**Workshop on Security and Privacy in Collaborative Working**

# Intellectual Property Management in Cross-Organizational Collaboration

Martijn Warnier[1], Stephan Lukosch[1] and Dominic Heutelbeck[2]

[1]Delft University of Technology
Delft, The Netherlands
[2]FTK - Forschungsinstitut für Telekommunikation e.V.
Dortmund, Germany
M.E.Warnier@tudelft.nl, S.G.Lukosch@tudelft.nl, dheutelbeck@ftk.de

The design and production of mechatronic products is multi-disciplinary as well as multi-organizational. In order to get the product to the market different companies have to collaborate. The possible scenarios in which such collaboration may take place are manifold. Possible roles of the companies include equal partners, supplier, OEM, etc. In each project, the constraints under which a product if designed vary and if a new partner enters a project the constraints may change radically. This abstract sketches a possible approach for handling cross-organizational collaboration projects.

A central problem in such a cross-organizational collaboration is the fact, that while the partners have to collaborate in one project, the same partners may be in competition regarding a second project. Thus, the mutual trust level strongly depends on external criteria and companies have to take careful measures not to expose critical intellectual property (IP) which may be found in product data streams shared within a project. As illustrated in Figure 1, in a case of complete mutual trust with no risk of competition, companies can completely expose their product data streams, including full designs, simulation data and streams from products in use. This scenario is called white-box shared IP. The second case is more complex, if the risk of competition is present, or the general trust level is low, fine grained control over the exposure of product data streams is required. The two companies have to make a trade-off between ease of collaboration and the protection of their individual intellectual property against misuse. These two interests are in direct conflict, as collaboration is most efficient, if access to the mutual data streams is unlimited which in turn results in the direct danger of exposing ones IP. On the other side of the spectrum, the IP of the individual companies is most secure, when no access is granted at all,

which makes collaboration impossible. In order to create a feasible trade-off, the two parties have to establish fine grained rules, policies, and IPR management.

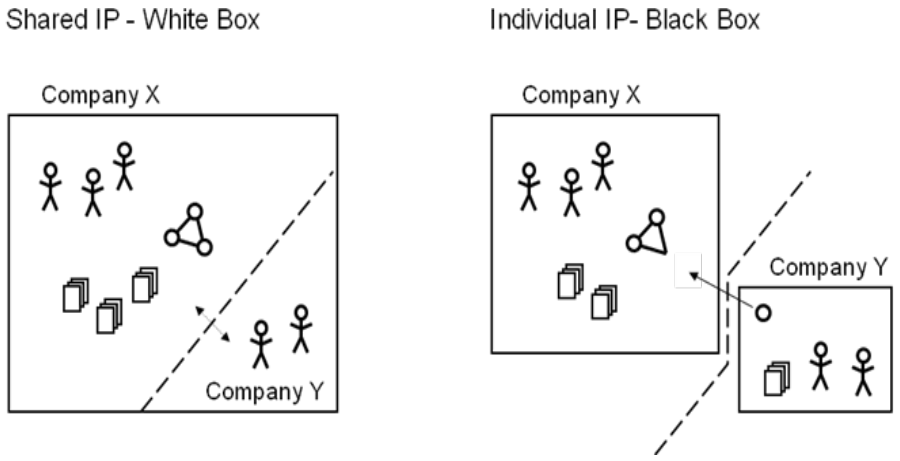


Figure 1: Cross organizational collaboration and IP protection.

The protection of intellectual property is in fact an upper layer problem of cross-organizational collaboration. To be able perform cross-organizational collaboration the partners have to follow five steps:

**1. Use a shared vocabulary**, i.e., share an ontology that captures the necessary concepts to perform the cross-organizational collaboration. There are three different ways to organize this. The organizations can (i) use the same ontology, (ii) merge ontologies or (iii) map their internal ontology to a shared ontology. Option (i) would be ideal, however this is not very realistic and doesn't scale if multiple organizations have to collaborated (in one or multiple projects). Option (ii) could work, though ontology merging is not straightforward. Moreover, this would lead to a different shared ontologies per collaborative project, which hinders interoperability. For example, if a third company joins two other organizations that are already collaborating they have to re-merge their ontologies. Therefore option (iii) is preferred. A lightweight core ontology has to be designed for this. The ontology should be designed to allow the individual companies to match their internal systems to their individual requirements and culture, while ensuring interoperability by using the core ontology.

**2. Agree upon a social communication protocol**, that enables the organizations to share information based on the core ontology defined in step 1. The protocol should also allow local access control enforcement which lets companies decide which information to share with partners.

**3. Establish trust levels**, between collaborating partners. Partners should agree on what information needs to be shared for the successful completion of project, and what information should be protected for IP reasons. The latter information should only be accessible by employees of the company that has the IP rights to the specific information.

**4. Specify rules and policies for access control**. A two-tiered access control model is used for this. On the first level a shared role-based access control (RBAC) policy can be defined on a per collaborative project basis. This role-based access control policy will be defined for the duration of the project. It would include information such as 'an engineer can alter everything in the sub-project he works on, can only read information that is relevant for the whole project and cannot access information in sub-projects' or 'a project manager can read all the information in the project'. The role-based access control policies define the global information that is necessary for an efficient collaborative process. The policy will typically not change for the duration of the project.

The second level of the two-tiered access control system is formed by access control lists (ACLs) on specific information (documents, film etc.). These access control lists can be used to narrow the access level set by the global RBAC policy. So, for example, even if all engineers can read some information as defined by the global RBAC policy, an ACL can be used to limit the access to a specific engineer. The ACLs are typically used on only a fraction of the information, since for most information the RBAC policy will suffice. Moreover, ACLs can be changed easily, by the owner of the information, which makes it easy to change access control dynamically, without violating the global RBAC policy. The latter can be very useful as situations can change during the collaborative process.

**5. Collaborate**. Using the approach outlined above.

This abstract sketches an approach for cross-organizational collaborative projects that allows flexible control of information access enabling IP-management in shared projects.