation Work Programme: Space, 2008

[18] http://www.spacenews.com/commentaries/100901-blog-licensing-intellectual-property-rights.html

[19] http://www.lawdit.co.uk/reading_room/room/view_article.asp?name=../articles/5160-ECJ-To-Hear-Premiership-Battle.htm