LOCAL VALUES
in a
NETWORKED
DESIGN WORLD

ADDED VALUE OF COMPUTER AIDED
ARCHITECTURAL DESIGN

DUP Science

scientific committee

HENRI ACHTEN	**TU-EINDHOVEN**
ALEXANDER ASANOWICZ	**TU-BIALYSTOK**
ANDY BROWN	**UNIVERSITY OF LIVERPOOL**
ADAM JAKIMOVICZ	**TU-BIALYSTOK**
JONAS AF KLERCKER	**TU-LUND**
GERNOT PITTIONI	**INGENIEURBÜRO DR. PITTIONI MÜNCHEN**
MARTIJN STELLINGWERFF	**W&K, SINT-LUCAS / TU-DELFT**
JOHAN VERBEKE	**W&K, SINT-LUCAS**

Printed in the Netherlands.

A World of Networks
Global and Local Impacts

AUTHOR

Gernot Pittioni

Ingenieurbüro Dr. Pittioni
Germany

Abstract

As a couple of years ago the use of computers slowly entered studios of architecture, the development of operating systems actually enables everybody to control even bigger networks within studios or offices. Recently these local networks started to get networked themselves.

Interactions between local design partners involve a large variety of problems

- different CAD-systems
- different versions of the same CAD-system
- different methods of transfer
- different security ideas
- different levels of technical knowledge

In the course of extension to a global level these problems in the first approach have been growing dramatically, involving additionally language and mentality problems. But in the outcome the exchange of documents and ideas improves in speed, quality and accuracy or this will at least happen in the near future.

Global networking offers a great challenge, we have to give this matter a big deal of efforts to earn the values and results, which may be achieved.

1   Introduction

It is wonderful to use computers. It is less wonderful to organise a secure net of computers. And it may be a troublesome activity to interact with other networks.

But why not consider it the other way round: It has been troublesome to introduce computers into the world of architectural studios. Things improved after collecting and storing data centrally by using local networks. Today we witness the values of a continually growing global network activity.

profession	employees	Operating system	LAN since	remarks
building ser-vices engineers	75	WINDOWS	1982	Multiple servers (NT, Linux) firewall and high security level network operated by service
engineer	12	WINDOWS	1985	NT-Server Considerable security facilities
engineer	18	WINDOWS	1985	NT-Server Considerable security facilities
building ser-vice	12	WINDOWS	1985	NT-server, good security, network-manager
engineer	5	WINDOWS	1987	Linux-Server Considerable security facilities
surv. engineer	15	WINDOWS	1987	Most expensive hardware
construction office	15	WINDOWS	1989	working with foreign PC-places (eastern Europe)
architect	6	WINDOWS MAC-OS	1990	NT-server, medium security network-manager
architect	28	WINDOWS	1991	NT-server, substantial security
architect	20	WINDOWS	1991	NT-server, medium security network-manager
architect	4	MAC-OS WINDOWS	1992	no special security no servers
architect	3	WINDOWS	1994	NT-Server, network manager
architect	3	MAC-OS	1994	firewall no network management
architect	7	MAC-OS WINDOWS	1995	Linux + NT-server, good security, network manager
architect	8	MAC-OS WINDOWS	1996	no servers no special security
architect	2	WINDOWS	1996	NT-Server, no security
architect	4	WINDOWS	1996	no server, network manager
architect	2	WINDOWS	1998	LINUX Server
architect	4	WINDOWS	1998	NT-server, medium security network managed by crew
architect	3	MAC-OS	1999	no server, firewall
architect	3	WINDOWS	2001	no server, no special security

Table 1 – network statistics of planning partners

We should try to get a firm hold on the doubtlessly valuable features instead of complaining about eventual drawbacks.

Using network-facilities brings different questions and has to be seen from different viewpoints:

- Which kind of communication do we want to establish
- Which level of security do we want to apply
- What kind of hard- and software is necessary

2 Networking locally

Modern operating systems offer easy facilities to run a LAN – a local area network. Generally no substantial knowledge is necessary installing this network and running the readily installed system.

Similar to former papers I have investigated the situation in the studios and offices of my planning partners. It is interesting to see that even those who had sworn four years ago to never touch any computer and who refused to send and receive any e-mails, they are having pretty networks in their studios, they produce CAD-data and are familiar with e-mails. In most cases it is done by the younger persons and not by the studio-owner, but this does not matter.

I have no deeper knowledge how all those networks are operated in detail, but as planning partner I cannot see any substantial problems there. To communicate with them is another problem, but this is handled later.

Collecting the networking statistics of some of my planning partners gives an interesting overview (see table at previous page).

A closer view gives us the following insights: Networks got common in engineering offices about fifteen to twenty years ago, architects followed a couple of years later. This we know for long.

Engineers don't use MAC-systems, architects are fond of MACs, but some MAC-users added PCs within their studios in order to avoid communication-problems with the PC-world.

Security still is a subject, which is handled very differently. Engineers apply more weight to security aspects, architects are either most careful or most careless or everything in between. Some are extremely afraid of virus-attacks and refuse to connect their local networks to the internet. I even saw stand-alone computers which did the job.

In former papers we discussed the problems we run into by sharing CAD-data using different systems, even different platforms. I have to confess, that things get better only at a slow pace. We very often have to handle CAD-data, which were produced on a very low level. As we pointed out at former occasions, that we mostly do not have any chance to see the quality of the transmitted data as long as you have not checked the contents of the layers. We still have to complain that we get very complex drawings from our architectural partners, where we simply do not have any chance to extract some reasonable input for our work. Graphic information, texts, numbers, hatchings, the plants and flowers, the symbols, everything is crunched up in one single layer or distributed within the layers on a random basis.

We witness a lot of different connection methods, if partners distribute information from LAN to LAN. This is the interesting point where we extend the subject from local networks to external networks. In our case only the distribution and data-transport of CAD-data is of interest and not specifically text-files or similar.

3   Connecting networks

Here we are hitting the interesting point. How does one planning partner in his own network get his information from the other one, who is working within another network. Similarly the same questions came up if offices developed branches.

For many years we transferred data from planning partner to planning partner by means of one or more CD-ROMs. This seemed to be safe and easy. Even in our days many data migrate this way, some partners refuse to do it otherwise.

We could very soon forget floppy disks to do this service, as they are having a very restricted volume of 1.44 Mbytes. There existed some media in between e.g. with ZIP-disks, which offer 100 Mbytes and thus enable partners to transfer reasonable volumes.

3.1 Transferring data by snail-mail

But at first we must accept, that by using CD-ROMs or other media we have to use snail-mail again. First we have to copy our data to these means of mass-storage, post it and the partner has to do the same vice-versa afterwards. It does not matter, if we compress – and decompress – the data, we interrupt the wonderful flow of electronic matter, by writing it to some kind of media and post it.
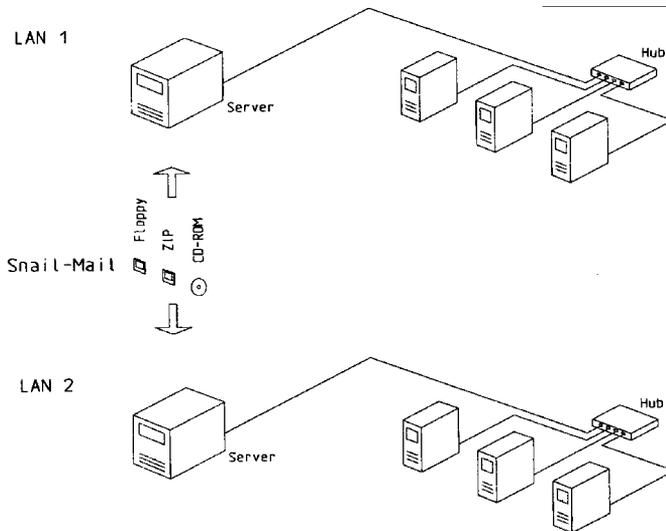

Figure 1. Snail-Mail

So very soon the need came up to avoid this intermediate phase, which did by no means fit into an over all electronic handling to transfer data between networks.

3.2 File transfer via phone

File transfer via phone-lines was the next step. Some of the partners even in our days stick to this method out of reasons, which refer to the phone billing. I cannot appreciate this kind of argumenting, as the phone-companies in our days offer billing-methods, which fit rather nicely to our needs.

Anyway, we have to describe the method. Each network provides some securely separated disk-space, and communicates with the other network by means of a password and the telephone. If we wanted to transfer a file-set, we had to call the other partner, tell him to connect his system to the phone-line. We could watch this procedure on the screen. Then the data transfer could start, data crawled very slowly, restricted by the phone-transmission. The partner, who transferred the file-set was paying the bill.
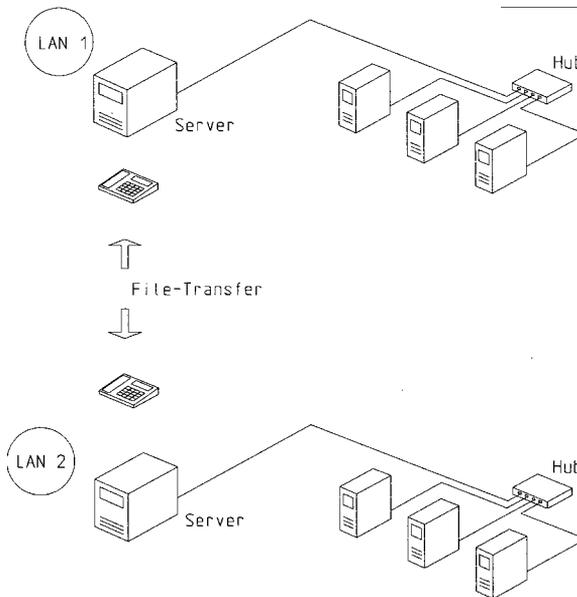

Figure 2. File transfer

Statistically this method of transferring files from network to network has lost any importance in our days.

3.3 Project-Servers

We practised this only when we had to handle large or very large projects, in Euros we would speak approximately about 20 millions and up.

Technology and software are rather old, but somehow the time needed for transmission did not satisfy. In our days of DSL-connection we should expect better performance. But today offices rarely refer to this method, because modern methods with modern technology using the internet are taking over.

The nice thought behind was that we could offer any project-participating person any information of the whole project. Of course this has to be limited for security-reasons. Any planning partner could apply for connection to the project-server, just verifying his

identity and getting access to the server by a password. The system checked his entry and allowed him to connect, to submit respectively to download information.

But, as data were growing rapidly within a large project and as the number of planning partners increased, there were numerous access-requests to the project-server. And the data flow afterwards via mostly weak and restricted phone-lines produced frustration, as long waiting periods were common.
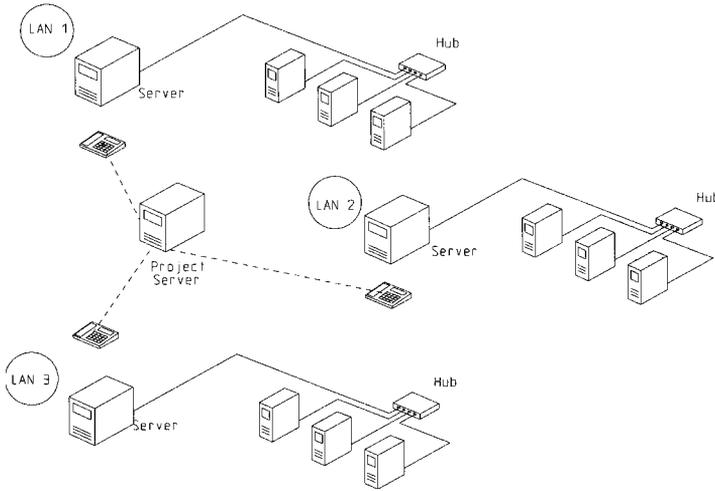

Figure 3: Project Server.

If more than two large projects were to be handled by the same project-server, the system soon was ignored by the partners, they returned back to fax and snail-mail. As explained above this technology has limited chances to survive, as other transfer-methods, even for large projects, are showing up.

3.4 Connecting networks via e-mail

E-mail-connection brought new power to the needs of data transfer. Very soon e-mail was not only used for short messages and limited sketches. The e-mail traffic concerning relevant data within networks grew substantially. Out of my experience this way of transmitting data is the most important in our days.

Partners observing narrowly their telephone-bills often were fighting the e-mail-connection, as everybody who sends information has to pay and everybody who gets information is paying as well. This was a feasible reason to refuse as long as the transmission was slow, but this has improved a lot. We should educate our partners to compress the data, but here sometimes problems show up working on different platforms.
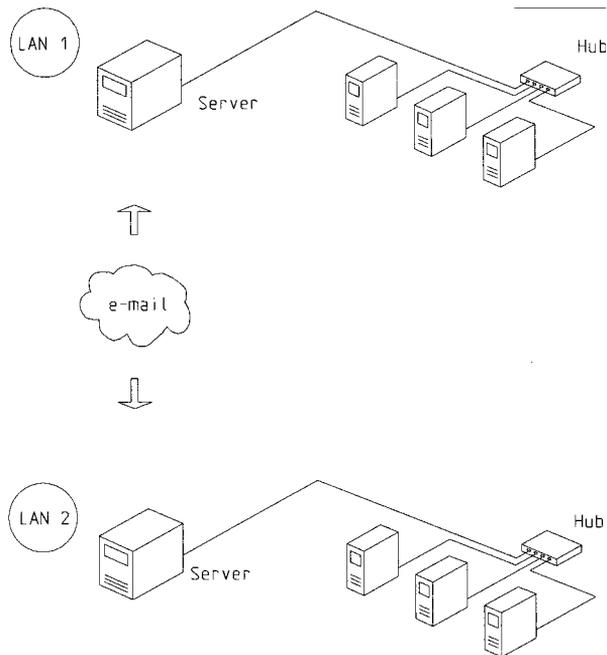
Figure 4. e-mail Transmission.

The only substantial drawback of this transmission is, that it exposes networks to partly substantial security risks. The risks of outside attacks are higher than with the other methods shown. We have to educate the partners to install efficient security features.

3.5 Connecting networks via VPN (virtual personal networks)

We rarely can expect that our activities are confined to an area around our office-location. The more tight the markets get, the more we are forced to travel. This may be a special German problem in this time, but generally it is a common concern. Many studios and offices tried to take roots in distant areas.

Travelling involved that we were cut off of information stored on our local network. The same problem arises, when distant office-locations want to connect to common data. This generates the need to expand the local network, the birth of VPN (Virtual Personal Network) was promoted. VPN uses the web for communicating distant locations, providing a secure tube, a "tunnel", through the billions of data within the web. When e-mail literally is shot through the web, VPN builds a sort of permanent connection.

These distant locations connected by VPN need not to be stationary, they may also be mobile. So we may connect our laptop to a mobile phone in some airport lounge, call up the VPN-connection and can move around the network data storage, as if we would sit relaxed in our office at home. Of course this requires powerful connection capacities, but these are easily topped by those kids, who want to download the newest music-events by their phones. We should love those kids.
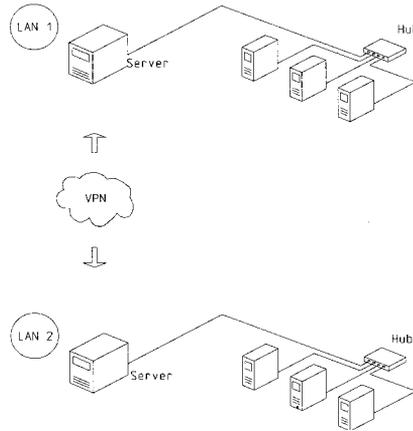
Figure 5: VPN (virtual private network) .

So we may summarize the facilities of VPN:
- Connection between two or more stationary locations
- Connection between two or more stationary and/or mobile locations

This is the vision of modern networking. Especially if there are more networks within one office-structure, we can use VPN successfully. The security problems are substantial, some words follow in the next chapter.

3.6 Download/Upload-Area on Homepages

Offering common information to planning groups we see a very simple way to do this. We can place this information on the homepage and allow downloading access to our partners – eventually by using a password, depending on the respective need to protect our data. Of course this extremely simple feature ends, when we want to extend the use to uploading activities, as security action tends to get much more sophisticated.
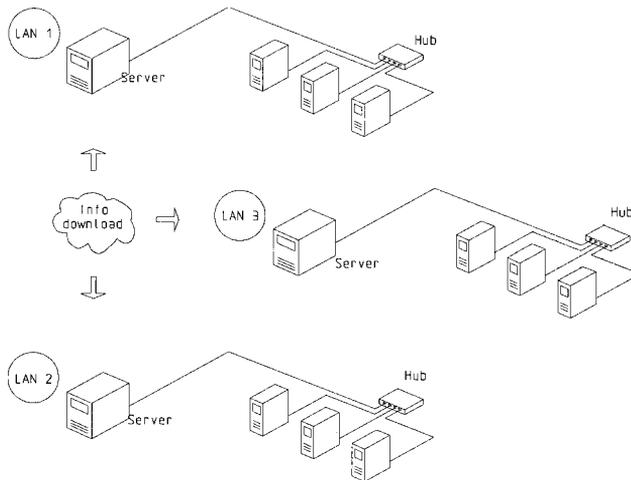

Figure 6: Information download

ADDED VALUE OF COMPUTER AIDED ARCHITECTURAL DESIGN

This method is a simplified version of the former spreading of information by project-servers, using the internet instead of telephone transmission. Those servers were equipped with expensive software, whereas the download area on the homepage can be done by any internet-user, capable of a little HTML.

Figure 7. Example of Download Area on Homepage .

Security is low of course and will be analysed – very generally – in the next chapter.

4   Security aspects

Generally security will differ in meaning, as we proceed from the simple LAN-structure to highly-sophisticated network-communications across the borders. So it will be appropriate to distinguish between the levels discussed in the former chapter. Nevertheless we should state at this point, that we in the first line want to see networking from a practical point of view and not from a theoretical point of security. Especially if we enter the use of the web, the discussion of fighting attacks is far from achieving really satisfying solutions. This results in very high-sophisticated encrypting methods, which have to be provided by the net-managements.

Security of delicate data gives a lot of headache to the network managers. And everybody has gone through the painful process of cleaning his system of undesirable junk material, which intruded the hard-disk coming over the e-mail-facilities.

Of course we have to distinguish between the inner security within the network and the

security-problems, caused by accepting data via media, phone-lines or internet. Here we focus on the second part, the inner security – though this is an outstandingly important subject and not always easy to handle – we have to subsume to being done more or less nicely by the respective network-users.

4.1 LAN to LAN by traditional media

Security within a Local Area Network – LAN – is mainly a question of data saving discipline, as said above. Security of data-transmission is reduced to the concern, is the medium (CD-ROM or formerly floppy-disk) infected or not. This can be handled by an accurately updated virus-protection. In the days of these media mostly stand-alone computers (not connected to the office-network) did the job of testing the media, prior to saving the data to the network-server.

4.2 File transfer by phone

Using download areas on servers only protected by simple passwords gives us a feeling of low security. No encrypting methods are provided and the partners have to be very careful not to get infected by incoming data.

4.3 Project servers – transmission by phone

Here the same problems as to security are found as with file-transfer. The only advantage is that the partners do not need to worry about infection of their data. This is the problem of the network-manager who has to care for the project-server.

4.4 Data-transmission by e-mail

This is the most common transmission-method in our days. Obviously this is most attractive for hacker-attacks. But, as we could watch in the past, those most efficient attacks came by mails, which were spread by automatically sent mails with a special attachment. They rarely can intrude our networks by mails with an attachment, consisting of CAD-data. Provided that our partner did not realize his infection and has sent the infected data unintentionally. And this we should be able to take for granted, that we do not collaborate with partners, who really want to send us infected data.

We have to face the danger of computer-viruses embedded in the attachments – and the data we transmit come by the attachments. So, the solution is rather easy, we have to be careful, while opening the attachment.

We can care for the safety of received data by providing an efficient firewall in the mail-server of the network as well as a thoroughly and automatically updated virus-protection on all computers in the network, which may accept e-mails. If the data are infected and the attachment is opened, the protection comes up at once with a significant warning. In this case we have to do the following:

- delete at once this infected attachment
- send an e-mail back at once to warn the partner that he is spreading infected data - a matter of good partnership
- urge the partner to immediately warn all other partners, he eventually has already sent the data.

Doing so, we can be rather confident to confine any possible damage by transmitted attachments.

4.5 Data-transmission using VPN

This very nice feature of course offers a wonderful challenge for attacks. We have to consider the unbelievable fact, that we try to establish a safe connection from one network to the other over the web, where billions of data – and unfriendly hackers – are crossing our way. The specialists call this tunnelling – the VPN-technology is building up a safe tunnel through the web for our connection. There exists a variety of tunnelling methods, which are very special. I think we should avoid to get into this deeper, as we mostly depend on the skills of our network-managers and cannot do much ourselves.

Within the tunnels the data run encrypted. What we said about the tunnelling methods is as well valid for the encrypting methods. The scientists have been developing these methods for decades, and in spite of this we witness every now and then that intruders are getting over these security-barriers.

After all we have to face the fact, that our system is rather widely exposed if somebody could intrude the connection. I myself am using VPN widely, I do not hesitate to connect to my servers by VPN from anywhere by my notebook and mobile phone, but I hide sensitive data within not accessible areas of my system.

We cannot do more in this point than to rely on the technology and use VPN or, if we are not convinced, leave this nice feature.

4.6 Using download areas from internet-pages

This is a very easy method, offers access to very limited data and therefore does not need extended security. I can judge the vulnerability of my information I want to put into the download-area. And if the community of partners decides to not store some special data there, we can apply on them the more sophisticated methods.

I am fully aware that the mere application of a password to enable access to the different sections of the download area offers only very low security for someone who uses professional hacker-tools. But once again, it is entirely our choice to select the data to present in the download area. This area, of course, is vulnerable to a certain extent.

The use of the password can be done in a way, that even more experienced web-users cannot read out the password needed, by studying the html-text, which is easily to access. An extremely simple way is to use the hyperlinked filename of the thus protected section, which cannot be seen by mere reading the html-text of the calling file.

5 Encrypting methods

As said above these methods are very special technologies and should not be a matter of deeper interest within our practical oriented focus. Anyway using connections within the web should create our concern and without any doubt we have to consult our network-specialists and ask them to explain thoroughly, which risks we are taking on behalf of which data within our system.

Generally they will be happy to confuse us with a variety of special terms we never have heard before. And if we ask for some explanations, we risk to not understand very much.

The cruel thing is that new technologies, which are added to an existing security-system may interfere in a way, that you have a lot of confusion afterwards. Authentification-methods may not co-operate with password-administration technologies. A lot of testing applied on the "hot system" is necessary.

Specialists speak from encrypting on a serie of levels – and there are seven levels of encrypting. Watching the messages, which hurry over the screen e.g. of a LINUX-administrated gateway, we will often see the term IPSec – security on IP-level. Special cryptographically protected codes and check-sums, which are sent with the packages, ensure the safety of our transmission.

The problem is presented mainly by the question, how can we enable the addressee to read the encrypted message, without enabling somebody to do so, who is trying to attack the transmitted data. There are symmetric and asymmetric encrypting methods and a variety of higher developments. Everybody, who uses home banking facilities will know, that the access affords a certain level of encrypting and we have to download the needed software.

Of course developers are working on always better encrypting methods, we are waiting for the AES, the Advanced Encryption Standard, which will be a symmetric algorithm, supporting 128, 196 or 256 bit length.

6   Hardware-requirements

As with everything concerning computers we witness the process of minimization also in the field of the hardware requirements of network-components.

Some years ago everything started with the print-servers, when computers with common size, which did the job, could be replaced by little boxes, somewhere hidden behind the printers. And a few weeks ago I watched my network-specialists remove a gateway-computer, weighing considerable 30 pounds, by a little equipment of the size of a cigar-box – see figure 9, where I added my mobile phone and a floppy disk to the picture, in order to get a feeling of the scale.

Figure 9: replacing the hardware

ADDED VALUE OF COMPUTER AIDED ARCHITECTURAL DESIGN

7   Conclusion and outlook

Summing up the above we can realize the development of a quickly growing network community, which has already crossed the borders.

We are earning the benefits of enormously efficient transmissions. We can tell our partners abroad by e-mail that we are needing some specific data urgently, and twenty minutes later we can open the respective attachment of the answering e-mail. The "delay" is mostly represented by the human reaction time and the search for the files within the partners' systems.

We discussed a variety of connecting procedures between different networks and glanced shortly at security and encryption methods.

The design process is taking advantage of these added values as the considerable delays caused by the traditional transferring processes, in near future are more and more reduced to the mere activities of human understanding and reacting.

8   Acknowledgements

9   References

Af Klercker, J. Henrichsen, J.: 2001, Can simulations in VE support architects in solving complex design problems, *in* Stellingwerff, M., Verbeke, J.: *ACCOLADE – Architecture – Collaboration Design,* DUP Science 2001

Kruijff, E., Donath, D.: 2001, Supporting Shared Architectural Understanding, *in* Stellingwerff, M., Verbeke, J.: *ACCOLADE – Architecture – Collaboration Design,* DUP Science

Madrazo, L.: 2001, NETWORKING: a web environment for a collaborative education, *in* Stellingwerff, M., Verbeke, J.: *ACCOLADE – Architecture – Collaboration Design,* DUP Science 2001

Maver, T., Petric, J.: 2001, MEDIA in MEDIATION: Prospects for Computer Assisted Design Participation, *in* Stellingwerff, M., Verbeke, J.: *ACCOLADE – Architecture – Collaboration Design,* DUP Science 2001

Pittioni, G.: 1997, CAD as Interaction Instrument between Planning Partners, *in: Added Value of Computer Aided Architectural Design*, 1st AVOCAAD International Conference – Brussels 1997, Proceedings.

Pittioni, G.: 2001, Present and future issues of networking activities seen from the engineering practice, *in* Stellingwerff, M., Verbeke, J.: *ACCOLADE – Architecture – Collaboration Design,* DUP Science 2001

Szewczyk, J. Jakimowicz, A.: Multi User Interface Problems in Current CAD Systems, *in* Stellingwerff, M., Verbeke, J.: *ACCOLADE – Architecture – Collaboration Design,* DUP Science 2001

ADDED VALUE OF COMPUTER AIDED ARCHITECTURAL DESIGN