Intellectual Property and Inter-organizational Collaborative Networks: Navigating the Maze

October 2004

Puay Tang and Jordi Molas-Gallart
Complex Product Systems Innovation Centre, SPRU, University of Sussex
The Freeman Center
Brighton, BN1 9QE
East Sussex, United Kingdom

Email address: J.Molas-Gallart@sussex.ac.uk

Email address: P.Tang@sussex.ac.uk
**Intellectual Property and Inter-organizational collaborative networks: navigating the maze**

**Abstract**

Intellectual Property (IP) is a key intangible asset influencing corporate performance and its management is increasingly recognized as a central element of corporate strategy. Analysts however, have largely focused on IP management *within* the firm, overlooking the different and pervasive problem of how to manage IP in the context of *inter-firm collaborative* projects. Here, groups of firms, often competitors, and sometimes their customer organizations, collaborate in the design, development, manufacture and maintenance of complex products. Such collaborations involve exchanges of large amounts of proprietary technical data, facilitated through the use of advanced IT tools. How can organizations exploit the capabilities offered by these tools without increasing the vulnerability of IP assets to misappropriation or leakage? In the UK defense market an extensive set of formal contractual tools are being developed to support IP management in collaborative projects. Through an in-depth study of IP management practice in UK defense projects we analyze the extent to which contractual tools can combine with technical solutions to provide answers to the problems posed by IP management in complex, long-term collaborative projects. We conclude that contractual and technical tools must be underpinned by managerial changes that bring together functions that remain separated in most large corporations: IT management, and legal and commercial departments.
Intellectual Property and Inter-organizational collaborative networks: navigating the maze

Introduction

Until recently, the management of Intellectual Property (IP) and its associated Rights (IPR) was treated as a specialized function within a company. Corporate strategy would concern itself mainly with the management of tangible and financial assets, and IP management would be left to specialist lawyers who would deal with patents and other forms of IP protection as needed. Similarly, IT (Information Technology) managers who dealt with corporate systems for data access control rarely consulted with the legal or commercial departments on IP issues such as the potential data leakage inherent in the treatment and transfer of electronic data.

This situation is changing. Toward the late 1990s, analysts were underlining the importance of IP and IPR management as a key element of corporate policy. IP is now seen as a strategic intangible asset influencing corporate performance.

Important as IP is for the modern corporation, scholars have found it a difficult concept to define accurately. The American Heritage Dictionary defines IP as a product of the intellect that has commercial value. The Oxford English Dictionary defines it as property which is the product of invention or creativity, and which does not exist in a tangible physical form. In short IP refers to intangibles that are commercially valuable. Yet, IP can be expressed in many different, tangible, forms: books, blueprints, designs, trademarks are all expressions of IP, which can be made available to other parties. The use of IT and electronic networks increases the risk of all these forms of IP to misappropriation or leakage, inadvertent or otherwise.
As the recognition of the commercial value of IP deepens, its protection becomes an increasingly important managerial challenge. Simultaneously, data replication and transmission is becoming easier thanks to rapid development in IT, thus augmenting the risk of data conveying valuable IP leaking to competitors. A US survey estimated that $53 and $59 billion were lost to 138 responding firms through incidents in which proprietary information was disclosed. Over two thirds of the firms surveyed “strongly agreed” with the statement “The Internet, networks, computers and related technologies have created significant new threats to sensitive proprietary information.” This potential threat emerged clearly as the most important source of concern, particularly among large companies.

Similarly, a 2004 survey of 203 companies conducted by the UK National High Tech Crime Unit, reported that 12 per cent of the firms had experienced instances of data theft through the Internet, causing losses amounting to approximately £7 billion. Such realization of the risks posed by the growing use of electronic data networks suggests the need for specialized IP and information management strategies addressing data control and access issues.

So far, corporate responses and academic analyses have focused on IP management within the firm. The problems and challenges faced are, however, likely to be different when managing IP in the context of inter-firm collaborative projects in which groups of firms, often competitors, and sometimes their customer organizations share in the design, development, manufacture and operation of complex products. In these cases large amounts of technical data (including designs, product specifications, manufacturing processes, etc.) can be shared through the use of advanced IT tools. The resulting “Shared Digital Environments” (SDEs) involve electronic networks, software platforms, and electronic data management systems used by project partners to manage and share technical data. SDEs are being proposed as a tool to assist large design, engineering and manufacturing projects in a wide variety of sectors, for reasons of efficiency and improved project management, among
others. The management of IP in SDEs poses problems that are different in nature and scope to those of IP management within the firm.

This article analyzes the nature of the problems posed by IP management in SDEs and discusses a range of approaches to their solution. It is based on an in-depth analysis of their use in the UK defense industries. In this area an exceptional effort is taking place to develop precise codes of practice and procedures affecting all aspects of the contractual process and project management including IP management. In collaboration with industry, the UK Ministry of Defence (MOD) has developed extensive guidelines and sets of contractual conditions on the management of IP in SDEs. This situation provides a unique test bed for analyzing the impact of formal regulations and processes on the management of IP, and the challenges faced when explicitly addressing IP management issues in inter-organizational networks and systems. Further, existing MOD procurement policies emphasize the use of inter-organizational IT networks to improve project performance. A context of detailed IP regulations is thus set against an effort to develop and implement large SDEs.

The article is structured as follows. We first discuss our approach. We then introduce the main relevant traits of present UK defense procurement practice, in particular the way it deals with IP, and analyze the specific IP management problems encountered when conducting collaborative ventures in the defense industries. We follow with a discussion of the strategies to respond to these challenges, and an analysis of the ways in which two specific SDEs have been implemented. We find that they have adopted different implementation models. We conclude with lessons for IP management in collaborative ventures.

**Our approach**

Our analysis has followed a case study methodology addressing the IP corporate management practices in the main British defense-related corporations and the way they relate to the IP practices of their main customer: the UK Ministry of Defence (MOD). The first step in our
study was a documentary study of the IP practices and regulations used in defense contracting laid out in the “contractual conditions” used by the MOD procurement agency (the Defence Procurement Agency –DPA). We followed with a program of semi-structured interviews using two different interview protocols, one addressing corporate policies and activities, and another oriented to the analysis of IP management practices within specific projects. The main objective of the interview program was to determine the ways in which firms addressed IP management in a digital environment both within the corporation and in collaborative programs.

To guide the interviews we designed a protocol structured according to a list of IP management topics with potential effects on firm and corporate performance. We based the list on IP management issues identified by the extant literature on IP management within specific sectors and firms. A panel of academic, industrial and government IPR experts validated the interview protocol, which we then piloted through a 6-hour long interview with two IPR and commercial managers of a major UK defense corporation. Following the pilot we adapted the protocol and used the two different formats, as noted above.

We then carried out interviews with all major UK defense systems producers. Between November 2003 and July 2004 we conducted detailed interviews with 20 relevant executives; including IP Directors, Commercial executives, IT systems directors, program directors and head engineers. In addition we held several meetings with other officials from industry, the DPA and a defense industrial association. In total we carried out 66 hours of meetings and interviews with 33 senior officials and executives. Except for six telephone interviews, the rest were all face-to-face interviews and meetings carried out by the both of us.

Within each participating company most of the interviewees were self-selected by their organizations based on their work on IP management and IPR issues both within the company and in collaborative projects and defense contracts. Because of the commercial
sensitivity of the issues explored we will not attribute the information collected and used in this article to any name and affiliation of the individuals interviewed.

**The case: Managing IP in the UK defense market**

All the firms and organizations involved in this study are simultaneously using different network technologies and inter-organizational systems in several projects. These are usually large complex projects involving a number of suppliers, coordinated through a prime contractor, to provide a system or a service for use by the UK armed forces. Under the current UK defense procurement approach, most of the above stakeholders participate in Integrated Project Teams (IPTs) set up by the DPA. The IPTs bring together representatives from the client organization, final users and industrial producers, and play a complex interface role between suppliers, the MOD client and military users. From an MOD perspective the IPT is seen as its internal “supplier,” in charge of delivering a system to frontline users. From the industry perspective the IPT plays the role of customer. Each IPT has a “Leader” who is the line manager for most core members of the IPT, and the formal point of contact with the MOD representative (final customer), and is responsible for meeting the agreed cost and performance targets and milestones.

In the British approach, IPTs are the key organizational mechanism for the management of defense procurement projects, and an avenue to facilitate constant communication among all main project stakeholders throughout the project’s life cycle, from conception, through research and development, production, operation, maintenance and upgrading and, ultimately disposal. In practice, every project establishes its own set of network technologies and inter-organizational systems, and its contractual conditions and procedures. The responsibility rests on the IPT and ultimately on its Leader: different projects will adopt different contractual clauses, different IT systems and different approaches to the management of IP. This means high set up costs for every project (there is an element of reinventing the wheel and limited
cross-project learning). Consequently, defense firms work with a wide variety of network environments and under varying contractual conditions. For instance, one of the firms interviewed is running 300 separate projects supported by different IT networking arrangements and contractual conditions to manage and share data with, often the same, customers and suppliers. Such a situation engenders not only additional costs but also a situation in which it is difficult to control and monitor the information flows through the variety of inter-organizational systems.

That every project sets up its own IT system and IP rules and practices is also explained by the lack of detailed corporate IP policies. Companies are familiar with the process of protecting their IP: it is common for large firms, including those in this study, to employ patent attorneys, copyright specialists, etc. within an IP department. For instance, the firms interviewed for this project either focused their IP management approaches on patenting strategies or relied on trade secrets. Yet a concentration on formally protecting firm IP does not amount to a full-fledged corporate IP management policy. Rather, a comprehensive IP policy should also include, for instance, monitoring of enforcement of corporate IPR and importantly, establishing company-wide processes and procedures for the treatment and use of corporate IP, whether they be formally protected or not. Instead, we have observed that the IP management “ethos” is biased, in the main, toward the protection processes – deciding whether or not to patent. Yet, the often-informal practices that determine, for instance, when and how to share proprietary information with clients and partners are not instituted as part of a corporate IP policy. The rest of this section discusses some of the problems that the defense companies and their customers have encountered when addressing IP issues in this context.
IP issues in collaborative environments

The protection of information within SDEs

The first key problem with an SDE is the protection of “background information.” Background information refers to the wide range of pre-existing proprietary information that a company brings to a collaborative project, from technical data and components and subsystems, to manufacturing processes and design techniques. These will need to be integrated with technology brought by other firms or developed for this project, and therefore other firms may need to have access to such “background information.” By sharing background information through SDEs companies run the risk of inadvertent leakage of commercially sensitive information; not only technical data about specific components, but also designs, design techniques or other processes that are not usually patented, but rather kept secret.

The second potential problem relates to the early release of “foreground information,” information developed during the course of the project. Although the MOD will have rights of use over such foreground information whenever it has funded its development, the concern for contractors relates to the possibility that, through an SDE, the customer may access data that is still being worked upon. First, work-in-progress foreground information may include commercially sensitive information on company techniques and processes that will not be present in the final data packs delivered to the customer. Second, firms are concerned about liability issues that may be derived from the customer accessing and using data that are still in draft form and not ready for delivery to the customer.

SDEs generate concerns in relation to both of these problems. Because digital data is easy to replicate, systems to monitor and track the information shared through the SDE and strict procedures on data sharing must be established. The establishment of such systems and
procedures is more than a technical problem. Although approaches exist or have been suggested for strict data access control, there is a palpable fear among the staff responsible for IP policy in all the companies interviewed that engineers do not adequately appreciate the importance that misappropriation of “background information” may have for their firm.

Anecdotes abound of engineers that were only too happy to share proprietary and commercially sensitive technical details with their peers in other companies. An example of this is an incident in which an engineer blithely shared the software architecture of the firm’s proprietary process with an engineer of a collaborating firm. Interviewees attributed such behavior to “cultural” traits within the engineering community that drive individuals to share their work with their partners across organizational divides, much in the same way that academics are widely known to do. Although most of the anecdotes belonged to instances in which such exchanges were not always facilitated by electronic networks (sometimes in conversations and data exchanges in paper form) concerns were expressed about what would happen when the digital systems for collaboration are in place that could allow a loquacious engineer to send reams of technical information across to project partners at the click of a button.

All companies were concerned about this problem, albeit in different degrees, depending on the extent to which they saw their competitive advantage as depending upon codified technologies that could be transferred to potential competitors. They all agreed, however, that there is a need to “educate” their engineering staff about the importance of protecting their IP, particularly as inter-organizational collaboration is increasingly being supported by advanced IT.
Convergence of product and process data

An effect of the use of IT in systems design is the confluence of product and process data within the same data sets. This is the case, for instance, in the manufacture of specialized components for aero-engines or for aero-structures, which is driven by unique software-based processes. Naturally companies do not wish to reveal these processes to third parties, but sharing product data in electronic format could imply sharing also software-based processes when product and processes data are inextricably linked. Companies that base their competitive advantage on the uniqueness of their manufacturing processes fear that an SDE could make them vulnerable to disclosure of their trade secrets.

Divergent approaches to IP management and data control among collaborators

To complicate matters even further, defense projects will often involve foreign partners operating within different legal and regulatory environments. This means, for instance, that an SDE will require data control access systems able to cope with the export and technology control regulations in each of the participating countries. As technical data, hence IP is covered under the export control regime of most NATO countries, sharing of IP invariably would come under export control considerations. Collaborating companies have to ensure that data mounted in an SDE does not violate each collaborating partner’s national export control regime. IP management methods will have to be coupled with the technical and regulatory structure emanating from the need to adhere to different export control regulations. Equally, coping with different approaches to IP management across countries is problematic. Firms may not be able to trust the practices of their foreign partners and may decide to withhold information. We were offered examples of firms involved in international collaborative research programs that were not contributing their best IP to the project, which
descended into a situation of generalized mistrust, sub-optimal performance of the project, and in some cases, product.\textsuperscript{13}

A related problem is the lack of consistency in the meaning of the terms used by firms and governments to class the different levels of information protection and access. For instance, terms like “restricted” are interpreted differently among firms. Although we found no cases in which these differences led to identifiable financial losses or leakage of vital IP, our interviewees were adamant about the need for consistency and common use of terms, particularly when structuring an SDE for collaborative projects.

\textit{The responses}

The issues and difficulties presented above may not pose an insurmountable barrier to the introduction of SDEs in collaborative defense projects. In fact, both customers in the defense agencies and their industrial suppliers have been seeking solutions to address the aforementioned problems through four different but interrelated areas:

1. the definition of codified procedures to enable the assured identification of all individuals accessing the system, together with their rights of use across all stakeholders;
2. the establishment of procedures and rules regarding the management of the SDE, and the marking and segregation of the data the SDE contains;
3. the network technologies and inter-organizational systems they support;
4. the underlying \textit{training} necessary to raise awareness of the importance of IP management among stakeholders and to explain the nature and implications of the tools and procedures in place.

The first two areas or aspects, can, in principle, be addressed through \textit{contractual conditions} and associated commitments.
Contractual conditions

Buyers may try to address the uncertainty on the use and sharing of IP and IPRs that follows from the collaboration of diverse partners in the development and production of large complex systems through the inclusion of detailed contractual provisions. In the UK, a wide choice of DEFCONs (“Defence Conditions”) and DEFFORMS (templates for annexes that can be appended to contracts) are available for contract officers to include in contracts. These provide detailed contractual clauses and provisions applicable to a wide set of situations. Table 1 lists the most relevant DEFCONs dealing with IPR, including data access issues.

Insert Table 1 here

Although it is not mandatory for IPTs to include specific DEFCONs within a contract, or to follow to the letter the text within a specific DEFCON, explicit guidance documents recommend the adoption of some DEFCONs in specific contractual conditions. For instance, DEFCON 14 is commonly included in contracts and its use is recommended whenever the contracted work is likely to generate IP. This and other generally used DEFCONs provide, in practice, an established contractual framework that defines the MOD negotiation policy for key aspects of defense procurement, including IPR. Yet it is ultimately the responsibility of the specific contractual team to decide which DEFCONs to include and whether or not to modify them.

While some DEFCONs are relatively straightforward and are applauded by the defense companies for their necessity, there are others that have given rise to serious contention between the MOD and defense suppliers. In part, the differences emerge from the difficulties to cover all possible future events through generic contractual provisions. For instance, many defense systems are used for long periods, extending over three or more decades during which they will be subjected to several planned and unplanned upgrades and changes, for
instance, the customer may require improvements in system capabilities to meet new challenges. Managing these complex systems over such long periods of time gives rise to difficult IP problems. We can distinguish two main sets of difficulties.

First, when there are several units of such systems operating side-by-side (for instance a squadron of fighter aircraft), it is common that the individual systems will have slightly different configurations although they may be formally identified as the same model. In practice, different sub-classes of each model may be identified ex-post by “working backwards” through the different modifications to which the planes have been subjected. In this situation, it is difficult to identify and monitor the ownership of the IP that may be involved in each small change, as well as the components that, being part of the initial system, have been superseded by new ones. A line-by-line definition of the different IPR contained within a complex system may not be possible, and therefore it may remain preferable to stipulate IPR conditions in generic terms.¹⁵

Second, ownership over product data can generate problems with long term system maintenance and repair needs. Contractual conditions try to address this situation. For instance, the application of DEFCON 15 will require from a contractor the supply of a “manufacturing data pack” to which the MOD will have rights of use for the purpose of competitive procurement. DEFCON 15 is only to be applied when the development of a system has been fully funded by the MOD. Yet, today’s highly complex defense systems are likely to include subsystems or parts, or involve processes, whose development has been privately funded. The leading prime contractors we interviewed pointed out that it is very likely that some of the IP that the client requests to be included as part of the manufacturing data pack will be the result of private investment, that is not funded by the MOD. They are therefore anxious not “to give away” data that could be and is likely to be commercially sensitive, particularly if the support and maintenance of the system is not to be undertaken by
the prime contractor, but by a third party. Furthermore, there is a cost to the provision of a
data manufacturing pack that the DEFCON does not appear to contemplate. As product
components and subsystems are constantly updated, keeping a manufacturing data pack
updated entails refreshing the data over the life cycle of the system to take account of the
changes introduced by the prime contractor and its supply chain. This cost, coupled with the
IP problem addressed above, does not appear to be thoroughly recognized by the MOD,
according to the interviewed companies.
The preceding examples show some emerging tensions in the application of IP conditions by
the UK MOD. The root of the problem here is that it is almost impossible to foresee and track
all the contributions, changes, and new requirements that will take place during a complex
system’s long life. Nonetheless, there was a consensus among our interviewees, shared by the
responsible officials at the DPA, that it is necessary to codify procedures for the protection of
IP when dealing with the procurement of complex, long-life cycle systems. In fact some
DEFCONS, such as DEFCON 15 referred to above, have been developed in collaboration
with industry.
Relevant to our article is the “687 family” of DEFCONs and DEFFORMs, which establish
how a “shared data environment” should be operated. For instance, DEFFORM 687C
provides a detailed “Electronic Information Sharing Agreement” setting out the obligations,
responsibilities of the SDE operator as well as user rights and obligations. DEFFORM 687c
was finalized in 2001, after about 18 months of preparation in which both representatives
from industry and from the MOD participated. In addition, the MOD developed a set of
guidance notes to these DEFCONs and DEFFORMs at the request and with the collaboration
of the Confederation of British Industry. These contractual tools can therefore be seen as the
outcome of consensus-seeking process between industry and the MOD, who formally endorse
their use. Yet despite their genesis and wide support basis “Type 45” (more below) is the
only full-fledged development and production program to implement some of the contractual tools in the “687 family.”

UK defense prime contractors see the use of most IPR DEFCONS positively. Most of them have worked well and provided a proven and carefully constructed solution to the needed codification of IP protection procedures. But they also insist that DEFCONS must continue to abide by a principle of equity in which the MOD may not assume ownership of company IP without adequate terms of compensation.

To sum up, the relationship between the UK defense customer and its suppliers when dealing with the development of a contractual system to deal with IP management issues is in a state of dynamic tension and one characterized by a mixture of collaboration and conflict. A continually evolving defense procurement policy, which, in turn, is driving changes in the content and application of contractual conditions, is perceptibly stirring up tensions within the main defense contractors. Still, there is broad agreement on the need to continue with the collaborative approach that has led to the development of some crucial IPR DEFCONs.

Supporting network technologies and inter-organizational systems

The technological foundations and the strategic rationale to deploy IT systems enabling the sharing of technical data information and collaborative working across geographically dispersed sites have been in place for some time. From the early 1990s communities of practice developed around concepts like TDI (Technical Data Interchange) and CALS (Continuous Acquisition Life-Cycle Support) among others. TDI focused on the development of common standards to exchange the electronic files used by different Computer-Aided Design and Computer-Aided Manufacturing (CAD/CAM). CALS was a more ambitious set of initiatives developing guiding principles and associated standard and technology developing activities aiming to create a new type of customer-supply network relationship that would use advanced Information and Communication Technologies to integrate the
different phases in the procurement of a complex system (design, production, support,...) into a continuous relationship. A key element in the implementation of the CALS vision was the creation of a “Contractor-Integrated Technical Information System”: a full technical data set that would accompany a complex system through its life-cycle, from conceptual design to system decommissioning, and would be delivered to the customer together with the system. In an SDE this data set would be available to partners during the system’s design and production.

Initial applications of these principles proved problematic. During the 1990s, the civilian Boeing 777 became the best-publicized case of collaborative design and production across different locations for an aircraft system. Not only was this example heralded as an innovative program for its team management approaches, but was also lauded for representing the first use of digital computers to design and electronically pre-assemble an entire plane. Further, joint design was achieved through a distributed computer network, consisting of mainframes and workstation installations in Japan, Kansas, Philadelphia, and other locations. Yet for all its achievements this IT system fell short of constituting a full-blown SDE in the way defined above. Instead of offering a centralized product database available online to project partners under various access control conditions, the communication between suppliers and Boeing was often carried out using more rudimentary techniques, which in the opinion of an interviewee was because 777 is “old technology” and the prime contractor did not see the need to introduce a more sophisticated IT system for data transmission. According to our interviewees, suppliers would e-mail their designs to the prime contractors sites and vice-versa, a process that was often slow and cumbersome given the size of the file attachments and the low speed of the modem links used. The slowness also caused project participants’ “design deadlines,” for instance, to be delayed because the IT network could not always cope with the volumes of data that was being transmitted. This
meant that file attachments were left sitting “on hold” until the system could clear the backlog of data transmission.

In practice, the diffusion of SDEs using centralized databases accessible to project partners is still very limited. The US-led Joint Strike Fighter (JSF) and the British “Type 45” Destroyer, described in more detail below, are the main examples of involvement by UK defense firms in programs in which an SDE is being used.

In Type 45 the prime contractor (who is not the leading manufacturer but is the systems integrator) is responsible for setting up a centralized product database system to which all project collaborators can have access, and to organize and control different levels of access to each of the “folders” in the system. The system is based on Internet architecture, can be accessed through a Wide Area Network or dial-up connections, and uses a suite of off-the-shelf software applications. In some cases the applications had to be modified in-house to adapt them to the specific needs of the program; this is the case, for instance, with Windchill, a set of software tools to enable a shared, Web-based configuration and document management system.

The prime contractor for JSF is “Lockheed Martin Aeronautics” (LMA), which is both the final assembler and systems integrator, and also a sub-systems and parts manufacturer for the aircraft. LMA has implemented an SDE, which again rests on Internet standards and a combination of off-the-shelf software tools, including “Metaphase” (a Product Data Management program enabling access to an extended supply network) and, again, Windchill (providing a Web access to program management data). LMA controls access to these facilities.

These examples show how Internet standards have been central to the implementation of SDEs in the defense sector. Yet there is a need to tailor the combination of off-the-shelf software technologies and Internet access to the specific needs of each complex project. As
we will see in the next section this still represents a difficult challenge for which no ready-made solution exists and that can be addressed using different implementation models (more below).

Training

The third response to the problems arising from the management of IP in collaborative projects is the need to inculcate in the engineering personnel a staunch sense of the importance of corporate IP. As noted above, all the firms interviewed expressed concern about the allegedly casual attitude of engineers towards the protection of company IP. The ease by which data can be transferred by electronic makes this concern more pressing, especially as the Internet is conventionally regarded as one giant copying machine. To combat this laissez-faire attitude toward the appropriate treatment of corporate IP, some companies have issued guidelines about sharing data across companies, warning employees about inappropriate sharing of data. Penalties for misappropriation of data can include dismissal, fines and even imprisonment. Others have introduced induction briefings on the management of IP and export control regulations, especially for those who are involved in international collaborative projects. However, these training sessions are conducted on a project-by-project basis, rather than as part of a corporate IP management policy. Interviewees unanimously agreed in the need for systematic training of engineers on the importance of corporate IP and the handling of these assets, as part of a company-wide IP policy.¹⁹

**Two implementation models**

As already discussed above, we found few defense programs with British participation in which an SDE system has been put in place. Here we show that the two main cases responded with dissimilar implementation models. They are different in the way the two major
constituents of an SDE solution as discussed in the previous section (the contractual framework and inter-organizational systems) are defined and combined. We can distinguish them accordingly:

1. A “regulated approach” as applied in UK contracts using elements of the 687 series of DEFCONs and DEFFORMs. These contractual conditions were defined by a group of experts from defense suppliers and the DPA and relate to the way in which the SDE will work.

2. A “prime-led” approach as applied in the US-led JSF transatlantic collaborative program. Here the prime contractor controls the definition of the inter-organizational system and imposes it, together with its associated IP conditions, to its international supply chain.

Regulated approach: Type 45 and contractual conditions

The Type 45 Anti-Warfare Destroyer is a large 7350-ton ship designed to provide fleet defense. Six platforms have already been contracted out of a total planned requirement of eight. This is the first full-fledged development and production program to implement an SDE following the approach laid out by the “687 family” of defense contractual conditions (DEFCONs) and forms (DEFFORMs). Type 45 draws upon DEFFORM 687a, which places obligations on the prime contractor to create, and manage a database of project information and make it accessible to users, and DEFFORM 687b, which establishes a “database information agreement” that sets out mutual obligations for all parties accessing it. These forms include IP clauses establishing, inter alia, that uploading data into the database does not imply the granting and unauthorized use of any IPR, and an obligation on the contractor to grant a user license to the customer (MOD) to operate and maintain the database system once this is transferred from the contractor.
Although the responsibility for creating and managing the SDE can be vested in a third party, in this case it is the prime contractor, BAE SYSTEMS Electronics Limited, who is in charge of setting up the SDE. This is one of the responsibilities of the “Prime Contract Office” (PCO), but it has involved other partners and stakeholders in the development of the system:

- through the application of DEFFORMs that are themselves the result of a process of negotiation among many industry stakeholders and Government.

- the PCO has drawn on the input from main stakeholders, which include five main supplier firms and the program client, the Defence Procurement Agency. These six organizations, which have access to the SDE through a dedicated Wide Area Network, were involved in defining the SDE, its applications and management, and the user practices. This process is conducted through an “Enterprise Integration User Group,” which comprises representatives of all the main stakeholders, who is responsible for overseeing the system implementation across stakeholders, and reviewing and updating the enterprise integration strategy. The resulting “Enterprise Integration Implementation Plan” affirms that IPR previously owned by a stakeholder will not “normally” be published in the SDE, and that, if it is, such “background IPR” will be protected by access controls and made accessible only to the required stakeholders.

The Type 45 SDE is however limited in the extent of the applications and data exchanges it supports. The system carries extensive information on project management tasks, and provides a tool for sharing project information across several participating firms and the client representatives. Yet the use of the system is limited to information that does not have a classification of “Confidential” or higher national security restriction, a classification of which is not unusual in defense projects. Technical data published in the SDE includes graphical representations of the “product geometry” and results in a “product model” that can be used to guide the evolving design within the collaborating firms. However, detailed design
data, as for instance the CAD files used for the design of the different elements are not shared through the SDE.

Despite these limitations the Type 45 SDE presents a new stage in the extent to which collaborative tools based on IT have been implemented to facilitate the collaboration across organizations involved in the development, production and operation of a complex product and the management of stakeholders’ IP. The system has now been in place for almost five years, has become a key tool in the management of the program, and is delivering the services to the PCO and its client.

It must be noted that the complexity inherent in setting SDEs is magnified when it involves international partners. For instance, participants in the Type 45 SDE pointed out that one of the reasons why the system operates with relative simplicity is that is a domestic project and that no foreign suppliers may access the system. The main reasons for the added complexity when dealing with international programs are the need to deal with complex export control legislation and to accommodate different national regulations on issues like IPR and privacy. The JSF case discussed below provides an example of the challenges faced when international collaboration is organized around an SDE.

Prime-led approach: the case of JSF

As discussed above, LMA, prime contractor for the JSF system has set up an SDE using a number of available digital networking technologies. For the suppliers this is a mandated system, imposed as a condition for collaboration and in which the prime contractor, who manages and controls the SDE, defines and establishes architecture and procedures. The SDE revolves around a Joint Data Library (JDL) that serves as the node for the sharing of technical data across project participants. Ownership of data in the JDL is indicated by restrictive agreed legends, which are included in the footer of all data and drawings. Access to the JDL is established through formal agreements, so-called Technical Assistance
Agreements (TAAs) between LMA and its suppliers. TAAs provide the formal approval mechanism enabling stakeholders to post and access data in the SDE and specify the kind of data that can be accessed and used by the supplier. TAAs have become a very complex tool to operate, particularly when they involve foreign (non-US) suppliers. Often several TAAs are signed with each supplier covering different sets of data for which the supplier acquires rights to upload and download. In particular, when the suppliers are foreign nationals such TAAs have to take into account existing US export control regulations and establish the relevant data access control accordingly. One the one hand this has a positive effect: as access to the JDL requires a TAA and, therefore, takes into account export control regulations. Data accessible by a partner through the JDL is, in practice, approved for transfer abroad in accordance with existing US export control regulations. On the other hand the system has become cumbersome to operate. For instance, a British firm participating in the program has signed over 160 TAAs covering, among other things, different requirements relating to the export and re-export of the technical data in different components and sub-systems. Furthermore, any data communication between two suppliers has to be approved by the prime contractor, regardless of the TAAs signed between the two suppliers and the prime.

Accordingly the JDL is partitioned: suppliers cannot access the project data of other suppliers, only LMA as prime contractor has access to all data and information in the JDL. Further, when a supplier is involved in different subsystems it will access different and separated folders under different TAAs. This means that different parts of a corporation working on other sections or aircraft sub-systems will not have access to each other’s data sets within the JDL. Again this has positive and negative effects. On the one hand, each supplier has its own set of folders containing its own information, which acts as a means of IP protection, avoiding potential confusion as to what information belongs to whom. On the other hand, the system slows down collaboration across suppliers. If a company needs data...
from another supplier, it will have to request it from the prime contractor, who will then “post” the information in a common folder available to both companies, after checking that the requested information is available and indicated on the TAAs signed by both companies. Last but not least, the management of the access control at individual level is even more cumbersome. Any supplier employee wishing to access JDL data will have to request permission from the prime contractor, who then manually checks whether the individual is covered by a TAA and what are the rights that this TAA establishes. Once this information is ascertained the prime contractor provides access to the relevant project folder or folders. Yet the onus is on the individual to ensure that the information or access rights it needs are listed on the relevant TAA. Participating companies have had to train the employees working on this system on the complex operating procedures by which it is regulated.

Summary

The need-to-know data access controls, the TAAs and the physical checking by the prime contractor for releasing information and data to each project participant, and the segmented folder structure in the JSF SDE represent the collective means to manage the IP of participating collaborators. Unwieldy as they may appear to be, it becomes apparent that in international collaborative projects, the issues of export controls and IP are co-mingled and that an SDE to support such collaboration will need to consider these dimensions, bearing in mind that export-controlled items also contain an array of IP and IPR. These considerations return us to the observation that an international collaborative SDE will be complex, but one whose difficulties may not be insurmountable. In this, however, apart from the construction of a robust IT system, the procurement authorities may jointly need to “harmonize” their treatment of IP used in and resulting from the collaborative project. Alternatively, industry can also try to establish guidelines for the management of future joint projects.20
In comparison, an SDE participated by domestic collaborators is less complicated, although as has been noted in the Type 45 case, an assortment of controls and procedures to manage the participants’ IP has been instituted. However, given its relatively “smaller” size and national character, it is questionable whether this type of SDE would be “scalable” for larger international projects.

**Managing IP in collaborative SDEs: some lessons**

This article has attempted to extend the current literature on corporate management of IP by exploring the issues that arise from inter-firm collaborative projects using SDEs. As noted earlier, the literature on this topic has primarily focused on how firms manage their IP within the firm. As well, there is a paucity of studies on how firms use IT to manage their IP. Nonetheless, it is evident from our research that, in the context of changing procurement practices, IP and commercial managers view with concern the way IP is going to be managed within new inter-organizational collaborative frameworks.

The two cases we have briefly discussed present two contrasting examples of the ways in which SDEs can be implemented in collaborative projects and IP managed within them.

- JSF represents a more complex program as it involves a large supplier network distributed across several countries. British suppliers participation in JSF’s type of SDE is more of a contractual imposition from their client than as a tool to help them in their tasks. They have had no participation in the definition of the system, taking as a given the conditions for participation. The SDE provides an avenue for communication with the prime contractor (LMA), but communication with other suppliers through the SDE has to be explicitly allowed by the prime.

- In comparison Type 45 has a much smaller number of partners (only six directly linked to the Wide Area Network) all of them located in Britain. In comparison with the JSF’s
hierarchical structure, the Type 45 SDE has developed a more collaborative environment, although responsibility for the SDE design and management remains with the prime contractor.

The restricted nature of the JSF SDE reduces the chances for leakage of IP through the electronic network and simplifies the IP management process. In the Type 45 SDE the threat of leakage is minimized given the nature of the data being exchanged. The system is intended to share only information generated by the project (foreground information). As background IP is kept outside of the scope of this kind of SDE, concerns about IP leakage and misuse are reduced.

Indeed, limiting the scope of this type of SDE and its functionality had lowered the risks and associated concerns. During our interviews it became apparent that, as far as IP management was concerned, the combination of contractual and technical solutions offered by this SDE was considered satisfactory. This is logical: had there been strong concerns about the management of IP within the digital environments being created, the system would not have been implemented. Yet, the construction of this SDE was based on a system that allowed the exchange of a limited set of data types or where accessibility to the data stored in the central repositories was severely restricted.

How can the scope of an SDE be extended so that the potential offered by IT to organize and co-ordinate complex design and engineering tasks across organizations be fully exploited, at the same minimizing IP misappropriation and leakage? The problems that our study has unveiled suggest actions that can expand the scope and functionality of future SDEs.

As we have seen, an approach to prevent unauthorized data access is to segment the data in the central database into different folders. Each participating organization will have access only to its own set of folders. This, as we have seen, can slow down collaboration among
suppliers. If a company needs data from another supplier, it will have to request it from the prime contractor, who after following an established set of procedures will “post” the information in a folder accessible to both suppliers. These approaches, managing information at the system level, are operationally convoluted.

The alternative is to administer the system by tagging each data element with information including its origin, security, commercial confidentiality markings, and access restrictions, and then linking the access rights of individuals to the markings. This requires a parallel identity and access management system, in which all individuals must have proof of identity to log on to the system. Access will depend on the individual’s organization, role within the organization and any other factors, like nationality, with a bearing on the definition of his or hers access privileges.

Such “data level” management system would allocate access rights automatically thus eliminating the need for a manual management of access privileges. The technologies and procedures to set up such a system exist. For instance, proposals have been put forward establishing detailed procedures to tackle security concerns and export control regulations in transatlantic arms collaboration programs. Further, experts interviewed for this project believe that the technological capabilities to set up sophisticated SDEs based on “data level” access management have existed for some time.

Yet, as we have seen present implementations have established for themselves modest objectives and operate at levels of functionality lower than that allowed by existing technologies. The main challenge for the establishment of an SDE is of a managerial nature, a point that has also been highlighted in a discussion on information security. Management of IP within SDEs depends primarily on three aspects: (1) commitment to an IP policy, which institutionalizes clear guidelines and codes of practices on the treatment of corporate IP, including training of research personnel; (2) the establishment of adequate processes for
marking and management of data and access control; and (3) recognition that a corporate policy entails integration of input from the IT, legal and commercial departments into its definition. These three dimensions generate up front costs and require a coordinated inter-organizational approach to IP and data management – the decision to embark in such initiatives will lie on the corporate executive tiers above the IT, with legal, and commercial departments in charge of implementing the system.

The first dimension flags out the point that management needs to deal the non-technical issues that can emerge when setting up SDEs. In particular, our study revealed that commercial and IP managers were particularly concerned about those aspects of IP management that are more difficult to control through contractual or technical measures. Disquiet was evident among all firms interviewed about the way in which engineers and designers were treating the information they were working on and the results of this work. There was a high perceived risk of leakage of technical drawings, designs, and other types of data as engineers involved in a collaboration were perceptibly willing to share them with colleagues from other companies. This risk is amplified by the capacity to copy and transmit data afforded by IT, but it is not necessarily linked to the way in which these facilities are integrated within an SDE. An SDE with a limited functional capability like that of the JSF discussed here offers little additional avenues for data leakage. The risks posed by project employees who are not aware of how to treat technical data may or who have no guidelines concerning the importance of specific information assets, however, could impede the implementation of more open systems and suggests the need for rigorous IP management policies and procedures to initiate these actions.22

Furthermore, although technical approaches to deal with this problem exist, such as the incorporation of “data level” access management into each document’s access controls to prevent unauthorized access upon release of a document, there is a need for a corporate IP
management policy to address training and raise awareness of the importance of blithe sharing of data. A corporate policy needs also to consider company wide processes and procedures for the treatment of company IP that is not formally protected and not focus on the protection mechanisms themselves, for instance, to patent or to keep a particular IP a trade secret.

Moreover, as different SDEs are created for different projects, there is a possibility that in the future, the same company will be involved in several SDEs using different systems, contractual conditions and IP sharing rules. Such complexity also calls for better training of research personnel in the treatment and management of IP, lest it result in incoherent IP management practices. Therefore, training on IP management in digital collaborative environments needs to rise above its current project-by-project approach. A corporate IP management policy should systematically address these issues and establish procedures and behavioral guidelines with respect to the treatment of IP and information.

Regarding the second aspect, technical solutions require detailed definitions of the access rights of the different types of users, security procedures that the users have to abide by, and the rights and responsibilities of the IT systems managers, backed up by adequate network technologies able to deliver the functionality needed to implement such a system.

Third, and importantly, a corporate IP management policy sits at the interface of IT strategy, commercial and contractual policies, and engineering and design practices. While it is necessary for commercial and legal personnel to “steer” the policy, it is the engineers and technical personnel who will, eventually, be responsible for their implementation. We have found the interaction between these two groups of people often tenuous. For instance, the Type 45 Enterprise Integration Plan establishes mechanisms to request the opinions of SDE users on the operation of the system. This is an example of a good management principle: such a policy provides an information channel between engineers using the SDE and those in
charge of its management. Yet, it follows established practice in that it falls short of bringing together engineering, IT personnel, commercial and legal communities in the definition of an IP policy approach. It must be noted that in ensuring that IP is properly protected and used, and data access effectively controlled in an SDE, contractual obligations, IP practices and IT architecture must be inextricably linked. This requires close collaboration between the commercial/legal and IT departments, and therefore needs to be led from the corporate executive level. Lapses in this collaboration would likely lead to an inadequate IP policy.

In more general terms the establishment of inter-organizational networks needs to account for the legal and regulatory environment within which SDEs operate. Experts that had participated in the development and, now, operation of the Type 45 SDE believed that its implementation had been made easier because of the national character of the program. An international project would be much more difficult to manage and would probably result in more modest functionality (as in the case of the JSF project). The requirements imposed by export control regulations will affect the architecture of an international SDE. Such difficulties are, however, not unique to defense projects; many high technology programs will deal with controlled technologies and will be subject to the same constraints regardless of their military or civilian character. The influence of regulatory constraints on the nature and structure of SDEs is crucial although it is often overlooked in the literature on inter-organizational networks.

Our study has argued that the nature of the IP challenges posed by the implementation of SDEs requires the commitment and support at the corporate executive level. Yet, IT implementations are viewed by project directors as additional costs rather than investments for the future, and it is often difficult to attribute specific monetary benefits to the introduction of these technologies. When in 1995 one of us carried out a study on the diffusion of CALS principles in the UK, an expert in a major defense firm stated that the
industry displayed “a file transfer rather than an open database mindset.” This situation appears to continue today. We cannot ascribe this situation to the impossibility of protecting IP management within such collaborative IT networks neither can we blame the technological difficulties in establishing open database architectures to underpin collaboration. The procedures and underlying technologies to establish the networks and protect IP exist. Their slow diffusion could be attributed to the detachment with which corporate executive deal with the details of IT systems to be used in specific projects. Yet to bring together the commercial, IP and IT functions within the company and across the different partners in a collaborative project, and to support the establishment of “shared data environments” an executive drive is needed.
### Table 1 DEFCONS relevant to IP management

| DEFCON 14 | Inventions and Designs – Crown Rights of Ownership of Patents and Registered Designs |
| DEFCON 15 | Design Rights and Rights to Use Design Information |
| DEFCON 16 | Repair and Maintenance Information |
| DEFCON 19 | Free User, Maintenance and Supply of Drawings |
| DEFCON 21 | Retention of Records |
| DEFCON 90 | Copyright |
| DEFCON 91 | Intellectual Property Rights in Software |
| DEFCON 126 | International Collaboration Clause |
| DECON 531 | Disclosure of Information |
| DEFCON 632 | Third Party Intellectual Property Rights – Commercial and Non-Commercial Articles and Services |
| DEFCON 687a | Provision of a Shared Data Environment Service |
| DEFCON 687b | Shared Data Environment System Transfer Arrangements |
| DEFCON 703 | Intellectual Property Rights – Vesting in the Authority |
| DEFCON 705 | Intellectual Property Rights – Research and Technology |

---

1 The research for this paper has been jointly funded by the UK Economic Social Research Council “E-Society Programme”, and the UK Ministry of Defence under the Joint Grants Scheme (ESRC Award Reference RES-335-25-0017). Authors gratefully acknowledge the comments of the executives of the defense companies interviewed, Prof. J. Adams and Robert Shields, Director, UKCeB. Responsibility for errors are solely ours.


Here we use the term “network” to refer to a group of organizations collaborating within a specific large project. “Network technology” is the technical information and communications infrastructure that supports the network, and an “inter-organizational system” refers to the applications shared by the network through its network technology.


Only one firm interviewed had a clearly articulated IP management policy supported by an IT system. This is used to track which patents were used in each of the firm’s products, so that the firm can monitor where and how patents are used and also to identify infringements.

To prevent similar incidents in the future, the former firm has begun instituting IP management training sessions. Yet, this is a project-based initiative rather than a corporate IP management policy.

Companies that saw their competitive advantage as based on their capacity of being “first to market” were relatively less concerned about the possibilities for competitors to copy their technologies and designs.

The practice of holding back one’s best technology when contributing to international collaborative programs has long been pointed out as a main problem in international arms collaboration.


However, there is a debate in the field of relational contractual theory as to the extent to which contracts can and should be written to address all possible eventualities in a complex, long-term project. Contract theorists have argued that contract is not an abstract formalistic mechanism, but one that typically involves development of relationships that go beyond the terms of a contract and evolve through the course of the project. Ian R. MacNeil, "Relational Contract Theory: Challenges and Queries," *Northwestern University Law Review,* Vol. 94, no. Issue 3 (1999): 877-907, Ian R. MacNeil, *The Social Contract* (London: Yale University Press, 1980). The
practice in defense contracting, however, has tended towards the detailed specification of conditions and deliverables trying to cover for all possible eventualities.


18 Yet a very sophisticated IT system for technical data sharing across U.S. partners, project design and engineering has been described and analyzed for the B-2 Stealth Bomber, an aircraft design and manufacturing project that predated the 777 by several years N. S. Argyres, "The Impact of Information Technology on Coordination: Evidence from the B-2 "Stealth" Bomber," Organization Science 10, no. 2 (1999): 162-80.

19 The need for training was also highlighted by ASIS, whose report also found that there was little evidence of training and awareness of information security in the U.S. ASIS International, PricewaterhouseCoopers, and American Chamber of Commerce, "Trends in Proprietary Information Loss. Survey Report," (Alexandria, VA: ASIS International, 2002). The report also found that proper labeling/marking and handling of classified information are the norm among companies, nor are employees typically trained to safeguard proprietary information in the office or while traveling.


22 According to an ex-commercial and contracts director and now consultant to defense companies, the potential of increased “tort risks” from damage to or leakage of data would otherwise be too high.
23 We found examples in our research where sophisticated international product data management and sharing systems proposed by the IT contractors in large international collaborative programs were unlikely to be accepted by the participating firms because of their cost.