

A GUIDELINE TO ORGANIZE COMMUNICATION INFRASTRUCTURE FOR ALLIANCES OF SME

Ph. Beaune¹, F. Biennier², E. Marcon³

(1) Ecole Nationale Supérieure des Mines de St-Etienne - Centre SIMMO
158 cours Fauriel, 42023 Saint-Etienne Cedex 2, FRANCE

Philippe.Beaune@emse.fr

(2) INSA de Lyon - Laboratoire PRISMa / IF502 - F69621 Villeurbanne Cedex, FRANCE

Frederique.Biennier@insa-lyon.fr

(3) LASPI – Univ. de St-Etienne - 20 av. de Paris - F42334 Roanne Cedex, FRANCE

Marcon@univ-st-etienne.fr

Information and communication technologies can be seen as driving elements in virtual enterprise organization. As far as alliances of SMEs are concerned, the required infrastructure must be light, with a rather low cost. To choose an acceptable infrastructure organization, a multi-criteria analysis describing the technical requirement and the way the virtual enterprise organization is perceived and integrated by each partner is proposed and can be used as a generic guideline to define adapted security policies in each enterprise..

1. INTRODUCTION

Alliances of enterprises appear as flexible and reactive organizations, gathering complementary or concurrent partners. Such organization performances are heavily related to the synergy between partners. Such organization are built for a particular project or for a longer period, and involve to adapt models and collaborative work strategy to this multi-enterprises context so that flexible organization could be built to preserve each enterprise autonomy and favors the emergence of the global synergy. This relies on a convenient infrastructure including both collaborative work support systems, shared information features and adapted communication infrastructure. Formal co-operations are mainly described thanks to well-identified and organized business processes. Such processes can be described precisely, optimized in a business process reengineering approach. Yet, as each entity has also its own business processes, “organizational conflicts” can be identified due to the potential differences between the alliance and the enterprises own strategies. An integration point of view involves that the alliance members use either the same software tools or at least tools with common interface. Such a formal point of view brings a reduced view on the alliance activity: partners co-operations are limited to consumer/provider relationships. Moreover, indirect (or informal) co-operation

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35585-6_68](https://doi.org/10.1007/978-0-387-35585-6_68)

favors the alliance “synergy”: by sharing different information, even intermediate results, the alliance members can adjust continuously their activity to the exact context. These requirements involve an information-based integration instead of a precise organization of the activities. Information flows reflect the global process without focusing on the exact internal organization of each process and the common information system allows information and experiences interchange even with indirect communication so that both direct and indirect co-operation can be supported.

Enterprise engineering or information engineering processes represent long and high cost projects that do not fit SMEs reactivity and flexibility requirements and potential level of investment. Standard solutions provided for such small companies need to be adapted to the alliance context. After a description of the different implementation of distributed information and decision systems, we will present how “inter-enterprise” network organization can be perceived to fit in the organization of the virtual enterprise, i.e. the alliance.

2. DISTRIBUTED ORGANIZATIONS

Organizing a virtual enterprise or an alliance of enterprises involves taking into account different decision centers: as each partner keeps its own autonomy decisions are often distributed among them. Potentialities carried out by information and communication features favor the organization flexibility: as the necessary information can be brought at the right time to the convenient person, several decision organization can be designed to fit the best the management requirements (Malone 1997). To achieve this, different logical infrastructures can be designed:

- An **“integrating”** (or even a “universal system”) **point of view** can lead to an organization based on an ERP system: such a system integrates all the enterprise information (in a centralized database) and can support a distributed decision system provided that each decision center can have access to the ERP information system. This rather high cost solution, provides poor interfaces to be used with other systems so that this organization is rather “closed” and involves that all the partners use the same ERP tool.
- An **“open” infrastructure**, where each partner can use its own tools, can be set according to different distributed architectures:
 - An **EDI-based organization** provides both specialized standards according to the exchanged information — as STEP for CAD information (Giachetti 1999) or XML for documents or business information (Li and Su 2000) — and a precise description of the processes organizing these inter-firms exchanges. These interchange contracts bring a legal and formal organization to support formal inter-organization co-operation.
 - **E-market-place** can be seen as EDI descendant (Unitt and Jones 1999). It consists in a lean infrastructure supporting direct interactions between clients and suppliers thanks to the Internet (Ordanini and Pol 2001, Fariselli et al. 1999). New developments provides a real business

support, instead of a simple product catalog (Mott 2000). Nevertheless, their diffusion as a common “business tool” is limited due to security problems that should be solved at different levels (database, cryptographic systems, communication network security...) (Davidson 2001). Such an architecture offers an open framework for business relationships. Yet, they show poor abilities for “informal co-operation” as well as for process management.

- **Distributed IT architectures** (using CORBA, DCOM or EJB supports) favor indirect co-operation of applications thanks to shared information systems. Coupled to exchange standards as STEP for CAD data for example (Zhang et al. 2000), they provide an open framework that can support both indirect and direct co-operation. Nevertheless, such “shared memory” infrastructure — as the one developed by (Sandakly et al. 2001) — relies on a rather detailed knowledge of the different information systems organization. Moreover, information systems protection (i.e. information integrity, confidentiality, access control...) must be taken into account the security policy of each partner.

As far as communication infrastructure is concerned, Internet based solutions appear as a convenient organization. The different networking abilities (file transfer, remote connection, email, web based applications...) can be integrated for each node to provide a comprehensive distributed architecture, as in the PRODNET project where each enterprise “node” is modeled to integrate all together the communication, security, authentication and cooperation features (Osorio and Barata 2001).

As far as SMEs are concerned, project rather long duration and heavy costs can be seen as major defects so that standard solutions are often proposed after a reduced engineering process. According to these constraints, significant improvements can be achieved by capitalizing basic requirements and “standard” needs from different case studies (Taylor et al. 2001). Despite of these different works, a missing link emerge between the generic logical organization of the distributed system and the standard solutions offered: the way the physical implementation is chosen reflects management options. Coupled to a super-structure organization (in our case an alliance of SMEs), the physical organization of the distributed system reflects the importance given to the virtual enterprise organization. According to different parameters as the alliance expected duration, the potential level of investment, ..., different physical implementation can be set (Biennier et al. 1999):

- **For a well identified alliance with its own management strategy and computing resources**, a client/server architecture can be implemented: the information system is organized on the alliance main server and each partner system considered as clients. This solution favors the alliance identity, provides an open frame for the collaborative work. Common tools can be shared as well as the information system so that a high level of integration is reached as proposed by (Wicaksana and Adibroto 1995). Nevertheless, this centralized approach involves that each partner manages both own systems and the alliance systems so the local management of the different processes are not obvious. Consequently, a groupware based organization can be implemented instead of this strict client/server architecture (Liang et al. 1994). The groupware level provides a more flexible organization and allows a supervised distribution of the

information system among the members of the alliance so that the alliance information system could be “integrated” in each entity own processes.

- **For well-defined co-operation in an alliance without resources**, a generalized EDI approach can be used: interchange contracts between partners can be used to define exactly the information flows and control processes. In this case, the alliance information system is split among the partners according to the information interchange agreements. In this approach, the alliance information system is strongly coupled to each partner information system but this approach is rather limited to formal co-operation and does not provide a flexible architecture. Informal collaboration can be taken into account thanks to other information exchange or by adding collaboration tools as video-conferencing systems, messages management...
- A last solution consists in **distributing the alliance information system among the different partners**. Information flows are implemented as file transfer or companion message and the information property is transmitted to the entity in charge of the information processing. At each time, the different partners can have a global view on the information system and have access to the different pieces of information. This solution shows a high level of flexibility. Information flows are used to implement formal co-operation whereas direct accesses to the convenient pieces of information implement indirect co-operation. As no interchange agreements are defined, the information flows description must be included in the information system so that each entity can identify them.

Moreover, all these IT solutions require adapted communication abilities. The network physical infrastructure organization is often seen as a key point in a security policy and reflects the organization strategic choices. Consequently, this distributed architecture organization must be extended to take into account recommendations on the network physical organization.

3. BUILDING A COMMUNICATION INFRASTRUCTURE

Building a communication infrastructure can be seen at two different levels:

- **Distributed application**: this point of view consists in defining a generic communication node architecture. In this case, an internet-based network communication, as proposed in the PRODNET infrastructure (Osorio and Barata 2001), or a value-added network coupling information and network providers (Oh and Chang 2000) provide standard “ready to use” solutions but do not take into account enterprises security policy.
- **Communication network** point of view points out the way the communication network is physically organized. The network engineering process must be adapted to fit the virtual enterprise particular requirements:
 - first, the communication infrastructure must include both LAN and WAN aspects;
 - second, as different enterprises co-operate, a particular attention must be paid to security requirements;

- last, the virtual enterprise infrastructure must be super-imposed to each enterprise infrastructure.

In order to guide the design of the network infrastructure, we propose a pre-diagnostic framework, integrating generic infrastructure elements and a multi-criteria analysis process to select them. To achieve this, we have organized the networks elements into two families: “clients” and “servers”. “Clients” nodes will have access to shared information and application thanks to “server” nodes. The different architectures reflect the integration level of the computer systems of the different enterprises vs. the alliance own system. To guide the analysis, we propose a typology of the potential clients and server nodes:

- **“Client nodes”** are characterized by the workstation definition and the way it is remotely connected to the “server” node (figure 1):
 - C1: standalone computer remotely connected through modem or an ISDN adapter to the server node
 - C2: a computer remotely connected through modem or an ISDN adapter to the server node but configured to implement a proxy server that will be used by computers belonging to the same LAN.
 - C3: a local network directly interconnected to the server node thanks to a router.
 - C4: a secured local network with a secured connection to the server node.

	“Client” model				Connecting equipment		System
	Stand-alone computer	Cluster & “Proxy”	LAN	Protected network	To the LAN	To the WAN	
C1	X				None	Modem / ISDN adapter	Client
C2		X			Hub/switch	Modem / ISDN adapter	Server
C3			X		Hub/switch	LAN/ISDN router	Client
C4				X	Switch + Firewall	LAN/ISDN router	Client

Figure 1 - “Client nodes” description

- **“Server nodes”** are characterized by the way they are connected locally and remotely (figure 2):
 - S1: a standalone computer only connected through remote access features as pool of modems or ISDN adapters. This computer is disconnected from the enterprise own network and involves, even when they are used locally, a phone connection.
 - S2: a remote access server, protected by a firewall, is set to allow remote connection to the LAN where the application servers are connected to. Access controls are implemented on each resource connected to the LAN.
 - S3: A VLAN architecture interconnecting several LANs thanks to ISDN routers. As in the previous case, access controls are reduced to those implemented on each resource.

- **S4:** A secured VLAN interconnecting several LANs thanks to routers and firewall is set. It may also include a remote access system based on pool of modems or ISDN adapters to connect remote standalone computers. The global security policy is taken into account thanks to the different firewall configuration and different protected / unprotected areas (DMZ) are built to protect the different areas of the information system (company own information system, alliance information system, ...) as shown in (Biennier and Favrel 2001).

	"Server" status			LAN connection		Remote client connection		LAN Equipment
	Stand alone computer	Protected Computer	Free computer	Protected	Free	Remote access server	Router	
S1	X					X		
S2		X			X	X		Hub/switch
S3			X		X		X	Hub/switch
S4		X	X	X		X	X	Switch

Figure 2 - "Server nodes" architectures

Designing the global communication infrastructure requires first to define the way the different component can be interconnected (figure 3) and give a guideline to select the convenient components. For this purpose, we have proposed a form describing the computerization level of the different companies, the used software and hardware used, their needs for collaborative work support, as well as the way the alliance is perceived (GRECOPME 1999)... These results are then used to select convenient nodes architecture according to few criteria. These criteria are gathered into three main discriminant clusters describing different points of view on the alliance:

- **Alliance liveliness:** this cluster is used to capture both the alliance planned duration (useful to evaluate the potential level of investment) and the alliance stability, i.e. the sensitivity of the proposed solution towards partners evolution
- **Enterprises computerization level:** this cluster gathers both objective and quantitative information (available equipment level, evaluation of the heterogeneity of the different systems...) and more subjective ones (as the computerization culture of companies). These last ones are used to evaluate the importance of the support and training periods.
- **Culture and management:** this cluster takes into account the way the security of the information system is managed (organization of shared access, confidentiality, ...), the available financial means as well as the importance of the alliance management policy (integration factor) vs. each company own policy.

Figure 4 presents briefly the importance of the criteria in the node type selection (from 0: not important to 3: very important). The final quotation was adjusted thanks to a distributed groupware-based prototype that allow us to show the possibilities carried out by the different types of nodes. Other criteria, as geographic implementation, number of interconnected sights, potential evolution of the alliance, etc., are not discriminating to choose one or the other node type. They must be taken

into account at the detailed design step to adjust the network capacity and the configuration of the access control according to a precise security policy.

Clients Servers	C1	C2	C3	C4
S1	Compatible	Compatible	IMPOSSIBLE	IMPOSSIBLE
S2	Compatible	Compatible	IMPOSSIBLE	IMPOSSIBLE
S3	IMPOSSIBLE	IMPOSSIBLE	Compatible	Compatible
S4	Compatible	Compatible	Compatible	Compatible

Figure 3 - Possible connections between client and server nodes

Main criteria	Criteria	"Client" component				"Server" component			
		C1	C2	C3	C4	S1	S2	S3	S4
Alliance liveliness	Duration	0	0	2	2	3	1	2	2
	Stability (partnership evolution)	1	0	2	2	1	1	1	1
Enterprises computerization	Computerization level (Cultural point of view)	0	2	2	2	2	2	2	3
	Computerization level (Equipment)	0	0	1	2	3	1	2	2
	Systems heterogeneity	0	0	1	1	0	0	1	1
Culture and management	Information sharing / Confidentiality	0	2	3	3	2	3	3	3
	Financial means	1	1	2	2	2	2	2	3
	Management policy	0	3	0	3	2	2	3	3

Figure 4 - Evaluation of the different types of nodes according to criteria clusters

These main criteria can take qualitative values. For instance, the stability values of an alliance can be *stable*, *weakly evolution*, *potentially high evolution*, or *unknown*. This permits us to build profiles for alliances according to each client and server type. We draw these profiles with radar charts where there is one axis for each criteria without a "not important" value (cf. figure 4) and an area for the validity of the node type. Then the decision maker can instantiate his own alliance with his own point of view : *Is the alliance stable ? or weakly evolutive ? etc.* At last, the decision maker can match the two radar charts in order to see if each node type is useful for his own alliance (cf. figure 5).

4. CONCLUSION AND FURTHER WORK

This guideline can bring SME managers to be in a position to easily evaluate which communication infrastructure is suitable for them to cooperate inside an alliance. But managers pay more and more attention to security problems. So this work has to be continued with the integration of some additional well-developed criteria close to security and confidentiality, and solutions close to Virtual Private Networks. In the GRECOPME consortium, another workgroup has developed a similar Decision Aided Tool (MAPSI) about the choice of an Information System and groupware

tools. Our propositions has now to be interfaced together because not all infrastructure can support any software systems.

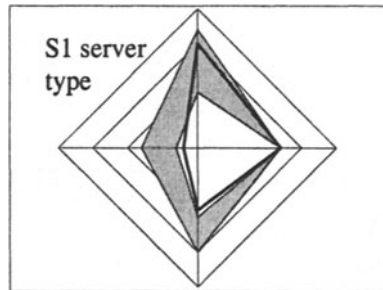


Figure 5 - Matching a profile and an alliance for the S1 server type

5. REFERENCES

1. Biennier F., Beaune P., Marcon E., 1999, Organization and Management of a Distributed Information System Shared by a Pool of Enterprises, Proceedings of IEPM'99, July 12-15 1999, Glasgow (Scotland), Vol. 2, pp. 465-475.
2. Biennier F., Favrel J., 2001. Secure collaborative information system for enterprise alliances: a workflow based approach. To appear in ETFA'01 proceedings. Juan les Pins, October 2001. 8 pages
3. Davidson M.A., 2001. Security for eBusiness. Information security technical report 6(2). pp.80-94
4. Fariselli P., Oughton C., Picory C., Sugden R., 1999. Electronic commerce and the future for SMEs in a global market-place networking and public policies. *Small Business Economics* (12). pp.261-275
5. Giachetti R.E., 1999. A standard manufacturing information model to support design for manufacturing in virtual enterprises. *Journal of Intelligent Manufacturing* (10). pp. 49-60
6. Consortium GRECOPME, 2000. Project GRECOPME: Final report. *Internal report*. 97 pages
7. Li H., SU S.Y.W., 2000. Business object modeling, validation, and mediation for integrating heterogeneous applications systems. *Journal of Systems Integration* (10). pp. 307-328
8. Liang T. P., H. Lai, N.S. Chen, H. Wei, M.C. Chen, 1994. When client / server isn't enough: coordinating multiple distributed tasks. *IEEE Computer*, 27 (5). pp. 73-79
9. Malone T., 1997. Is empowerment just a fad ? Control, decision making, and IT. *Sloan Management Review* 38 (2). pp. 23-35
10. Mott S., 2000. The second generation of digital commerce solutions. *Computer networks* (32). pp. 669-683
11. Oh J. C.J., Chang S.G., 2000. Incentives for strategic vertical alliances in online information product market. *Information Economics and Policy* (12). pp. 155-180
12. Ordanini A., Pol A., 2001. Infomediation and competitive advantage in B2b digital marketplaces. *European Management Journal* 19(3). pp. 276-285
13. Osorio A.L., Barata M.M., 2001. Reliable and secure communications infrastructure for virtual enterprises. *Journal of Intelligent Manufacturing* (12). pp. 1 71-183
14. Sandakly F., Garcia J., Ferreira P., Poyet P., 2001. Distributed shared memory infrastructure for virtual enterprise in building and construction. *Journal of Intelligent manufacturing* 12). pp. 199-212
15. Taylor M.J., Sheehan J.F., Mulhaney A., 2001. Soft issues in small-scale network development and implementation: a case study in an SME. *Systemic practice and action research* 14(3). pp.239-249
16. Unitt M., Jones I.C., 1999. EDI: the grand daddy of electronic commerce. *BT Technology Journal* 17 (3). pp. 17-23
17. Wicaksana D.S., Adibrot A., 1995. Data base concept on computer integrated manufacturing in enhancing product's quality. in Proceedings of « Congrès International de Génie Industriel de Montréal: La productivité dans un monde sans frontière », Langevin A., Riopel D., Kieffer J.P. Eds., Montréal: Editions de l'école polytechnique de Montréal, vol. 1, pp. 571-576
18. Zhang Y.P., Zhang C.C., Wang H.P., 2000. An internet based STEP data exchange framework for virtual enterprises. *Computers in industry* (41). pp. 51-63